Nottinghamshire Information Sharing Protocol

Version	1.7
Date	May 2018
Author	Nottinghamshire Records and Information Group
Document Owner	Nottinghamshire Records and Information Group
Approving Committee	Nottinghamshire Records and Information Group
Review Date	May 2020

Change History

Version	Date	Description of change
0.01	May 2014	Draft
0.03	July 2014	Amended in line with consultation with members of the Records and Information Group
1.0	August 2014	For individual organisational approval
1.1	February 2015	Derbyshire Health United signed the ISP Page numbers for appendices have been amended
1.2	March 2015	CNCS and Nottinghamshire Police signed the ISP
1.3	October 2015	CRI Nottinghamshire* signed the ISP *CGI (Change, Grow, Live), as of the 1st April 2016
1.4	December 2015	Age UK signed the ISP
1.5	May 2016	Additions re sharing for purposes of safeguarding, updates to legislation, sharing with the fire service, sharing with the police and added appendix re responsibilities for accessing other organisations clinical or information systems
1.7	May 2018	Reviewed and updated in line with legislative changes

Version: 1.7

Contents

1. Why do we need a Protocol to share information?

Organisations already share a great deal of information, much of which is general, strategic or financial in nature, and some of which is personal confidential data relating to individual citizens. With statutory agencies, organisations, the voluntary and the private sectors working more closely together, patients and the public need to have confidence that information held about them is shared securely and appropriately to promote optimum care and personal safety, whilst respecting individual rights to privacy and confidentiality.

Both public and private organisations working with patients and citizens in Nottinghamshire must demonstrate a commitment to share information responsibly, appropriately, and securely. They must establish procedures and agreements that manage the exchange of information, and make sure that those processes are open, transparent, and accountable, whilst keeping personal confidential data protected throughout.

This Protocol sets out the principles and commitments that will underpin the secure and confidential sharing of information between organisations involved in delivering health and social care services in Nottinghamshire, in accordance with national and local policy and legislative requirements. The Protocol is also intended to inform members of the community why information about them may need to be shared and how this sharing will be managed**. The Protocol is an overarching principles document and on its own is not an information sharing agreement**. **Signatories are committing themselves to the production of the necessary detailed agreements to facilitate specific information sharing initiatives and to ensuring that data protection impact assessments are carried out where indicated by risk, see Appendix 8 for examples of when a DPIA may be required.**

The specific information sharing agreements will set out the detail of what information is to be shared, how it will be shared and who it will be given to. The individual Information Sharing Agreements will also set out the limits to any information sharing and the extent to which information may be passed on to a third party without recourse to the originator of that information. All individual Information Sharing Agreements have been developed by the participating agencies and comply with the principles set down in the overarching Information Sharing Protocol. The Information Commissioner's Office (ICO) Data Sharing Code of Practice should be referenced to ensure compliance with best practice requirements. Responsibility for producing Data Protection Impact Assessments and specific Information Sharing Agreements rests with the organisation leads and Information Asset Owners who require the sharing, supported and approved by the Information Governance Lead, Senior Information Risk Owner and Caldicott Guardian for each organisation.

This document represents the information sharing requirements of Nottinghamshire's health and social care community to deliver our agreed outcomes and improvements for patients/citizens. Statutory responsibilities remain, as always, with each organisation, but collectively, this represents the commitment of all parties signed up to this Protocol.

As Nottinghamshire's local health and social care community must work together to improve our agreed outcomes and improvements for our patients/citizens, it necessitates the structured sharing of information between all partners. Effective and structured sharing of

information between partners has the ability to inform care and planning, allows us to understand trends and patterns of activity, to respond to emergencies appropriately, and to support the lives and safety of individuals, families and communities. In a world of increased information gathering and recording, we have a moral and statutory responsibility to share information carefully and responsibly. Effective use of information will support us in achieving all the ambitions and aspirations we have for those living in Nottinghamshire.

2. Structure

This overarching Information Sharing Protocol outlines the principles and standards of expected conduct and practice of the signatories and their staff and applies to all sharing of personal confidential and non-personal information. The Protocol establishes the organisations' intentions and commitment to information sharing and promotes good practice when sharing personal information. It also contains the legislative standards that all types of personal information sharing must comply with.

3. Aims and objectives of the Protocol

The purpose of this overarching Protocol is to set out a framework for partner organisations to manage and share information on a lawful and 'need to know' basis with the purpose of enabling them to meet both their statutory obligations and the needs and expectations of the people they serve.

Specifically, this Protocol aims to:

- Set out the general principles of information sharing;
- Identify the lawful basis for sharing information;
- Set out generally what information will be shared;
- Define the common purposes for holding and sharing data;
- Set out how information will be stored.

4. What does the Protocol cover?

The Protocol applies to the following types of data:

4.1 Personal confidential data and personal sensitive data

The term personal confidential data refers to any information held either as manual and/or electronic records, or records held by means of audio and/or visual technology, about a living or deceased individual who can be personally identified from that information.

Certain types of personal information have been classified as special categories of personal data, the EU General Data Protection Regulation 2016/679 (**GDPR**) provides that additional conditions must be met for that information to be used and disclosed lawfully. Special categories of personal data refers to information that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, Trade Union membership, the processing of

genetic data, biometric data for the purpose of uniquely identifying a natural person (living individual), data concerning health, sexual life or sexual orientation.

4.2 Anonymised information

Information that falls into this category is data about people that has been aggregated or tabulated in ways that make it impossible to identify the details of individuals. This can be shared without the consent of the individuals involved and the processing is outside the provisions of the GDPR. However, care should be taken to ensure that it should not be possible to identify individuals either directly or in summation. This can happen when anonymised information is combined with other data from different organisations, where the aggregated results produce small numbers in a sample, or where traceable reference numbers are used. This is sometimes known as 'jigsaw matching'. Further guidance on anonymised information and requirements can be found in the Information Commissioner's Office 'Anonymisation Code of Practice'.

4.3 Non-personal information

Information that does not relate to people; e.g. information about organisations, natural resources and projects, or information about people that has been aggregated to a level that is not about individuals.

There is a general presumption and expectation that anonymised and non-personal information will be shared, unless there are exceptional reasons not to do so. These may include:

- commercial confidentiality;
- where disclosure may forfeit the organisations duty to ensure safe and efficient conduct of organisational operations;
- policy formulation (where a policy is under development and circulation would prejudice its development);
- protect other legal and contractual obligations; and
- where information is marked protectively (refer to your organisations standards for information classification for further details).

This Protocol applies to all employees' including anyone conducting business on the organisations behalf, temporary and contract staff and all employees of the organisation and partner organisations who are signatories to this information sharing protocol.

The Protocol also applies to any organisation or agency which has been commissioned to deliver services on behalf of any organisation party to this Protocol where permission has been given to the third party organisation to disclose information.

The Protocol is intended to complement any existing professional Codes of Practice that apply to any relevant professional groups working within any organisation, and does not constitute legal advice.

5. The Information Sharing Protocol Principles

This Protocol recognises that sharing of information should be done fairly and lawfully, be properly controlled and should strike a balance between the specific rights of individuals and the public interest. The following are the principles to be applied whenever personal confidential data is shared or exchanged. The organisations signed up to this Protocol are fully committed to ensuring that these principles are adhered to at all times.

The overarching principle established by this Protocol is information about individuals will be shared appropriately, securely and lawfully to promote safety and quality of healthcare for individuals and in specific purposes in the wider public interest.

