MULTI - AGENCY OVERARCHING INFORMATION SHARING PROTOCOL

Aims and Objectives

1 The Protocol aims to ensure compliance and consistency by achieving the following objectives:

- Creating a legally binding Protocol to govern working practices and create greater transparency, data security and improved services for users;
- Offering guidance on how to share information lawfully;
- Increasing understanding of Data Sharing principles and legislation;
- Developing a Partner Agency Information Sharing Arrangement template (Appendix J to the Protocol) 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 Agencies from allegations of wrongful use of data;
- To monitor and review information flows.

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

- Apply the “Fair Processing” and “Best Practice” standards that are in the Information Commissioner’s Data Sharing Code of Practice and checklists;
- Comply with the Data Protection Act and other relevant legislative provisions;
- Develop individual Partner Agency Information Sharing Arrangements that comply with the Protocol and clearly and transparently demonstrate the reasons for sharing data and provide assurance on this activity.

General Principles

3 The Protocol recognises and promotes recommended good practice and legal requirements to be followed by all Partner Agencies. The Protocol does not alter existing arrangements already in place for urgent sharing, for example, relating to child protection and safeguarding.

4 All Partner Agencies 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. The Protocol encourages sharing of data, but does not alter the statutory duties of those organisations signed up to it.

Data Sharing and the Law

5 The main legal provisions relating to information sharing are contained in the Protocol.

6 When creating a Partner Agency Information Sharing Arrangement (Appendix J), a lawful basis for the proposed information sharing must be identified and recorded.

7 It is recognised that information shared between different Partner Agencies may be subject to FOI or Subject Access requests. The Protocol describes the process to follow where such a request is received.

Organisational Responsibilities

8 Each Partner Agency is responsible for ensuring that their organisation and security measures protect the information shared under the Protocol.

9 General responsibilities include:

- Ensuring that the information shared is necessary for the purpose for which it is shared, is shared only with those people who need it, is accurate and up-to-date, is shared in a timely fashion, and is shared, handled and processed securely. The Partner Agency Information Sharing Arrangement will provide more details in each particular case;
- Considering the impact that any decision to share information may have on the individual, their safety and well-being and on others who may be affected by their actions;
- Privacy statements to govern consent for information sharing should be compatible with the aims of the Protocol;
- Partner Agencies should independently or jointly ensure compliance with any Partner Agency Information Sharing Arrangements they are involved in;
- Partner Agencies should consider making it a condition of employment that employees will abide by their rules and policies on the protection and use of personal and/or sensitive personal information;
- Contracts with external service providers should include a condition that they abide by the relevant Partner Agencies' rules and on the protection and use of personal and/or sensitive personal information;
- Incident reporting procedures should be in place to notify other Partner Agencies in the event of an information security incident;
- Ensuring that adequate security measures are in place to protect information;
- Ensuring that each Partner Agency Information Sharing Arrangement establishes the specific arrangements for retention and disposal of information for all parties involved, including details of the exact arrangements for the transfer, storage and destruction of data where required;

- If a Data Subject withdraws consent to process their personal information (by serving a notice under section 10 of the Data Protection Act), other Partner Agencies must be notified so that they can cease processing this data as soon as possible;
- Decisions about whether to share information or not and the reasoning behind them should be recorded. If information is to be shared then Partner Agencies should record exactly what data is to be shared, with whom and for what purpose. Specific processes should be recorded in the Partner Agency Information Sharing Arrangement;
- All Partner Agencies agree to publish a copy of the Protocol on their websites, so that the public are aware of the processes in place for information sharing.

10 Additional Personal & Sensitive Personal Data responsibilities:

- Personal Data should only be shared for a specific lawful purpose or where appropriate consent has been obtained;
- Staff should only be given access to Personal Data where there is a legitimate need;
- The Protocol does not intend to give unrestricted access to information. Other Partner Agencies should only be able to access data on a justifiable need to know basis and only relevant employees should be allowed to access the data in order to carry out their duties effectively. Access must be removed when it is no longer necessary;
- All employees who will handle and share data within each organisation should be trained so that they are aware of and comply with their responsibilities and obligations to maintain the security and confidentiality of personal information;
- Information sharing must be compliant with relevant legislation and with any other conditions Partner Agencies may attach in each agreed Partner Agency Information Sharing Arrangement. The legal basis for sharing must also be recorded in the Partner Agency Information Sharing Arrangement;
- Personal Data shall not be transferred to a country or territory outside the European Economic Area (EEA) without an adequate level of protection for the rights and freedoms of the Data Subject in relation to the processing of Personal Data.

