Livewell Southwest

Template for developing Data Sharing Protocols

Version No 1.1

Notice to staff using a paper copy of this guidance

The policies and procedures page of LSW intranet holds the most recent version of this document and staff must ensure that they are using the most recent guidance.

Author: **Information Governance Group**

Asset Number: **828**

Reader Information

Title	Template for developing Data Sharing Protocols V.1.1
Asset number	828
Rights of access	Public
Type of paper	Template
Category	Corporate
Document purpose/summary	The purpose of this template is to provide a framework for detailed data sharing agreements between LSW and other agencies.
Author	Information Governance Group
Ratification date and group	24th February 2016. Policy Ratification Group
Publication date	3rd March 2016
Review date and frequency (one, two or three years based on risk assessment)	A full review will take place two years after publication, however it will be monitored regularly and changes made accordingly in line with best practice and legislation.
Disposal date	The PRG will retain an e-signed copy for the archive in accordance with the Retention and Disposal Schedule, all copies must be destroyed when replaced by a new version or withdrawn from circulation.
Job title	Information Governance Lead
Target audience	All LSW staff
Circulation	Electronic: (LSW) intranet and website (if applicable) Written: Upon request to the PRG Secretary on ☏ 01752 435104. Please contact the author if you require this document in an alternative format.
Consultation process	Information Governance Group
Equality analysis checklist completed	Yes
References/sources of information	Worcestershire Mental Health Partnership NHS Trust Information Sharing Protocol Toolkit (2010) Please refer to the Data Protection, Confidentiality, Calidicott & Safe Haven Policy & Procedure available on healthnet
Associated documentation	N/A
Supersedes document	V.1.
Author contact details	By post: Local Care Centre Mount Gould Hospital, 200 Mount Gould Road, Plymouth, Devon. PL4 7PY. Tel: 0845 155 8085, Fax: 01752 272522 (LCC Reception).

Document review history

Version no.	Type of change	Date	Originator of change	Description of change
0.1	New document	14/01/2013	Information Governance Lead	New document
1	Ratified	April 2013	PRG	Addition to Section 5
1.1	Reviewed	December 2015	Internal audit	7. Caldicott (Page 18) Changes to reflect Caldicott 2 and the addition of Principle 7

Template

Data Sharing Protocol

Between

Livewell Southwest

&

Name of Organisation (1)
Name of Organisation (2)
Etc. (3+)

Version No.

Version Date:

Contents		Page

Template for developing Data Sharing Protocols

1. Purpose

The purpose of this Protocol is to provide a framework for detailed information sharing agreements between Livewell Southwest (LSW) and (*lists organisations/agencies).*

2. Partner agencies covered by this protocol

Organisations / Agencies	**Protocol Lead Person**

3. Relationship of this protocol to other protocols

This Protocol sits at Tier (*delete as appropriate) Two or Three* in a framework for Plymouth. Its relationship to other protocols can be seen in the table below:

Tier One	Overarching Data Sharing Agreement: Standard for sharing personal data.
Tier Two	Data Sharing Arrangement: General protocol for sharing information across health and social care services in Plymouth.
Tier Three	Operational Arrangement: Detailed information sharing agreements relating to specific functions/services.

4. Legal basis for information sharing

NHS Act 1977: Enables the sharing of information between NHS professionals and practitioners from other agencies carrying out health services that would otherwise be carried out the NHS.

Health Act 1999: States that NHS and Local Authorities shall cooperate with one another in order to secure the health and welfare of people (this allows practitioners to share information).

When sharing information, the partner agencies will work within the requirements of the national legal framework. Key elements in this are:

- The Data Protection Act 1998
- The Human Rights Act 2000
- Freedom of Information Act 2000
- The Crime and Disorder Act 1998

- The Common Law Duty of Confidentiality
- Caldicott Principles

The principle elements of this legislation are described in appendix one.

5. Reasons for sharing information

Reasons for sharing personal information will be limited to one or more of the following:

- Delivery of effective services including personal care, treatment or advice.
- Assuring and improving the quality of services.
- Investigating complaints or actual/potential legal claims.
- Monitoring and protecting public health, safety and well being.
- Risk management.
- To avoid duplication of information gathering.
- For the prevention and detection of crime with law enforcement agencies such as the Police and NHS Protect.