The partner organisations agree:

- to share information with each other where it is lawful and when they are required to do so;
- to share information for the purpose of providing direct care in accordance to the 7th Caldicott principle 'the duty to share information is just as important as the duty of confidence' (see **Appendix 1**) and the Health and Social Care (Safety & Quality) Act 2015 legal 'duty to share information';
- To share information which is relevant to safeguard children and adults from harm;
- to comply with the requirements of the GDPR and in particular with the principles relating to the processing of personal data and the legal framework governing information sharing. For more information, please see **Appendix 2 and 3**;
- to share information in accordance with the 7 Caldicott principles, see **Appendix 4;**
- to inform individuals when and how information is recorded about them and how their information may be used as part of fair processing responsibilities;
- to ensure that adequate technical and non-technical security measures are applied to the personal data they hold and transfer;
- to develop local Information Sharing Agreements that govern the way transactions are undertaken between partner organisations and with other organisations that are not parties to this Protocol;
- to ensure that data protection impact assessments are carried out for new sharing arrangements, see appendix 8 for details of when to complete a DPIA;
- to promote staff awareness of the Protocol and ensure that staff have had the appropriate level of training in information security and confidentiality;
- to promote public awareness of the need for information sharing through the use of appropriate communications media;
- considerations of confidentiality and privacy will not automatically cease on death;
- to share information and ensure patient/citizen confidentiality by embedding the 5 rules* into organisational systems and processes.

*The Health and Social Care Information Centre's 'A Guide to Confidentiality in Health and Social Care 2013' sets out that there should be no surprises about how confidential information about individuals is used and the five rules set out how the obligations are to be fulfilled:

Rule 1: Confidential information about service users or patients should be treated confidentially and respectfully.

Rule 2: Members of a care team should share confidential information when it is needed for safe and effective care of an individual.

Rule 3: Information that is shared for the benefit of the community should be anonymised.

Rule 4: An individual's right to object to the sharing of confidential information about them should be respected.

Rule 5: Organisations should put policies, procedures and systems in place to ensure the confidentiality rules are followed.

6. Commitments in support of the Protocol

Signatories to this Protocol are committed to the implementation of an appropriate level of Information Governance throughout their organisation, in accordance with recognised national standards including the Information Governance Toolkit (see Appendix 6 which outlines staff responsibilities when accessing another organisations clinical information system).

Signatory commitments include:

- Adhere to the principles and commitments of this Protocol whenever exchanging personal information, whether with a co-signatory or other agency/organisation;
- Share statistical and anonymised data wherever possible, eliminating the use of personal confidential data except where reasonably necessary;
- Ensure that all staff (including temporary employees, contractors and volunteers) are aware of and comply with their responsibilities arising from both the Protocol and relevant legislation, and receive adequate training in order to do so;
- Implement their own policies, protocols or guidance on confidentiality, data protection, information security, records management and information quality, which are appropriate to their organisation and comply with recognised codes of practice.

Establish efficient and effective procedures for:

- Ensuring that the legal basis for processing personal information (including sharing) is clearly identified.
- Where there is no specific legal duty to process personal information, consideration should be given to obtaining fully informed, explicit consent from individuals whose data are being processed. Consent must not be offered if processing is otherwise mandated by law and/or other regulatory requirements;
- Informing citizens what information they collect and share about them, whether or not the basis for processing (including sharing) is consent;
- Sharing of personal information identified as part of a detailed information sharing agreement;
- Addressing complaints arising from the misuse or inappropriate disclosure of personal information arising from information sharing decisions;

- Enabling access to records of individuals by those individuals on request;
- Amending records where they have been shown to be inaccurate and informing partners where these are shared;
- Reviewing and destroying information in accordance with good records management practice and the Information Sharing Protocol;
- Sharing information without consent when necessary, recording the reasons for that disclosure (including legal basis) and the person responsible for making the decision;
- Making appropriate information-sharing an obligation on staff and allocating senior staff responsibility for making complex disclosure decisions;
- Ensuring that personal information is protected at all times, through the use of appropriate protective marking, security and handling measures;
- Developing and working to detailed, specific information sharing agreements that support identified purposes;
- Ensuring that future developments in technology reflect the requirements of the Protocol and any detailed protocols that support it;
- Sharing information free of charge unless special charging arrangements have been agreed;
- Seeking legal advice where appropriate;
- Ensuring their registration as Data Controllers with the Information Commissioner's Office is adequately maintained for the purposes for which they may need to process and share information with one another;
- Supporting the principles of equality and diversity within the community and ensure that whenever information is provided to the public it will be supplied in appropriate formats and languages;
- Supporting the principle that secure and lawful sharing of information can protect patients, individuals and the public.

7. Purposes for which information will be shared

In relation to the sharing of personal confidential data you must ensure that it is justifiable and is supported by a sound legal basis which can be through:

- Legal/statutory [1](e.g. sharing for direct care in accordance with Caldicott principles and 'best interests' under the Mental Capacity Act 2005)
- Sharing specifically in regards to safeguarding adults and children (e.g. in compliance with the Children Act(s) 1989 and 2004 and the Care Act 2014)
- Consent [2]

[1] Examples of legal bases for processing can be found in Appendix 10

[2] For GDPR purposes use of consent to share may not be the most reliable basis for a public authority. Under the common law duty of confidence consent may still be considered for disclosure of confidential material. However, data may be shared without consent in cases where there is an overriding public interest.

- Court Order
- Exceptional circumstance e.g. serious harm/wider public interest outweighs the duty of confidence (e.g. support investigation of a serious crime).

In consideration of the purpose of the data sharing you must firstly consider whether anonymised data is adequate to meet the purpose. This is a requirement as set out in the Caldicott principles and rule 3 of the Health and Social Care Information Centres' (HSCIC) 'Guide to Confidentiality in Health and Social Care', there is also addition guidance provided by the Information Governance Alliance which should be read in conjunction with this document.

The partner organisations will ensure that information is requested and shared on the principle that it will be made available only on a justifiable 'need to know' basis. This means that staff will have access to information only if the function they are required to fulfil in relation to a particular citizen cannot be achieved without access to the information in question.

Sharing personal confidential data and personal sensitive data (please also refer to 7.1 and 7.2 regarding consent considerations)

- to support the provision of direct care to patients/citizens and avoid duplication of information gathering;
- to allow provider organisations to cooperate so that they can deliver the care and services that those with complex needs rely on;
- to ensure that children, young people, adults with care and support needs and the public are protected through statutory multi agency co-operation and information sharing for example through the policies and procedures of the Local Safeguarding Children and Adult Boards or Multi Agency Public Protection Arrangements.
- to support the investigation of complaints or actual/potential legal claims;
- to ensure compliance with legal and or statutory responsibilities e.g. court orders;
- to support statistical analysis for research and teaching.

Sharing **anonymised information**- it is generally accepted that anonymised data can be shared to support the following purposes.

- to support the provision of quality local data at appropriate levels so that policy is evidence-led;
- to support the planning and commissioning of more efficient, easier to access services;
- to support improvements to existing and new services;
- to manage, report and benchmark performance;
- to promote accountability to patients, stakeholders, local residents and Government;
- to monitor and protect public health and well-being;
- to enable better co-ordination in promoting and marketing of public events across Nottinghamshire.

