MULTI-AGENCY INFORMATION SHARING PROTOCOL

NORTH EAST & NORTH CUMBRIA REGION

Version: 13.0	
Created: *May 2006*	**Last Updated:** *April 2025*

Author: Protocol Review Group
Approved by: Protocol Signatories
Audience: All signatory organisations

Contents **Page**

Version Control

Version Number	Date	Status
1.0	May 2006	Approved
2.0	March 2008	Approved
3.0	Oct 11	Draft
4.0	Jan 12	Draft
5.0	Feb 12	Draft
6.0	Feb 13	Draft
7.0	March 13	Approved
8.0	Jan 15	Approved
8.1	Aug 15	Approved
8.2	April 17	Draft
8.3	May 17	Draft
9.0	June 17	Approved
9.1	October 17	Draft
9.2	February 18	Draft
9.3	October 18	Draft
10.0	October 18	Approved
10.1	October 19	Decision made by all members at NE SIGN Meeting 23/09/2019 that current version will be extended for the period of one year and all existing signatories will remain valid List of signatories is held by CDDFT DSP Team in the following location G:\itservices\ig\shared\Information Sharing\High level protocols – Tier 1 & 2\Tier 1\Multi Agency IS Protocol\MA ISP extended to Nov 20
10.2	November 21	Draft
11.0	January 2022	Approved NENC SIGN 17/01/2022
11.1	March 2022	Updated Durham Constabulary Form
12.0	March 2024	Updated Police form and updated names and contacts. Various updates from NENC SIGN received.
12.1	April 2024	Additional updates prior to approval
13.0	April 2025	Full review and updated Appendix ISA template

1. Introduction

1.1. The North East and North Cumbria (NENC) Overarching Multi-Agency Information Sharing Protocol (the Protocol) has been developed to ensure that information is being shared lawfully, appropriately, and in compliance with best practice.

1.2. The Protocol aims to establish consistent principles and practices to govern sharing of personal and non-personal information taking place between Partner Agencies.

1.3. The Protocol is to facilitate information sharing between Signatories whilst ensuring that personal data is safeguarded and confidentiality maintained.

1.4. This is an overarching Protocol designed to provide a framework for all operating procedures and practices regarding information sharing

1.5. Each Signatory has their own procedures for information sharing and maintaining confidentiality and it is important to note that the Protocol does not supersede these; it is an inter-agency framework highlighting common issues of good practice.

1.6. The ethos of the Protocol is for Partner Agencies to share information in all situations to improve service delivery and resident outcomes and to support safeguarding, except where it would be unlawful to do so. It is recognised that refusing to disclosing data can be a risk just as much as disclosing too much data.

1.7. A list of signatories to the Protocol can be found at Appendix A.

1.8. An Information Sharing Agreement is best practice and is not a legal document, most data processing transfers will be included within Data Protection Impact Assessments, specific contracts and or Data Protection Agreements / Protocols.

1.9. When creating or approving an Information Sharing Agreement, the template form in appendix E can be appended to the Information Sharing Gateway if used and or required.

2. Objectives of the Protocol

Partner Agencies and their employees need to feel confident of their obligations when requested, or requesting, to share information. This Protocol aims to ensure compliance and consistency across the region by achieving the following objectives:

- To agree standards that each organisation will follow, govern working practices and create greater transparency, data security and improved services for users;
- By offering guidance on how to share information lawfully;
- Increasing understanding of Data Sharing principles and legislation;
- Developing a Partner Agency Information Sharing Agreement template (see Appendix E) to make it easier and quicker to formalise local information sharing activities, ensuring risks are managed and providing assurance for staff and

service users, whilst ensuring compliance with the overarching Protocol;
- To protect Partner Organisations from allegations of wrongful use of data;
- To monitor and review information flows.

3. Signatory Responsibilities

It will be the responsibility of the signatories to commit to:

- They are registered with the Information Commissioners Office in accordance; with current Data Protection Legislation

- Apply the standards that are prescribed in guidance and Codes of Practice issued by the Information Commissioner's Office and **https://ico.org.uk/for-organisations/**

- Comply with the provisions of Data Protection legislation which includes, but not limited to:
    - The UK General Data Protection Regulation (UKGDPR)
    - Data Protection Act 2018 (DPA)
    - Privacy and Electronic Communications Regulations (PECR)
    - Computer Misuse Act 1990
    - Digital Economy Act 2017 (DEA)
    - Human Rights Act 1998
    - Common Law Duty of Confidence
    - Health and Social Care Act 2012

Please note this list is not exhaustive and, accordingly, each Signatory has a duty to refer to appropriate legislation when making decisions regarding information sharing:

- Develop Partner Agency Information Sharing Agreements that comply with the Protocol and clearly and transparently demonstrate the reasons for sharing data and provide assurance on this activity. Appendix E – template agreement

- All organisations that are signatories to the Protocol are expected to have a Data Protection Officer. If a Partner Organisation is not required to have a Data Protection Officer, by statute, then they are expected to have a designated information governance lead. Data Protection Officers or Designated Leads are listed in Appendix A of this Protocol.