Reasons for sharing non-personal information will be limited to one or more of the following:

- Managing and integrating the planning of services.
- Contracting and commissioning the provision of services.
- Auditing of accounts, care and performance.
- Statistical analysis.
- Research.

The partners to this agreement will adhere to the requirements of the Data Protection Act 1998 in relation to processing personal and sensitive information.

6. Standard for sharing information

6.1 General

All information shared for the purpose of this Protocol should be accurate, current and should not be shared indefinitely. The quantity and coverage of data shared should be directly related to the purpose of sharing, and not excessive.

6.2 Confidentiality

Personal information held by an agency shall be deemed to have been provided in confidence, unless consent to share this information has been given by the subject.

All agencies accept this duty of confidentiality and will not disclose personal information without the explicit consent of the person concerned, unless there are statutory grounds or other overriding justification for doing so.

People requesting disclosure of personal information from agencies party to this Protocol will respect this responsibility and will not seek to override the procedures which each agency has in place to ensure that information is not disclosed illegally or inappropriately.

6.3 Consent

Unless statutory exemptions apply, all agencies will endeavour to seek explicit consent from the individual concerned to share their personal information.

Consent will normally be obtained at the earliest opportunity, and in relation to specified purposes for collecting the information. Explicit consent should be obtained for sharing information that does not directly contribute to, or support the delivery of services for the individual, and the individual's decision to restrict the disclosure of their personal information should be appropriately respected.

In seeking consent to disclose personal information to another agency party to this Protocol, an individual will be made fully aware of:

- The nature of the information that will be shared.
- Who the information will be shared with.
- The purposes for which the information will be used.
- Other relevant details including their right to withhold or withdraw consent.
- The potential consequences of not sharing information (e.g. this service may not be available to you).

Based on this explanation, people have the right to withhold or specify limitations as to the sharing and use of their information. Individuals can withdraw their consent to share at any point.

Where there is evidence that a person does not have the capacity to give informed consent, staff may only disclose information about that person where it is in the best interests of the person concerned to do so, or when there is some other, lawful reason for them to do so. Decisions to share information in these circumstances will always be recorded. The Caldicott guardian can be consulted in these circumstances.

6.4 Time limit on consent

Consent to disclose personal information will be limited to the duration of the purpose for which consent was obtained.

All agencies agree that once the purpose for which consent was obtained is over that consent will be deemed to have lapsed.

In the event that similar or subsequent additional work needs to be undertaken with that individual, a new consent to disclose must be obtained.

6.5 Disclosure of Information without consent

Disclosure of personal information without consent must be justifiable under the Data Protection Act, and the person must be informed unless a specific exemption applies.

6.6 Quality of information

All agencies are responsible for ensuring that they have processes and procedures in place for ensuring that information is recorded accurately, that there are methods in place for checking this and to ensure that shared information is of sufficient quality.

7. Processes for informing individuals about use of data

Whenever an agency first collects information from an individual it must comply with the Data Protection Act 1998 requirement to provide that person with a Fair Processing Notice.

This means that the agency must provide the following information:

- The identity of the agency who will act as the Data Controller (which may be self evident).
- The purposes for which the agency will be processing the person's information.
- Details of how and why that information may be shared with other agencies.

Agencies will establish processes to seek explicit consent to share information, and will ensure that proper systems are in place to record whether consent has been given or not.

This Protocol will be a public document and will be included in the Publication Schemes of the partners under the Freedom of Information Act.

8. Processes for dealing with subject access requests and complaints

Each agency undertakes to respect and comply with any requests by people to exercise any of their rights under the Data Protection Act 1998. The most relevant rights are:

- Section 7 – subject access requests – the right to see personal information held about them.

- Section 10 – the right to prevent processing likely to cause damage or distress.
- Section 14 – the rights to rectify, block, erase or destroy any inaccurate client information. Each agency will ensure there is a Data Protection Officer or equivalent responsible for over seeing these requests. They will verify the identity of the applicant and will then ensure that the data subject receives a copy of the requested information within 40 days (subject to the statutory exemptions).

Agencies will put in place efficient and effective procedures to address complaints relating to the disclosure of the use of personal information that has been provided under the protocol.