Sharing **non-personal information**

- to support collective partnership working and projects;
- to support organisational communication and marketing;
- to comply with statutory obligations, including but not limited to requests for information. This will typically be requests your organisation would probably deal with under the provisions of the Freedom of Information Act 2000 and/or the Environmental Information Regulations 2004.

Please note, it may not be necessary to disclose all information held regarding a patient/citizen and only such information as is relevant for the purpose for which it is disclosed should be passed under the sharing arrangement to the recipient(s).

7.1 Sharing with consent

7.1.1 Sharing with consent under GDPR

If organisations are relying on consent under the GDPR they must have considered the consent checklist developed by the Information Commissioners Office:

- We have checked that consent is the most appropriate lawful basis for processing.
- We have made the request for consent prominent and separate from our terms and conditions.
- We ask people to positively opt in.
- We don't use pre-ticked boxes or any other type of default consent.
- We use clear, plain language that is easy to understand.
- We specify why we want the data and what we're going to do with it.
- We give individual ('granular') options to consent separately to different purposes and types of processing.
- We name our organisation and any third party controllers who will be relying on the consent.
- We tell individuals they can withdraw their consent.
- We ensure that individuals can refuse to consent without detriment.
- We avoid making consent a precondition of a service.
- If we offer online services directly to children, we only seek consent if we have age-verification measures (and parental-consent measures for younger children) in place.

7.1.2 Sharing with consent under the duty of confidence

In seeking consent to disclose personal confidential data, the individual concerned will be made fully aware of the nature of the information that it may be necessary to share, who the information may be shared with, the purposes for which the information will be used and any other relevant details including their right to access, withhold or withdraw consent.

For further guidance on consent, please see **Appendix 5**.

7.2 Sharing without consent under GDPR

Some key legislation aims to ensure that children, young people, adults with care and support needs and the public are protected through statutory multi agency co-operation and information sharing.

The **Children Act 2004** (s. 11) provides a legal basis for the processing and sharing of relevant data by the relevant public sector bodies that are partners to this agreement.

The Act, although amended by the Health and Social Care Act 2012, does not provide a basis for processing by non-Public Sector bodies, i.e. healthcare providers that are not NHS Trusts or NHS Foundation Trusts, charities, or private providers.

The Act emphasises the importance of safeguarding the welfare of children by stating that relevant partner agencies - which include the Police, Children's Services Authorities, Clinical Commissioning Groups, NHS Commissioning Boards and other NHS statutory bodies, must ensure that functions are discharged having regard to the need to safeguard children. The Act (S10) also states that they must make arrangements to promote co-operation between relevant partner agencies to improve the well-being of children in their area. Well-being is defined by the Act as relating to a child's:

- physical and mental health and emotional well-being
- protection from harm and neglect
- education, training and recreation
- the contribution made by them to society
- social and economic well-being

Although most commonly used to refer to young people aged sixteen or under, 'children' in terms of the scope of this Act means those up to the age of eighteen.

The **Children Act 1989** provides for children and young people information can be shared under s.47 (children in need of protection) or even s.17 (children in need of services) Children Act 1989[3]. If the information to be shared does fall within these sections of the 1989 Act, then these will be the main legal gateway.

The **Care Act 2014**, section 6, provides a legal basis for sharing information in respect of adults at risk of abuse or neglect by placing a duty on local authorities and their statutory partners to cooperate in order to protect adults with care and support needs experiencing, or at risk of, abuse or neglect. The statutory partners include the Police, the Probation Service, Clinical Commissioning Groups, NHS Commissioning Boards and other NHS statutory bodies.

The **Localism Act 2011** gives local authorities the power to do anything that individuals may generally do. Under S1 of the Act they have the power to do anything which they consider is for the benefit of the authority, its area or person's resident or present in its area.

[3] http://www.legislation.gov.uk/ukpga/1989/41/contents

Crime and Disorder Act 1998[4], section 115, provides a legal basis for sharing information for the prevention and detection of crime and disorder with: Police; Probation; Local Authorities; NHS Trusts; Clinical Commissioning Groups and other NHS statutory bodies.

Fire and Rescue Services Act 2004, section 5A, provides a legal basis for sharing relevant information by providing the fire and rescue authority with a power to do (a) anything it considers appropriate for the carrying out of any of its functions, (b) anything it considers appropriate for purposes incidental to the carrying out of any of its functions (whether directly or indirectly incidental) or (c) anything it considers to be connected with (a) or (b).

Human Rights Act 1998 gives force to the European Convention on Human Rights and, amongst other things, places an obligation on public authorities to protect people's Article 2 right to life and Article 3 right to be free from torture or degrading treatment. There needs to be a balance between the desire to share, with a person's rights under Article 8 to respect for private and family life, home and correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in the interests of national security, public safety or for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The Mental Capacity Act 2005. Under the Mental Capacity Act 2005 staff are required to apply 5 principles in their assessments to decide whether to share information without consent in a persons' best interests. As described in 2.4 of the MCA Code of Practice, "it is important to balance people's right to make a decision with their right to safety and protection when they can't make decisions to protect themselves. The starting assumption must always be that an individual has the capacity, until there is proof that they do not.

Under the Mental Capacity Act 2005 there would have to be good reasons for not undertaking an assessment of mental capacity regarding the decision to share information without consent, and these would need to be documented carefully.

Conditions for processing and exemptions under the Data Protection laws

There are specific circumstances when it may be lawful to disclose personal data about an individual without their consent. The GDPR and Data Protection Act 2018 recognise that in certain circumstances personal data may only be disclosed if one of the following conditions apply:

- for the purposes of a contract or steps taken to enter into such contract to which the individual is party;
- where required to protect the vital interests of the individual concerned or another individual; or
- Where necessary for the performance of a task carried out in the public interest or where a partner organisation is acting under official authority, this would include the exercise of any partner organisation's statutory function or exercise of government function;

[4] http://www.legislation.gov.uk/ukpga/1998/37/contents

In addition where the personal data consists of special categories of personal data one of the following conditions must also apply:

- where necessary for reasons of substantial public interest:
  - in the exercise of any partner organisation's statutory function or exercise of government function; or
  - where consent cannot be given or cannot reasonably practically be obtained:
    - for the provision of a confidential counselling, advice or support services;
    - for the purposes of the prevention or detection of an unlawful act; or
    - to protect members of the public against dishonesty, malpractice or other seriously improper conduct, or unfitness or incompetence;
- where required to protect the vital interests of the individual concerned or another individual where the relevant individual is physically or legally incapable of giving consent;
- by a health professional or a social work professional (or such other person who is subject to a legal duty of confidence) where necessary for health or social care purposes i.e. preventive or occupational medicine, the assessment of the working capacity of an employee, medical diagnosis, the provision of health care or treatment, the provision of social care, or the management of health care systems or services or social care systems or services; or
- by a health professional (or such other person who is subject to a legal duty of confidence) where necessary for reasons of public interest in the area of public health.

Please note that the disclosure and use of personal data will be still be subject to the data processing principles referred to in Appendix 3.

Provided the disclosure is for one of the circumstances mentioned above, there are certain exemptions for the party disclosing the data which apply in limited circumstances. To the extent that the Article 5(1) and 5(2) principles (set out in Appendix 3 for information) prevent disclosure, the exemptions dis-apply the need to meet the GDPR principles in respect of the information covered in the exemption.

The exemption disclosures include:

- disclosures required by law or in connection with legal proceedings;
- disclosures required for the prevention or detection of crime.