- Ethical standards must be maintained;

- All organisations must ensure any data processors are under contract and on approval of the appropriate agency.

- All Partner Organisations agree to be responsible for ensuring measures are in place to guarantee the security and integrity of data and that staff are sufficiently trained to understand their responsibilities and comply with the law. This document

encourages sharing of data, but does not alter the statutory duties of those organisations signed up to it.

- Appropriate arrangements exist to monitor the adherence to this protocol. This document shall be reviewed every two years unless significant new legislation or guidance from central government makes it necessary to have an earlier review.

4. Requirements for Information Exchange

4.1. Routine Information Sharing Agreement

Partner Organisations will use the Information Sharing Agreement template in Appendix E of this protocol. Alternatively, partner organisations may wish to use the Information Sharing Gateway, which is an online information sharing tool.[1]

Whilst the template Information Sharing Agreement is primarily intended for Information Sharing Agreements between Partner organisations, it may be used by Partner organisations to demonstrate arrangements with organisations who are not signatories to the Protocol.

Partner Organisations are responsible for maintaining, reviewing, and storing any completed agreements that they enter in to.

Partner organisations will also work towards routinely publishing agreements so that information sharing arrangements are sufficiently transparent.

Within the NENC region the use of the Information Sharing Gateway (ISG) for those partners who have licenses, is recommended for the management of an agreement and automated signatures.

4.2. Ad-Hoc Information Sharing Arrangements

Partner organisations recognise that sometimes information will have to be transmitted from one organisation to another without an Information Sharing Agreement being in place. This could be because the transmission of data is required urgently and/or because the disclosure is to comply with a specific legal requirement.

Ad-Hoc transmissions should be appropriately recorded and authorised according to each Agencies' own Data Protection policies. At the very minimum the record should indicate:

- the purpose of disclosure,
- the lawful basis for disclosure,
- why non-disclosure would prejudice the stated purpose,

[1] The information sharing gateway is an online framework to support information sharing across a number of organisations. It is hosted and provided by Lancashire and Cumbria Information Governance Group and is available via. paid licences.

- any other restrictions on use of the data.

Where disclosure takes place without the proper record being established, for example when an emergency occurs, then a retrospective record must be created and retained for audit purposes usually within the patient record or emergency preparedness, resilience and response.

4.3. Power to Disclose

Signatories must ensure that they have an express obligation, express power or implied power to share information with third parties or within their organisation prior to sharing information.

Signatories must also ensure that there are no statutory prohibitions on disclosure.

4.4. Data Processing

4.4.1. Any disclosure of personal data must have regard to both common and statute law, for example: defamation, the common law duty of confidence, the principles of the Data Protection legislation, the Human Rights Act 1998 and the Freedom of Information Act 2000, to ensure that confidential information should be exchanged, as defined within operating procedures, of each agency.

4.4.2. In addition, all Signatories will make available privacy notices in accordance with the UKGDPR.

Partner organisations are required to process personal data to ensure they have a valid condition for processing under the relevant legislation.

4.5. Criminal Offence Data Disclosures

When requesting Criminal Offence Data, Partner Organisations will ensure that they use the Criminal Offence Data Disclosure Form in Appendix D of this Protocol. [2] Appendix D is written with the intention of disclosing Criminal Offence Data under Schedule 2(2) of the Data Protection Act 2018.

The requesting authority must ensure that Appendix D form includes:

- the purpose of disclosure,
- an explanation as to how disclosure meets the requirements of Schedule 2(2) and Schedule 2(3),
- why non-disclosure would prejudice the stated purpose,
- a Counter Signature from an appropriately senior officer.

[2] The Protocol recognises and adopts the ICO's definition of 'Criminal Offence Data' as being personal data relating to criminal allegations, proceedings, convictions, or related security measures : *Guide to the General Data Protection Regulation,* Information Commissioner's Office (August 2018)

The receiving authority should take care to ensure the above criteria have been submitted prior to the disclosure of Criminal Offence Data. The receiving authority should have a procedure in place to ensure such requests can be processed efficiently but securely.