In the event of a complaint relating to the disclosure or the use of an individual's personal information that has been supplied/obtained under the Protocol, all agencies will cooperate and assist in order to resolve the complaint.

All agencies will ensure that service users are provided with information about the complaints procedure when consent is obtained or upon request.

9. Processes for informing and guiding staff about the arrangements

All agencies will ensure that their staff (full/part time, temporary, agency, students etc.) who have access to, or are likely to come into contact with, personal information sign a confidentiality agreement as part of their terms and conditions of employment.

Agencies will ensure that all staff are aware of and comply with their responsibilities and obligations with regards to:

- The commitment of the agency to only share information legally and within the terms of the Protocol.
- Information will be shared on a need-to-know basis.
- Staff will be made aware that disclosure of personal information that cannot be justified, whether inadvertent or intentional, will be subject to disciplinary action.

Agencies will ensure that employees who need to share personal information are given appropriate training to enable them to share information legally, comply with any professional codes of practice and any local policies and procedures.

Agencies will nominate a lead person who will be responsible for the day to day management of the scheme within their agency, providing guidance for staff and for ensuring that any Tier Three protocols are approved through the appropriate information governance arrangements in their agency.

The person nominated will have sufficient seniority within the agency to influence policies and procedures at executive level. It is anticipated that within NHS Provider Services or Social Care Agencies, this person will be the Caldicott Guardian, Head of Information Governance or equivalent.

10. Additional requirements – security arrangements

All personal information must be kept in a secure environment, where access is controlled and security measures are in place. All agencies will put in place policies and procedures governing the security, storage, retention and destruction of personal information.

All agencies will put in place policies and procedures governing the access by their employees, and others, to personal information held within their manual and/or electronic systems and to ensure that access to such information is controlled and restricted to thosewho have a legitimate need to have access.

All agencies will put in place policies and procedures that govern the secure transfer of personal information both internally and externally. Such policies and procedures must cover:

- Internal and external postal arrangements.
- Verbal, face-to-face, telephone.
- Facsimiles.
- Electronic mail (secure network or encryption).
- Electronic work transfer (encrypted).

All agencies will have in place appropriate measures to investigate and deal with inappropriate or unauthorised access to, or use of, personal information, whether intentional or inadvertent.

In the event that personal information which has been shared under the Protocol is compromised or possibly compromised, the agency making the discovery will without delay:

- Inform the information provider of the details.
- Take steps to investigate the cause.
- If appropriate, take disciplinary action against the person(s) responsible.
- Take appropriate steps to avoid a repetition.

On being notified that an individual's personal information has or may have been compromised, the original provider will assess the potential implications for the individual whose information has been compromised and if necessary will:

- Notify the individual concerned.
- Advise the individual of their rights.
- Provide the individual with appropriate support.

- Undertake a generalised risk assessment and consider notifying the Information Commissioner's Office.

11. Implementation plan

The lead persons for this protocol from each agency will be responsible for:

- Prioritising and supporting the development of detailed Tier Three agreements by operational staff.
- Reviewing and revising this protocol as appropriate.

12. Partner sign off

The signatories to the Protocol recognise and accept the principles laid down in this document as a legal and secure framework for the sharing of personal information between their agencies in a manner compliant with their statutory and professional obligations and responsibilities.

This Protocol applies from *(enter date)* shall be reviewed every three years. The review shall be undertaken by a representative from each organisation / agency and Data Protection Officers/Caldicott Guardians as appropriate.

Agency	**Name and job title**	**Signature**

All policies are required to be electronically signed by the Lead Director. Proof of the electronic signature is stored in the policies database.

The Lead Director approves this document and any attached appendices. For operational policies this will be the Locality Manager.

The Executive signature is subject to the understanding that the policy owner has followed the organisation process for policy Ratification.

Signed: Director of Professional Practice, Safety & Quality

Date: 1st March 2016

Appendix One – Legislation

1. Data Protection Act 1998 (www.dataprotection.gov.uk)

The key principles of the Data Protection Act are:

1) Personal Data must be processed (e.g. collected, held, disclosed) fairly and lawfully and that processing must satisfy one of the conditions in Schedule 2 of the Act. The processing of sensitive data is further protected in that processing must also satisfy at least one of the conditions of Schedule 3 of the Act.
2) Personal Data shall be obtained and processed for only one or more specific and lawful purpose(s).
3) Personal Data shall be adequate, relevant and not excessive in relation to the specified purpose(s).
4) Personal Data shall be accurate and kept up to date.
5) Personal Data shall not be held for longer than is necessary.
6) Processing of Personal Data must be in accordance with the rights of the individual.
7) Appropriate technical and organisational measures should protect Personal Data.
8) Personal Data should not be transferred outside the European Union unless the recipient provides adequate protection.