The decision to disclose under these circumstances must be documented and relevant i.e. details of the condition/exemption relied upon, who made the decision, who the information was disclosed to and the date. A decision not to share information must also be recorded.

Where person data is used in the substantial public interest, the partner organisation must have in place a policy document which explains the partner organisation's procedures for securing compliance with the data protection principles in connection with the processing of personal data, and explains the partner organisation's retention and erasure policies, giving an indication of how long such personal data is likely to be retained.

Where personal confidential data needs to be shared in order to fulfil statutory requirements, these requests will be considered and approved by the appropriate Caldicott Guardians or Senior Information Risk Owners (SIROs) of the partner organisations.

Staff should seek advice where necessary from their organisation's Data Protection Officer/Information Governance Manager and safeguarding lead(s) or team(s).

8. Implementation, Monitoring and Review

The Protocol has been developed in consultation with stakeholders within Nottinghamshire. The Protocol is owned by all of its signatories. The intention has been to develop an over-arching code of behaviour for all information sharing applications. This will be supplemented by agreements for specific purposes which will adopt the principles and commitments in the Protocol as their base line and identify any additional service specific requirements.

Work to develop individual agreements will be pursued through the partnership of Nottinghamshire organisations and stakeholders.

The Protocol will be reviewed annually and will be updated to account for any changes in legislation and developments in national guidance. Issues arising from data breaches of the Protocol, changes in legislation, or recommendations arising from review will be presented to the Nottinghamshire Records and Information Group (RIG) for initial consideration.

Each partner organisation will be individually responsible for monitoring and reviewing the implementation of the protocol and any individual Information Sharing Agreements they may have.

9. Sharing with organisations who are not signatories to this protocol

Any organisation who is not party to this overarching Protocol, but who wishes to share information may do so, providing that there is an existing Information Sharing Agreement in place with the third party, that they agree to comply with the terms of this overarching Protocol and have adequate technical and non-technical security arrangements in place, including compliance with the Information Governance Toolkit, which is considered best practice.

10. Personal Data Breach

All agencies who are party to this Protocol will have in place appropriate measures to investigate and deal with the inappropriate or unauthorised access to, or use of, personal data whether intentional or unintentional.

In the event that personal data shared under this Protocol is or may have been compromised, whether accidental or intentional, the organisation making the discovery will, without delay:

- inform the organisation who provided the data of the details;
- take steps to investigate the cause;

- take disciplinary action against the person(s) responsible, if appropriate;
- take appropriate steps to avoid a repetition;
- take appropriate steps, where possible, to mitigate any impacts.

On being notified of a breach, the original information provider along with the organisation responsible for the breach, and others as appropriate, will assess the potential implications for the individual whose information has been compromised, and if necessary will:

- notify the individual(s) concerned;
- advise the individual(s) of their rights; and
- provide the individual(s) with appropriate support.

Where a breach is identified as serious because of the possible impact it may have on individuals it should be reported to the Information Commissioner's Office within 72 hours of the relevant Partner organisation becoming aware of it. For organisations reporting breaches via the Information Governance Toolkit, breaches reported via the Toolkit will be shared with the ICO. The original information provider, along with the breaching organisation and others as appropriate, will assess the potential implications, identify and agree appropriate action.

11. Complaints

Partner organisations must have in place procedures to address complaints from members of the public relating to the inappropriate disclosure of information. The partner organisations agree to cooperate in any complaint investigation where they have information that is relevant to the investigation. Partners must also ensure that their complaints procedures are well publicised.

If the complaint affects more than one partner organisation it should be brought to the attention of the appropriate complaints officers who should liaise to investigate the complaint.

A complaint about one agency about another must be raised between the Caldicott Guardians of each organisation to resolve accordingly.

12. Protocol Signatories

The Information Sharing Protocol was originally agreed by the Nottinghamshire Records and Information Group.

The Partners below have agreed to abide by the terms of this Protocol, its schedules and any variations to the Protocol or its Schedules:

Appendix 1 - Caldicott Principle 7 'the duty to share information for direct care'

Sharing information for direct care- guidance for frontline staff

Health and social care information should be securely safeguarded and remain confidential, within the 'care team', at all times.

You can share information which is in the **best interests** of the patient or citizen **and** is for purposes of **direct care.**

Direct care is provided by health and social care staff working in multi-disciplinary 'care teams' which may include doctors, nurses and a wide range of staff on regulated registers, including social workers.

You can share information with staff who have a '**legitimate relationship'** with the patient or citizen which includes the staff member seeing the patient/citizen for purposes of direct care, the patient agreeing to a referral, the patient/citizen presents in an emergency situation where consent is not possible or the patient/citizen is told of proposed communication and does not object.

Sharing of relevant personal confidential data for direct care is done under 'implied **consent**', as long as the patient/citizen is informed, would not be surprised by the sharing and does not object. Implied consent still requires an 'affirmative action' on the part of the individuals, for example, if a patient/citizen agrees to a referral, it is reasonable to imply consent for sharing information relating to the referral with the third party.

You therefore **do not need written/signed consent** to share information for direct care with staff who have a legitimate relationship with the patient/citizen.

You should have the confidence to safely, securely and appropriately share information. In all cases there should be **no surprises** for the patient/citizen with regards to who their information has been shared with and it is advisable to discuss the sharing of information with the patient/citizen and document this in the patient record.

There is a **duty to share information** in the best interests of patients within the framework of the Caldicott principles which includes: justify the purpose, use of confidential data should be absolutely necessary, use/share the minimum, ensure access on a need to know basis, ensure everyone is aware of responsibilities (re confidentiality and security of data) and compliance with the law. This has been brought into legislation – Health & Social Care (Safety & Quality) Act 2015.

You can share information across health and social care with professionals who are part of the patients/citizens 'care team'. Sharing of relevant information is important in order to provide a seamless, integrated service.

The need to share information does not entail the sharing of everything, r**elevant, necessary and proportionate information should be shared** with professionals and or staff when they have a 'legitimate relationship' with the patient or citizen.

Relevant information is defined as information that may directly influence the decision over what care is given to a patient or citizen and how that care should be given.

Once information has been shared with a professional who has a ‘legitimate relationship’, the recipient then becomes responsible and accountable for that information in a professional capacity.

Appendix 2 - Legal Framework and Categories

The legal framework within which public sector data sharing takes place is complex and overlapping and there is no single source of law that regulates public sector information sharing.

The purpose here, therefore, is to highlight the legal framework that affects all types of personal information sharing, rather than serve as a definitive legal reference point.

The general legal framework surrounding the sharing of information includes:

- the law that governs the actions of public bodies (administrative law);
- the Human Rights Act 1998 and the European Convention on Human Rights;
- the common law duty of confidence;
- the EU General Data Protection Regulation 2016/679;
- the Data Protection Act 2018;
- the Freedom of Information Act 2000;
- No secrets, Department of Health 2000;
- Caldicott Principles; and
- legislation that covers specific aspects of public service delivery (e.g. child protection, patient records).
- Regulatory codes of practice and guidance (such as Information Commissioner's Office, Care Quality Commission, and Ofsted).

Overall the law strikes a balance between the rights of individuals and the interests of society. The law is not a barrier to sharing information where there is an overriding public interest in doing so (such as where it is necessary to do so to protect life or prevent crime or harm) provided it is done fairly and lawfully.