Partner Organisations should take care to ensure that requests for data relating to the abuse of children or vulnerable adults should follow the separate protocols that are in place across the region.

4.6. Restrictions

Partner organisations should ensure that they only use the information, that they have received, as a consequence of an Information Sharing Agreement, for the purposes stipulated in the agreement. Contravention of this may result in the termination of an arrangement. This does not apply if Partner organisations are required to process the data if compelled by a statutory obligation (i.e. Court Order).

Where a Partner organisation receives a request for information, which could involve the disclosure of information that originated from a Partner organisation, then the originating organisation should be consulted prior to disclosure. It should be noted that the decision to disclose rests with the receiving organisation and that the originating organisation does not have an automatic veto. [3] The deciding authority must take another organisation's concerns seriously and if disclosure takes place against the wishes of that organisation then a sufficient explanation / justification must be provided to that organisation.

Further restrictions on information disclosures may be imposed as part of an Information Sharing Agreement. Restrictions should not impede an agency's ability to comply with legislation.

Signatories will ensure that any restriction of rights is proportionate to the purpose for which the information is shared. In assessing proportionality Signatories will consider the impact on the data subject against the wider benefits of sharing the information.

4.7. Confidentiality

4.7.1. Before sharing information, Signatories will consider whether a duty of confidence is owed to the data subject or any other person.

4.7.2. If a duty of confidence does exist, Signatories will consider whether disclosure is lawful.

- Consent – confidentiality cannot be breached in circumstances where the person to whom the duty of confidence is owed consents to disclosure
- Public interest – there is a general public interest is preserving

[3] An information request could be, but not necessarily limited to, a Freedom of Information Request, Environmental Information request, or Subject Access Request.

confidentiality, however, the law recognises that there may be instances where there is a countervailing public interest in disclosure

- The reason the information came into existence – if information was brought into existence for a particular purpose, it is generally accepted that the information can be disclosed for that purpose
- Court order or legal obligation – if there is a court order for disclosure or the disclosure is in pursuance of a legal obligation then you should satisfy yourself that any disclosure sought is required by law or can be justified in the public interest. (Confidentiality is not to be considered separately)

4.8. De-identified, Pseudonymised and Anonymised Data

4.8.1. Where the purpose can be achieved using pseudonymised data, the key for re identification is not shared.

4.8.2. Signatories will consider whether any intended aims can be achieved using depersonalised, pseudonymised or anonymised data. Where data is required for performance management or reporting purposes, depersonalised, pseudonymised or anonymised data will be shared unless there is a justifiable reason for sharing personal data.

4.8.3. Signatories recognise that sharing multiple sets of de-personalised, pseudonymised or anonymised data may, if combined, result in identifiable data.

4.8.4. If there is any doubt regarding the sharing of de-personalised, pseudonymised or anonymised data the advice of the relevant Designated Officer must be sought.

4.8.5. The identity of the data controller is recorded against any data that has been provided by third parties. Signatories will not allow secondary use of the data without the express consent of the data controller. Please refer to the ICO's Anonymisation Code of Practice.

4.8.6. Where de-identified, pseudonymised and anonymised data is shared signatories will commit to not attempting to re-identify the data and are aware that to do so must be completed in accordance with the legislation.

4.9. Multi-Disciplinary Teams

4.9.1. Where Signatories are working in integrated multi-agency teams, Tier 3 agreements (as appropriate and in accordance with local arrangements) will be developed to set out a framework for sharing information.

Appendix E contains a template for the preparation of these service level protocols.

4.10.Rectification of Data that has been shared

4.10.1. Should any factually inaccurate information have been shared with other organisations then the responsibility lies with the organisation identifying the inaccuracy to notify the source organisation who must then follow procedure as outlined in Appendix G.

5. Security

5.1. Security

5.1.1. Each Partner organisation is expected to have adequate security measures in place to protect information that they have received via an Information Sharing Agreement and in accordance with relevant data protection legislation.

5.1.2. Partner organisations should ensure that an adequate and secure transmission method should be utilised and agreed upon as part of an Information Sharing Agreement.

5.1.3. Partner organisations are expected to include standards of good practice, such as recognised Information Security Standards such as ISO: 27001, Cyber Essentials plus, Data Security and Protection Toolkit. Partner organisations should be able to produce an Information Security Assurance statement upon request.

5.1.4. Employees at Partner organisations will be fully trained on how to handle and process personal data, special category data, criminal conviction data, and any other information that attracts a level of sensitivity.