11 Non-Personal Data responsibilities:

- Partner Agencies should not assume that non-personal information is not sensitive and can be freely shared. In particular, anonymised data when combined with data from other sources may lead to individuals being identifiable. The consent of the originating Partner Agency should be obtained if data is to be shared with a third party;
- Business/commercially sensitive data also requires protection against loss or corruption. The conditions on handling these types of data will depend on the protective mark applied, or as otherwise determined by the original data owner/controller.

Individual Responsibilities

12 Every individual working for the Partner Agencies is personally responsible for the safekeeping of any information they obtain, handle, use and disclose and must be trained to carry out these duties.

13 Individuals should request proof of identity, or take steps to validate authenticity before disclosing any information requested under this Protocol and associated Partner Agency Information Sharing Arrangements.

Restrictions on the use of Information Shared

14 All shared information, personal or otherwise, must only be used for the purpose(s) specified at the time of disclosure(s) as defined in the relevant Partner Agency Information Sharing Arrangements, unless obliged under statute or regulation, or under the instructions of a court or as agreed elsewhere. Any further uses made of the data will not be lawful or covered by the Partner Agency Information Sharing Arrangements.

15 Secondary use of non-personal information may be subject to restrictions (eg commercial sensitivity). If a Partner Agency wishes to share such information with a third party they should consult the information's original owner.

16 Certain information is subject to additional statutory restrictions, for example Criminal Records and Child Protection. Details of any further restrictions will be included in relevant Partner Agency Information Sharing Arrangements.

Consent – Personal and Sensitive Personal data

17 The usual way to gain and control consent is through privacy statements or notices. These are written or oral statements given to individuals when information is collected about them and which cover, among other things: who is collecting the information, what will be done with it and who it will be shared with. These should be updated regularly to ensure they remain relevant and cover any planned information sharing activities.

18 Data subjects must have the right to withdraw consent at any time; if consent is withdrawn the Partner Agency in question must inform the other Partner Agencies as soon as practicable.

19 Personal data can be disclosed in certain circumstances without consent. When a Partner Agency has a statutory obligation to disclose personal data the consent of the data subject is not required. However, where appropriate, the data subject should be informed such an obligation exists. In a case where a Partner Agency decides not to disclose some or all of the personal data requested, the requesting authority must be informed.

20 Consent has to be signified by some communication between the Partner Agency and the data subject. If the data subject does not respond, this cannot necessarily be assumed as implied consent. When using sensitive personal data, explicit consent must be obtained subject to any existing exemptions. In

such cases the data subject's consent must be clear and cover items such as the specific details of processing, the data to be processed and the purpose.

21 Specific procedures apply where the data subject is not considered able to give informed consent. The relevant Partner Agency's policy on capacity to give consent should be followed in these circumstances.

22 Under certain circumstances, disclosures of information to another Partner Agency may be justified when a relevant statutory exemption is met; these include:

- the prevention and detection of crime;
- the apprehension or prosecution of offenders;
- the assessment or collection of tax or duty.

23 In cases where statutory exemptions do not apply Partner Agencies may still need to disclose personal information for safeguarding purposes if sharing the data would be in individuals' best interests.

Security

24 Any information shared under this Protocol must be stored securely by the receiving Partner Agency.

25 It is expected that each Partner Agency has achieved or will aim to work towards information security standards such as ISO 27001, compliance with the NHS Connecting for Health Information Governance Toolkit or will adhere to a similar level of compatible security. Only nominated representatives can access, request information, and make disclosure decisions. Data should be stored securely to prevent unauthorised access and disclosure.

26 Each Partner Agency agrees to apply appropriate security measures, commensurate with the requirements of principle 7 of the DPA. Partner Agencies are encouraged to have an Information Security Policy in place setting out the minimum standards of security they require. The Protocol sets out the principles which should be followed where Partner Agencies do not have a specific policy in place.