Often personal information can be shared simply by informing people from the outset what purposes their information will be used for and then sharing only for those agreed purposes. There are however special legal considerations around sharing information that is personally sensitive or is special category data, because this could have serious consequences for individuals. In deciding whether the law allows personal information to be shared, the following four steps should be considered (as recommended by the Ministry of Justice):

1. Establish whether there is a legal basis for sharing the information (i.e. whether the reason for sharing the information has a statutory basis – eg safeguarding for the purposes of the Children Act 1989) or whether there are any restrictions (statutory or otherwise) to sharing the information;

2. Decide whether the sharing of the information would interfere with human rights under the European Convention on Human Rights;

3. Decide whether the sharing of the information would breach any common law obligations of confidence;

4. Decide whether the sharing of the information would be in accordance with the GDPR, in particular the Data Protection Principles, which are that personal information must be:

- Processed lawfully, fairly and transparency
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Secure and
- the data controller shall be accountable for complying with these principles and being able to demonstrate such compliance.

Further detailed guidance on using personal and sensitive personal information fairly in accordance with the GDPR is set out in **Appendix 3.** In addition, the Freedom of Information Act 2000 gives anyone (an individual or an organisation) a right to request access to information from a public body. Where an exemption applies (e.g. it is third party personal information or commercially sensitive information), disclosure may be refused.

Appendix 3 – Data Protection Principles

Data protection and privacy legislation sets out standards which must be satisfied when obtaining, recording, holding, using or disposing of personal data. These are summarised by the Data Protection Principles. Under the key principles of the GDPR, personal data must be:

Lawfulness, fairness and transparency. Personal data must be processed lawfully, fairly and in a transparent manner. There should be no surprises – data subjects should be informed about why information about them is being collected, what it will be used for and who it may be shared and one of the conditions for processing must be met under Article 6 and, in the case of special categories of personal data, Article 9;

Purpose limitation. Only use personal information for the specified, explicit and legitimate purpose(s) for which it was obtained and ensure it is not processed in any other manner that would be incompatible with that purpose(s);

Data minimisation. Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Only collect and keep the information you require. It is not acceptable to collect information that you do not need. Do not collect information 'just in case it might be useful one day';

Accuracy. Personal data must be kept accurate and up to date. Have in place mechanisms for ensuring that information is accurate and up to date. Take care when inputting to ensure accuracy and have local procedures in place to manage requests for information to be erased or rectified without delay;

Storage limitation. Identifiable personal data should be kept for no longer than is necessary. The legislation within which area you are working in, will often state how long documents should be kept. Information should be disposed of in accordance to your organisation's Records Management Policy (including retention and disposal);

Integrity and Confidentiality. Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. This involves as appropriate:

- using pseudonymisation and encryption of personal data;
- ensuring the confidentiality of faxes by using Safe Haven faxes;
- keeping confidential papers locked away;
- ensuring confidential conversations cannot be overheard;
- ensuring information is transported securely;
- good information management practices;
- guidelines on IT security;
- procedure for access to personal data;
- a retention and disposal policy for confidential data
- adherence to approved codes of conduct under Article 40 of the GDPR.

In addition to the principles data must be processed in accordance with individuals' Data Subject rights

These rights include the right to:

- receive an information/privacy notice about the data processing;
- make subject access requests;
- rectify inaccurate personal data;
- erase certain personal data in certain circumstances such as where it is no longer required for the purposes it was obtained or consent has been withdrawn and there is no other legal justification for retaining the personal data;
- restrict processing in certain circumstances such as where the individual has objected to data processing whilst the outcome of the decision relating to the objection is pending;
- have the controller communicate any rectification or erasure or restriction of use of personal data to each recipient to whom personal data has been disclosed;
- data portability but only where processing is carried out by automated means and is based on consent or further to a contract to which the individual is party;
- object to processing of data for a public task unless there are legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims;
- object to direct marketing;
- Be informed about automated decision making processes authorised by law that significantly affect them and respond to any request for that decision to be reconsidered;
- Not to have decisions that affect them from being made solely by automated processes unless they consent, relates to a contact they are party to; or is authorised by law;
- Seek compensation if they suffer damage or distress through contravention of the Act;
- Request an assessment by the Information Commissioner of the legality of any processing that is occurring.

If sending information outside the European Economic Area (EEA), there must be a legal basis for the transfer, and personal information must be adequately protected through use of appropriate safeguards such as contracts incorporating standard data protection clauses adopted by the European Commission. Consider carefully what is posted on websites or sent via email. Where appropriate, obtain approval from the data controller.

Appendix 4 –Caldicott Principles

The Caldicott Review 2013 re-enforced the original principles of 1997 regarding the use of client information in health and social care organisations and added a 7th principle regarding the sharing of information.

- **Principle 1 - Justify the purpose(s)**

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed by an appropriate guardian.

- **Principle 2 – Do not use personal confidential data unless it is absolutely necessary**

Person confidential data items should not be included unless it is essential for the specified purpose (s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose (s).

- **Principle 3 -Use the minimum necessary personal confidential data**

Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

- **Principle 4 -Access to personal confidential data should be on a strict need to know basis**

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may been introducing access controls or splitting data flows where one data flow is used for several purposes.

- **Principle 5 -Everyone with access to personal confidential data should be aware of their responsibilities**

Action should be taken to ensure that those handling personal confidential data - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient/citizen confidentiality.

- **Principle 6 - Comply with the law**

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

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

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

Appendix 5 - Consent: Guidance notes

Consent under GDPR

Consent should only be relied on where there is no other legal basis for processing.

For consent to be valid, it must be:

- fully informed – the individual is aware of what information will be shared, with whom and for what purpose, and who controls the data (data controller);
- specific – a general consent to share information with 'partner organisations' would not be valid. Specific means that individuals are aware of what particular information we will share, who with and for what purpose;
- freely given – the individual is not acting under duress from any party.
- There is an unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
- the individual must have capacity to give consent
- able to be withdrawn. This may be time limited, for example, if an individual has given consent to use of their information in a research project, they cannot withdraw consent after the research has been published.

Individual organisations may have their own procedures for dealing with issues of implied/explicit consent in order to allow it to meet its lawful obligations. Staff should refer to organisational procedures.

Even if consent is being used as a lawful basis for processing (Article 7 GDPR), all processing must still be legal in accordance with Article 6 of GDPR, and, if special category information is being processed, Article 9 and other relevant law (for example, Privacy & Electronic Communications Regulations 2003 may apply to 'bulk' communications such as newsletters, particularly if they contain third party advertising).

To give valid informed consent, the person needs to understand why their information needs to be shared, what type of information may be involved, who that information may be shared with and the possible consequences if it is not shared (if relevant).

If there is no alternative that obtaining consent the person should also be advised of their rights with regard to their information namely:

- the right to withhold their consent
- the right to place restrictions on the use of their information
- the right to withdraw their consent at any time, and any limits to this (for example, publication of research that they have previously consented to be involved with).
- the right to have access to their records.

In general, once a person has given consent, that consent may remain valid for an indefinite duration unless the person subsequently withdraws that consent. However, it is best practice for practitioners to review this regularly.

If a person makes a voluntary and informed decision to refuse consent for their personal confidential data to be shared, this decision must be respected unless there are sound legal grounds for disclosing without consent. The consequences of not providing consent should be explained, e.g. such as not receiving the right treatment or service/amount of support.