5.1.5. Partner organisations may wish to insist on further Information Security controls as part of individual Information Sharing Agreements.

5.1.6. All Personal Confidential Data transmitted electronically must be encrypted to the satisfactory standard.

5.2. Retention and Destruction

5.2.1. Signatories will comply with the relevant Data Protection legislation and relevant government standards / best practice. To this end, Signatories will ensure that Information Sharing Agreements contain arrangements for the retention and destruction or return of information.

5.3. Caldicott Guardians and Designated Officers

5.3.1. All NHS and Social Care organisations have a Caldicott Guardian to oversee access to patient/service user information. The Caldicott Guardian is responsible for agreeing and reviewing protocols governing the disclosure of patient/service user identifiable information across organisational boundaries.

5.3.2. Other agencies have Designated Officer who are responsible for carrying

out a similar role, this may include Senior Information Risk Owners (SIRO's).

5.3.3. The contact details of Caldicott Guardians and Designated Officers are provided in Appendix H – Signatories List.

5.4. Issues and/or Non-Compliance in relation to the Application to this Protocol

5.4.1. In the first instance issues will be directed to the contact person in Appendix D.

5.4.2. Issues and or non-compliance in relation to the protocol regarding processing of personal data will be referred to the data controller, and will be investigated in accordance with the data protection legislation, regulation and relevant organisational procedures.

5.4.3. Responsibility for dealing with persistent non-compliance with the Protocol lies with the Chief Executive or signatory for the relevant organisation.

5.5. Refusal to share

5.5.1. Signatories will record any refusal to share information and will include the reasons for that decision. Specific Information Sharing Agreements will define procedures for a senior member of staff within the organisation to review information sharing decisions. Where necessary this may involve liaison with the Signatory's Designated Officer.

6. Monitoring and Review

6.1. Policy Management

Representatives from organisations meet bi-monthly to discuss the latest Information Governance / Data Security and Protection (IG/DSP) updates and share best practice. This meeting is the 'North East and North Cumbria Strategic Information Governance Network' (NENC SIGN) and is open to any IG / DSP Practitioner regardless of whether or not they are a signatory to the Protocol. Information Sharing will be a standing agenda item of this group.

A Protocol Review task and finish group will meet every two years in accordance with any significant changes to relevant legislation - usually immediately following a meeting of the North East and North Cumbria Strategic Information Governance Network. The Protocol Review task and finish Group will be made up of any of the Partner organisations listed in Appendix A – this will be a voluntary arrangement.

The Protocol Review task and finish Group will review the Protocol documentation and agree on any changes that are required to be made according to local and national guidance or legislative changes.

Individual Information Sharing Agreements should have their own review arrangements included within the formal agreement.

6.2. Specific Procedures

6.2.1. All procedures, including Information Sharing Agreements, devised as a result of the Protocol will state who is responsible for the monitoring and review process in relation to them.

Appendices

Appendix A: List of Signatories and Information Governance Contacts
Appendix B: Terms of Reference for the Protocol Review Group
Appendix C: Relevant Legislation
Appendix D: Criminal Data Disclosure Form
Appendix E: NENC Template Information Sharing Agreement
Appendix F: Signature Form
Appendix G: Communicating Rectifications of Personal and Special Category Information between Organisations
Appendix H: Signatories List

Appendix A: List of Signatories and Information Governance Contacts

Emergency Services
County Durham Fire and Rescue Service Data Protection Officer: DPO Email:
Durham Constabulary Data Protection Officer: Leigh Davison DPO Email: Leigh.Davison@durham.police.uk
North East Ambulance Service Data Protection Officer: Seema Srihari DPO Email:
North West Ambulance Service Data Protection Officer: DPO Email:
Local Authorities
Durham County Council Data Protection Officer: DPO Email:
Darlington Borough Council Data Protection Officer: DPO Email:
Hartlepool Borough Council Data Protection Officer: Laura Stones Scrutiny & Legal Support Officer DPO Email:
Gateshead Metropolitan Borough Council Data Protection Officer: DPO Email:
Newcastle City Council Data Protection Officer: DPO Email:
Middlesbrough Borough Council Data Protection Officer: DPO Email:
Redcar & Cleveland Borough Council Data Protection Officer: DPO Email:
Stockton Borough Council Data Protection Officer: DPO Email:
Cumberland Council Data Protection Officer: Sarah Pearce DPO Email:

Health Bodies
Northumbria NHS Foundation Trust Data Protection Officer: Tracey Best DPO Email:
Newcastle NHS Foundation Trust Data Protection Officer: Julia Scott DPO Email:
Gateshead NHS Foundation Trust Data Protection Officer: Dianne Ridsdale DPO Email:
Tees, Esk, and Wear Valley NHS Foundation Trust Data Protection Officer: Andrea Shotton DPO Email:
South Tees NHS Foundation Trust Data Protection Officer: Kerry McLean **DPO Email:**
North Tees & Hartlepool NHS Foundation Trust Data Protection Officer: Kerry McLean DPO Email:
South Tyneside and Sunderland NHS Foundation Trust Data Protection Officer: Jim Carroll DPO Email:
County Durham and Darlington NHS Foundation Trust Data Protection Officer: Lisa Nattrass DPO Email: **cddft.dataprotectionofficer@nhs.net**
Cumbria, Northumberland, Tyne and Wear NHS Foundation Trust Data Protection Officer: Angela Faill DPO Email:
North Cumbria Integrated Care NHS Foundation Trust Data Protection Officer: Yvonne Salkeld DPO Email: **DPO@NCIC.nhs.uk**

Sunderland Care and Support Data Protection Officer: DPO Email:
North of England Commissioning Support (NECS) Data Protection Officer: Gillian Flynn DPO Email:
NENC Integrated Care Board Data Protection Officer: Liane Cotterill DPO Email:

Appendix B: Terms of Reference for the Protocol Review Group – NENC SIGN

NE SIGN TOR v6.0
Final Jan 25.docx

The Terms of reference are reviewed on an annual basis and can be requested from any representative of the NENC SIGN group.

Appendix C: Relevant Legislation

ICO web site - **https://ico.org.uk/**

Link to Data Protection Act 2018 -
http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Link to General Data Protection Regulation – **https://gdpr-info.eu/**

Link to Human Rights Act 1998 -
https://www.legislation.gov.uk/ukpga/1998/42/contents

Link to Health and Social Care Act 2015 –
http://www.legislation.gov.uk/ukpga/2015/28/pdfs/ukpga_20150028_en.pdf

App C Relevant
legislation V9.3 Oct 1

Appendix D: National Police Chiefs Body (NPCC) Criminal Data Disclosure Form

Data Protec. 3 File
Build - Request Forr

Cumbria Police
Revised Personal Inf

Appendix E: Template Information Sharing Agreement v9.0

App E MA ISA Agreement template

Appendix F: Signature Form

North East and North Cumbria Overarching Multi Agency Information Sharing Protocol

By becoming a Partner Agency to this Protocol, Partner Agencies are making a commitment to:

Apply the standards that are prescribed in guidance and Codes of Practice issued by the Information Commissioner's Office and. **https://ico.org.uk/for-organisations/**

Comply with the provisions of Data Protection legislation which includes, but not limited to:

- The UK General Data Protection Regulation (UKGDPR)
- Data Protection Act 2018 (DPA)
- Privacy and Electronic Communications Regulations (PECR)
- Digital Economy Act 2017 (DEA)

Follow the standards prescribed by the Protocol document which includes processes for sharing information on both a routine and ad-hoc basis.

All Partner Agencies agree to be responsible for ensuring measures are in place to guarantee the security and integrity of data and that stuff are sufficiently trained to understands their responsibilities and comply with the law. Agencies will recognise that this document encourages sharing of data, but does not alter the statutory duties of those organisations signed up to it.

Organisation:	**Organisation Name**
Data Protection Officer:	Name:- Email:- Date of Signature
Caldicott Guardian / Senior Information Risk Owner:	Name:- Email:- Date of Signature

Signature forms will be kept in a central location held by the Protocol's secretary

Appendix G: Communicating Rectifications of Personal and Special Category Information between Organisations

1.1. The Caldicott Guardian (CG) or Designated Officers from the source organisation will ensure that all factually inaccurate information has been rectified at source.

1.2. The CG from the source organisation will communicate the issue to all CGs (or equivalent) for all other organisations known to have received information relating to the data subject from the source organisation.

1.3. The source CG will request that all information relating to the data subject that was provided by the source organisation and is held by the recipient organisation is also rectified.

1.4. The CG from the recipient organisation will confirm in writing to the source CG that the appropriate rectification and actions have been completed.

1.5. To ensure the candour the source CG will make contact with the client to assure them that the appropriate rectification and actions have been completed across all organisations with which the source organisation has shared their data.

1.6. The Caldicott Guardian for the GP practice will always be involved with rectification so that any changes are also made to the primary care record where relevant.