27 Should additional security arrangements be required, these should be set out in the individual Partner Agency Information Sharing Arrangements. To determine what security measures are appropriate in any given case, each Partner Agency must consider the type of information and the harm that would arise from a breach of security. In particular, each Partner Agency must consider:

- Where the information is stored;
- The security measures programmed into the relevant equipment;
- The reliability of employees having access to the information.

28 It is the responsibility of the Partner Agency which discloses Personal Data to make sure that it will continue to be protected by adequate security by any other agencies that access it by including clearly stated requirements in Partner Agency Information Sharing Arrangement. Once the information has been received by the Partner Agency they will have their own legal duties with respect to this information.

29 In the event of a security breach in which information received from another Partner Agency is compromised, the originator should be notified at the earliest opportunity.

30 It is accepted that not all Partner Agencies will have security classification in place, however, it is recommended that signatories to Partner Agency Information Sharing Arrangements: (i) protectively mark the materials they share to indicate the level of sensitivity, and (ii) align the protective marking classification they use with that used by Central Government or similar.

31 Specific storage and security arrangements, as well as access to data, will all be detailed in the Partner Agency Information Sharing Arrangements, which should be periodically reviewed to ensure that security arrangements are appropriate and effective.

Information Management

Data Quality

32 Information shared should be as complete (but not excessive), accurate and up-to-date as practicable to ensure it can be used for the purposes for which it is required.

33 Information discovered to be inaccurate or inadequate for the purpose should be notified to the relevant data owner.

Data Processing

34 Partner Agencies are expected to ensure that the Personal Data and Sensitive Personal Data they hold is processed in accordance with the Data Protection Act principles.

Data Retention

35 Each Partner Agency will apply relevant regulations and timescales to the retention, review and disposal of information (electronic and paper based), only keeping information for as long as is necessary in relation to the purpose it was obtained.

36 Each Partner Agency must take all reasonable steps to ensure that information is disposed of or destroyed in a way that makes reconstruction unlikely.

37 Agencies should also make any Partner Agencies they share information with aware of their rules on data retention and whether these apply to the data being shared.

Training

38 An e-learning package has been developed which is offered to Partner Agencies to this Protocol to support implementation. Partner Agencies are encouraged to ensure relevant employees complete this training. This training should ideally be completed by employees who will have any responsibility for handling or sharing information, to ensure they can undertake their duties confidently, efficiently and lawfully.

39 Alternatively, Partner Agencies are encouraged to support the implementation of the Protocol by carrying out their own form of training for relevant employees. The training should focus on the principles of the Protocol and include an explanation of:

- the aims and objectives of the Protocol;
- the main provisions of the Protocol, including information security and the handling of Personal Data and Sensitive Personal Data;
- the process involved in setting up an Partner Agency Information Sharing Arrangement;
- the forms and templates accompanying the Protocol;
- the Information Sharing Contacts.

Review Arrangements

40 An Information Governance Monitoring Group will be established, and will meet at least annually. Membership will comprise the relevant Information Sharing Points of Contact. The responsibilities of the Information Governance Monitoring Group will be to:

- Review information governance procedures to establish whether they are still effective and working in practice;
- Monitor the effectiveness of the Protocol and associated documents and update the contents when appropriate;
- Share best practice among Partner Agencies and update guidance to reflect this where necessary;
- Build a culture of information sharing between Partner Agencies by proactively communicating the aims of the Protocol;
- Promote and implement education/training practices designed to encourage behaviour change in relation to information sharing;
- Support the development of Partner Agency Information Sharing Arrangements under the Protocol;
- Review and update the Protocol as necessary;
- Review and update the e-learning package accompanying the Protocol as necessary.

41 Any Partner Agency can suspend their obligations under the Protocol for 30 days, if they feel that security has been seriously breached or there are concerns over the operation of the Protocol. Any suspension will be subject to a risk assessment and resolution meeting comprising of all the signatories of the Partner Agencies or their nominated representative. This meeting will take place within 14 days of any suspension.

42 Any Partner Agency may withdraw from the Protocol. The Partner Agency's signatory to this Protocol must notify the Chairs of the Information Governance Monitoring Group in writing, stating the reason for the withdrawal.