If consent was one of the original legal bases for processing, new consent will be required where there are to be significant changes to:

- the personal data that will be shared,
- the purposes for which it will be shared, or
- the partners involved in the sharing (i.e. the proposed data sharing is not covered by the original information/privacy notice).

Capacity to consent

For a person to have capacity to consent, he/she must be able to comprehend and retain the information material to the decision and must be able to weigh this information in the decision making process. See guidance as defined in the Mental Capacity Act 2005.

Young Persons - Section 8 of the Family Law Reform Act entitles young people aged 16 or 17, having capacity, to give informed consent. The courts have held that young people (below the age of 16) who have sufficient understanding and intelligence to enable them to understand fully what is involved will also have capacity to consent. This is augmented by the Gillick Competency [5]test.

It should be seen as good practice to involve the parent(s) or guardian/representative of the young person in the consent process, unless this is against the wishes of the young person. In the case where the wishes of a young person, who is deemed competent to give consent, are opposed to those of their parent/carer, then the young person's wishes should take precedence.

Recording consent - all agencies should have in place a means by which an individual, or their guardian/representative, can record their explicit consent to personal data being disclosed and any limitations, if any, they wish to place on that disclosure.

The consent form should indicate the following:

- details of the agency and person obtaining consent;
- details to identify the person whose personal details may/will be shared;
- the purpose of sharing personal information;
- the organisation(s) with whom the personal information may/will be shared;

[5] See CQC guidance - http://www.cqc.org.uk/guidance-providers/gps/nigels-surgery-8-gillick-competency-fraser-guidelines

- the type of personal information that will be shared;
- details of any sensitive information that will be shared;
- any time limit on the use of the consent;
- any limits on disclosure of personal information, as specified by the individual;
- details of the person (guardian/representative) giving consent if appropriate.

The individual or their guardian/representative, having signed the consent, should be given a copy for their retention. The consent form should be securely retained on the individual's record and relevant information should be recorded on any electronic systems used, in order to ensure that other members of staff are made aware of the consent and any limitations.

Disclosure without consent

Disclosure of personal information without consent must be justifiable on statutory grounds, or meet the relevant conditions for processing under the GDPR. Without such justification, both the agency and the member of staff expose themselves to the risk of prosecution and liability.

There are exceptional circumstances in which a patient's right to confidentiality may be overridden, for example:

- if an individual is believed to be at serious risk of harm, or
- if there is evidence of serious public harm or risk of harm to others, or
- if there is evidence of a serious health risk to an individual, or
- if the non-disclosure would significantly prejudice the prevention, detection or prosecution of a crime, or
- if instructed to do so by a court.

In deciding whether or not disclosure of information given in confidence is justified it is necessary to weigh the harm that would result from breach of confidence against the harm that might result if you fail to disclose the information.

Legislation which permits the sharing of data without consent includes (and is not limited to):

- NHS (Venereal Diseases) Regulations 1974
- Notifications of Births and Deaths Regulations 1982
- Codes of Practice, Mental Health Act 1983, s 1.3 – 1.13 and s 14
- Police and Criminal Evidence Act 1984
- Public Health Act 1984,Public Health (Infectious Diseases) Regulations 1998 and the Health Protection (Notification) Regulations 2010
- Children Act 1989 s 47
- Children Act 2004
- Controlled Drugs (Supervision of Management and Use) Regulations 2013
- Abortion Regulations 1991
- Finance Act 1994
- VAT Act 1994, s 91

- Criminal Procedure Investigation Act 1996
- Social Security Administration (Fraud) Act 1997
- Audit Commission Act 1998
- Crime and Disorder Act 1998, s 115
- GDPR, Articles 6 and 9;
- Data Protection Act 2018
- Human Rights Act 1998
- Mental Capacity Act 2005
- Terrorism Act 2000 s 19
- Civil Contingencies Act 2004
- Care Act 2014
- Fire and Rescue Service Act 2004

All agencies should designate a person(s) who has the knowledge and authority to take responsibility for making decisions on disclosure without consent. This person(s) should hold sufficient seniority within the organisation with influence on policies and procedures. Within the health and social care agencies it expected that this person will be the Caldicott Guardian.

If information is disclosed without consent, then full details will be recorded about the information disclosed, the reasons why the decision to disclose was taken, the person who authorised the disclosure and the person(s) to whom it was disclosed.

A record of the disclosure will be made in the patient's record and the patient/citizen must be informed if they have the capacity to understand, or if they do not have the capacity then any person acting on their behalf must be informed.

If information is disclosed without consent, there may be some exceptional circumstances (particularly in the context of police investigations or child or adult protection work) where it may not be appropriate to inform the patient/citizen of the disclosure of information.

This situation could arise where the safety of a child (or possibly sometimes of an adult) would be jeopardized by informing the patient/citizen of such disclosure. In many such situations it will not be a case of never informing the patient, but rather delaying informing them until further enquiries have been made. Any decision not to inform, or to delay informing, should be recorded on the patient's record, clearly stating the reasons for the decision, and the person making that decision.

Appendix 6 - Staff responsibilities and accountabilities for accessing another organisations information or clinical/care information system(s)

The below outlines best practice requirements for accessing a clinical information system within a different organisation. The authority for granting access remains with the 'data controller' of the system and this must still be managed in accordance with internal policies and procedures. **For clarity signing this information sharing protocol does not permit or provide authority for accessing other signatory organisations clinical or other information system.**

The purpose of this guidance is to set out clearly the responsibility and accountability of the staff accessing different organisations information (by middleware) or systems by approved access and log in. In order to facilitate quality and safe care, it is necessary for clinical colleagues to be able to view elements of a patient's record held in different systems by a variety of care organisations.

The guidance below supplements the principles set out in the Nottinghamshire Information Sharing Protocol and has been developed to ensure patient/citizen confidentiality and security of data; maintaining the trust of patients/citizens that data is being accessed appropriately and legitimately in whatever care setting.

Organisational signatories to the Nottinghamshire Information Sharing Protocol should ensure the below is incorporated within internal policies, procedures and where appropriate staff contracts or confidentiality agreements.

Before accessing another organisations held patient/citizen information (by middleware or approved remote login) staff must ensure:

1. They have a 'legitimate' relationship with the patient/citizen (seeing them for purposes of providing direct care);

2. Where necessary obtain consent from the patient/citizen to view the available information. Access to patient/citizen information via middleware may, for example, only be permitted if the patient/citizen consents and all users are required to indicate that the patient/citizen has consented before accessing any personal confidential data, usually a consent box will appear in such circumstances. Best practice is always to discuss with the patient/citizen what information is being accessed and why.

3. Access is via a secure and approved connection, paying particular attention to surroundings and any impact this could have on breaching confidentiality. Access is facilitated by using approved organisation owned equipment in accordance with policy.

4. Where access to data is expedited in exceptional circumstances without explicit patient/citizen consent (where this is required see point 2 above) this is done using

clinical judgement to access data via an 'emergency override function' and the rationale should be documented accordingly in the patient/citizen record.

5. They have undertaken and are up to date with Information Governance training and are aware of and following their organisations Information Governance policies and procedures which include data protection and confidentiality, information security, remote working, internet and e-mail use, network security, smart card use/password management, secure transfer of data/safe haven, records management and data quality.

6. They are aware of their responsibilities to comply with the law particularly the GDPR, common law duty of confidence and the Human Rights Act 1998.

7. Data sharing and access to any patient/citizen information must be in line with the 7 Caldicott principles and only the minimum and necessary amounts of patient/citizen personal confidential data is accessed or shared for purposes of providing direct healthcare in the best interests of patients/citizens. You must also use clinical and professional judgement about which parts of a patients/citizens record should be viewed as just because you have the potential to access a full record does not mean this is appropriate in provision of the aspect of care you are providing. Caldicott principle 7 provides that relevant information should be accessed and shared for direct care with the care team where it is in the patients/citizens best interests.

8. The patients/citizens must be provided with sufficient information about who can access their information (via privacy notices)

After accessing another organisation held patient/citizen information:

1. Provide justification (if requested to do so by the 'data controller' of the information) why access to a particular record was made. Understand that inappropriate or illegitimate access could result in a disciplinary matter.
2. Understand that any inappropriate or non-justified access will be logged and managed as a data breach which could involve serious consequences for the organisation and detrimentally impact on the patient/citizen.
3. Not make the information available to any third parties (outside the direct care relationship) without seeking consent from the 'data controller'. This includes receiving a subject access request from the patient/citizen or their representative.
4. Not use the information for purposes other than providing direct care to the patient/citizen without seeking consent from the 'data controller'. For clarity: information for any other use than direct care of the individual involved must not be extracted from another organisation's records without agreement of the 'owner' organisation, and where required, from the patient/citizen(s) concerned..
5. Ensure that they comply with the duty to update the patients/citizens GP (where appropriate) or other care professional if the system being accessed does not allow you to do this and where an update is paramount for the continuity of care. This is also important to support working in a multi-disciplinary and multi-professional way.

6. Any data quality or accuracy issues are reported to the GP or other professional, particularly where this presents a patient/citizen safety/clinical risk.
7. Ensure they comply with the duty to share information appropriately for safeguarding and this should be underpinned by clear guidance and training.
8. Ensure compliance with Professional Codes of Practice.
9. In the event of an Information Governance incident or identified inappropriate/illegitimate access to data inform the organisation responsible for employing the individual so they can instigate an investigation. The 'data controller' of the record which has been accessed inappropriately must also be informed as part of the investigation.

Appendix 7 – References

- Data Sharing Code of Practice – Information Commissioners Office http://ico.org.uk/for_organisations/data_protection/topic_guides/data_sharing
- Guide to Confidentiality; Health and Social Care Information Centre 2013 http://www.hscic.gov.uk/confguideorg
- The Caldicott Review 2013 https://www.gov.uk/government/publications/the-information-governance-review
- General Data Protection Regulation 2016
- Data Protection Act 2018
- Common Law Duty of Confidentiality
- Human Rights Act 1998
- Freedom of Information Act 2000
- Environmental Information Regulations 2004

Appendix 8 – Data Protection Impact Assessment

A Data Protection Impact Assessment (DPIAs) must be undertaken when there are any significant changes to proposed processing of data, for example, in relation to a new service, or a new arrangement for one organisation to directly access the records system of another organisation. Project managers are responsible for undertaking DPIAs, seeking advice from Information Governance, Data Protection Officer, Caldicott Guardian, Senior Information Risk Owner as required, and, ultimately, approval from one or all of these, as indicated by the project. See local processes in your organisation, and, if necessary, seek advice from local Information Governance experts or the Data Protection Officer.

As a general guide:

DPIAs focus on information (not 'whole project') risks and benefits of processing personal information. In summary, they should describe:

- Whose data are being processed and who is involved with processing
- What detail is being processed (data fields)
- The rationale for the processing "why it's needed" – including the legal basis. If consent is not being used, then the legal basis under GDPR may require additional support from other relevant legislation.
- Information security and records management arrangements (including retention and eventual disposal)
- Controls and assurance – for example, confirmation of organisations' accreditation with ISO27001 Information Security standard.
- Any risks associated with processing, and how these will be mitigated (for example, pseudonymisation, aggregation of age groups, etc.)
- Benefits and risks of processing should prioritise the individuals concerned, followed by the benefits and risks to future patients/citizens in the service(s), organisations and/or the 'public good'.

Examples of when you will need to consider DPIA:

A community health provider, local authority and charity want to start a partnership to deliver a healthy eating programme.

A commissioner wants to evaluate outcomes of a new service and commission an external partner to undertake this with the service provider.

A GP practice wants its staff to use a messaging app to improve efficiency.

A health professional wants their organisation to sponsor and agree set up of a social media group to support parents of children with a specific health condition.

A large acute provider is procuring a new patient administration system.

Essentially, a DPIA must be undertaken for any project or initiative that involves new or changed processing of any personal data.

The DPIA may be very short. The first question in any DPIA is “Does this project include new or changed use of personal data?” If the answer is ‘No’, then this question should be documented as evidence of consideration of potential data protection and/or privacy issues, and the DPIA is complete.

Appendix 9 – What should be in an Information Sharing Agreement

Ensure that you follow your organisation's local policy and processes in relation to Information Sharing Agreements. In general, contents should be, at minimum:

- Parties to the agreement – organisations with full contact details and named responsible person. If one or more contracts are associated with the sharing agreement these should also be referenced.
- Roles of each party – providing or receiving data? What authority do they have over the data/what decisions will they be making? – this will help to inform whether each organisation is a data controller or data processor.
- Organisation accreditations (such as ISO27001, confirmation of registration with Information Commissioner's Office, etc.)
- Specific purpose(s) for which the data sharing is required (all intended purposes should be described, it may be appropriate to describe each one on a separate pro forma as a 'schedule' to the agreement)
- Description of the data shared (this may need to be attached as a list of data fields) – include any anonymisation/pseudonymisation arrangements and frequency of transfers
- Legal basis for sharing (which may be consent or other)
- If consent, how is this recorded and managed (for example, if someone withdraws consent)
- How individuals will be informed about the processing
- How requests for subject access will be dealt with (for example, in a shared service, it may be appropriate for the service receiving the request to provide all data, in consultation with other organisations, which improves the patient/citizen experience)
- Information security arrangements – how data will be stored and communicated
- Controls and assurance as relevant and required for the project:
  - Staff roles and qualifications/training
  - Incident reporting
  - Monitoring and audit of the arrangements
- General governance arrangements – for example, if one participating organisation is replaced by another as services are re-procured
- Retention and disposal/destruction arrangements
- Date of end of the agreement, or, if ongoing, review date
- Authorisation: seniority for authorisation dependent on the project, in accordance with organisations'' local processes.

In general, if a contract is in place, then all this information should be contained within the contract: a separate agreement should not be required.

Appendix 10 – Legal Bases

Key points:

- GDPR requires a legal basis for processing personal data. Consent is only one of these. Public authorities, particularly, may be legally obliged to undertake personal data processing by various other legislation. Primary question: Would the person whose data is being processed expect us to be processing in this way? – think 'No surprises' and inform.
- Whilst GDPR provides many more conditions for processing than the Data Protection Act 1998, it is less prescriptive as to how those conditions are met.
- Organisation boundaries in a health and care pathway should not create a barrier to care. Apply Caldicott 'Minimum Necessary' principle.
- National and regional systems for shared care records and recording consent for non-care use of data (research, national audit, etc.) are under development.
- Unless there is a risk of harm to the patient or third party, always inform, even if consent is not the legal basis for processing. Provide choice where possible.
- Data Protection Impact Assessments provide the evidence for compliance with data protection principles and ethical use of information with respect to individuals' privacy.
- GDPR is grounded in "reasonableness" – document rationales and decision-making processes as applicable to circumstances.

The below covers many processing scenarios; it is not comprehensive or intended to be exclusive of others.

Legal basis: patients

GDPR[6] Articles 6 (lawfulness of processing any personal data) and 9 (lawfulness of processing sensitive personal data): particularly

6(1)(c) necessary for legal obligations

6(1)(e) public interest or public duty

6(3) the above supported by Member State law (*UK legislation as applicable to circumstances*)

9(2)(c) processing for 'vital interests' (safety, safeguarding, public safety, etc.)

9(2)(h) allows processing for the provision of healthcare (direct care) or the management of healthcare systems (invoice validation, commissioner reporting, quality audits – essentially, mandated activity).

[6] https://gdpr-info.eu/ provides an easily navigable unofficial version of GDPR (no endorsement of provider implied/intended). Articles are the law itself; recitals provide context, rationale and clarification and may be relied upon by courts in decision making.

9(2)(i) allows processing for “ensuring high standards of quality and safety of health care.” – which would cover research, audit, service improvement and addressing public health/inequalities.

9(2)(j) (together with Article 89 and relevant recitals) relates to archiving, statistical analysis and research.

Consent, OR other relevant legislation gives “the rest” of the legal basis for processing:

- Health and safety, patient safety, safeguarding and public health: as applicable to circumstances. Examples: various Children Acts (‘s47’ is in the 1989 Children Act); Mental Capacity Act 2005 (and associated Deprivation of Liberty Safeguards) and many others – CQC has a useful list here: http://www.cqc.org.uk/guidance-providers/regulations-enforcement/regulations-service-providers-managers-relevant.
- Health & Social Care (Safety & Quality) Act 2015 s3 brings the Caldicott ‘Duty to share for care’ (Principle 7) into law. Providers are required to share information in the best interests of patients and this legislation makes that explicit. Patients who decide to opt out must have potential consequences on the quality of their care fully explained to them.
- Health & Social Care Act (2012). Various parts of this legislation directly apply to some organisations (local authorities re: public health, CCGs). Bizarrely, there is no reference to many provider organisations: I think it's fair to infer that SoS would expect us to undertake service improvement activities on his behalf as he's an awfully busy man: Part 1, section 2 places a duty on the Secretary of State for Health improve quality of services etc.
- Health and Social Care Act 2008 (Regulated Activities) Regulations 2014 do not only give the CQC powers. Regulation 2 requires providers to “assess, monitor and improve the quality and safety of the services provided in the carrying on of the regulated activity (including the quality of the experience of service users in receiving those services)” (r2(a)).
- GDPR (6)(1)(e) – public interest or public duty may be appropriate, with a fully explained rationale for the processing, for example, service evaluation for improvement, etc. This is in line with normal ‘making a case’ practice (business case, audit protocol, other rationale for use of resources documentation).

Remember: even where consent is not sought, patients must be informed appropriately about processing, particularly ‘non-care’ use and should be given choice where possible, in line with current practice and the common law duty of confidentiality. See Data Protection Impact Assessment, below, and additional information about research at the Health Research Authority’s website[7]. Although overall governance differs, principles of data protection and confidentiality are similar for research and audit.

Legal basis: staff

[7] https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/

GDPR Articles 6 (lawfulness of processing any personal data) and 9 (lawfulness of processing sensitive personal data): particularly

6(1)(c) necessary for legal obligations

6(3) the above supported by Member State law

9(2)(b) employment provisions (see also Article 88)

9(2)(c) processing for 'vital interests' (safety, safeguarding, public safety, etc.)

9(2)(h) occupational health provisions

Consent, OR other relevant legislation give "the rest" of the legal basis for processing:

- Employment and employment-related law: as applicable to circumstances, including occupational health, pensions, provision of IT services and equipment, health and safety, etc.
- Obligations in relation to provision of health services (examples: incident reporting and investigation, staff names in patient/citizen records)
- Obligations in relation to registered professions as provided by registration bodies, or other legislation (examples: Duty of Candour, transparency obligations in relation to declarations of interest, freedom of information)
- GDPR (6)(1)(e) – public interest or public duty may be appropriate, with a fully explained rationale for the processing, for example, service evaluation for improvement, etc. This is in line with normal 'making a case' practice (business case, audit protocol, other rationale for use of resources documentation).

Staff should be appropriately informed about processing of their personal data through recruitment information, contracts of employment and policies, handbooks, etc.

Legal basis: others

Primarily applicable to Trust membership, patient engagement and charitable activities.

GDPR lawful basis likely to be:

6(1)(c) necessary for legal obligations

6(3) the above supported by Member State law

Consent, in accordance with Article 7 (demonstrable, fully informed, freely given, can be withdrawn)

Other relevant legislation or 'rules' should be provided where appropriate:

- Legal obligations in relation to public interest, safeguarding and (where applicable) from Monitor, charity and company law as applicable to circumstances.

Special circumstances: complaints, freedom to speak up ('whistleblowing')

The GDPR focus on individuals' rights actually makes it less restrictive than current legislation in many respects. There is no substantive change to principles of processing personal data for complaints or in relation to raising concerns internally.

There is no 'one size' for all situations. Document and explain decision making processes, seeking advice from DPO, SIRO and Caldicott Guardian where required.

GDPR: particularly -

6(1)(c) necessary for legal obligations – as supported by relevant law, codes of practice and regulatory requirements

9(2)(c) processing for 'vital interests' (safety, safeguarding, public safety, etc.)

Article 90 – professional secrecy – may apply in some circumstances

Other relevant legislation or 'rules' should be provided where appropriate (duty of candour, etc.)

Acting on third party information: if there are patient safety allegations or implications then investigation is covered under the 'vital interests'.

Disclosure of information to third parties where no consent is in place: guidance on disclosing third party information in relation to a subject access request may be useful[8]. In summary, consider what the third party may already legitimately know. For example, if a clinician is aware that a family member has been present at discussions with clinicians about the patient's care, then disclosure in line with 'what they already know' may be appropriate as no breach of privacy will occur.

Under GDPR, more consideration of Gillick competency may be necessary in relation to children's' rights over their information, for example, competent children wishing to restrict parental access to all or part of their records.

Data Protection Impact Assessments and Privacy by Design

The European Convention of Human Rights Article 8[9] Right to a private and family life is qualified by the rights and freedoms of others – including organisations who are required to process personal information, or who have a legitimate purpose for doing so.

Privacy by Design and Data Protection Impact Assessment (DPIA) simply give personal information the same importance in business cases and planning as finance, human resources and capital and physical assets. All too often, Information Governance ends up being a barrier because data protection and privacy considerations have not been built in

[8] https://ico.org.uk/media/for-organisations/documents/2014223/subject-access-code-of-practice.pdf - Subject Access Code of Practice, p15 and p36-8

[9] Implemented into UK law by the Human Rights Act 1998.

from the design of a project. It is important that DPIA is seen as a process, rather than 'filling in a template', although certain information is always needed:

- whose data?
- what data, and what are we doing with it?
- why (benefits and risks)?
- how (processes, data security)?
- where (which organisations, more data security)?
- when (frequency of processing – one off, regular? and retention)?

A DPIA can be as short as: "Does this project/change include processing personal data?" – No.

For those familiar with research ethics concepts, DPIAs can be thought of as 'research protocols for not-research projects'.

DPIAs for business change projects or procurement can be useful to identify efficiencies as well as to support compliance.