Schedule 2 of the Data Protection Act 1998 specifies conditions Relevant to the
Processing of Personal or Sensitive Data.

a) The data subject has given his/her consent to the processing
b) The processing is necessary for:
   - the performance of a contract to which the data subject is a party, or
   - for the taking of steps at the request of the data subject with a view to entering into a contract.
c) The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.
d) The processing is necessary to protect the vital interests of the data subject.
e) The processing is necessary for the administration of justice for the exercise of any functions conferred on any person by or under any enactment for the exercise of any functions of the Crown, a Minister of the Crown or a government department for the exercise of any other functions of a public nature exercised in the public interest by any person.
f) The processing is necessary for the purpose of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except when the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject. The Secretary of State may by

order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

Schedule 3 of the Data Protection Act 1998 specifies additional conditions relevant for the processing of sensitive personal data. Sensitive personal data means data about:

- The racial or ethnic origin of the data subject.
- Their political opinions.
- Their religious beliefs or beliefs of a similar nature.
- Trade union membership.
- Physical or mental health or condition.
- Sexual life.
- Criminal offences or alleged offences.

These conditions are:

1) The data subject has given his/her explicit consent.
2) The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.
3) The processing is necessary –

   (a) in order to protect the vital interests of the data subject or another person, in a case where -

   (i) consent cannot be given by or on behalf of the data subject, or

   (ii) the data controller cannot reasonably be expected to obtain the consent of the data subject, or

   (b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

4) The processing –

   (a) is carried out in the course of its legitimate activities by any body or association which -

   (i) is not established or conducted for profit, and
   (ii) exists for political, philosophical, religious or trade-union purposes,

   (b) is carried out with appropriate safeguards for the rights and freedoms of data subjects,

   (c) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and

(d) does not involve disclosure of the personal data to a third party without the consent of the data subject.

5) The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

6) The processing –

(a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
(b) is necessary for the purpose of obtaining legal advice, or
(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

7) The processing is necessary –

(a) for the administration of justice,
(b) for the exercise of any functions conferred on any person by or under an enactment, or
(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

8) The processing is necessary for medical purposes and is undertaken by -

(a) a health professional, or
(b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

9) The processing -
(a) is of sensitive personal data consisting of information as to racial or ethnic origin,
(b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and
(c) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

10) The personal data is processed in circumstances specified in an order made by the Secretary of State.

3. Human Rights Act 2000 (www.humanrights.gov.uk)

Article 8.1 of the European Convention on Human Rights (given effect via the Human Rights Act 2000) provides that “everyone has the right to respect for his private and family life, his home and his correspondence”.

This is however, a qualified right i.e. there are specific grounds upon which it may be legitimate for authorities to infringe or limit those rights.

Article 8.2 of the European Convention on Human Rights provides “there shall be no interference by a public authority with the exercise of this right except as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention of disorder of crime, for the protection of health or morals, or for the protection of the rights and freedoms of others”.

In the event of a claim arising from the Act that an organisation has acted in a way which is not compatible with the Convention rights, a key factor will be whether the organisation can show, in relation to its decisions(s) to have taken a particular course of action:

a) That it has taken these rights into account;
b) That it considered whether any breach might result, directly or indirectly, from the action, or lack of action;
c) If there was the possibility of a breach, whether the particular rights which might be breached were absolute rights or qualified rights;
d) (if qualified rights) whether the organisation has proceeded in the way mentioned below.

4. Crime and Disorder Act 1998 (www.homeoffice.gov.uk/cdact)

The Crime and Disorder Act 1998 introduces measures to reduce crime and disorder, including the introduction of local crime partnerships around local authority boundaries to formulate and implement strategies for reducing crime and disorder in the local area.

Section 115 of the Act provides that any person has the power to lawfully disclose information to the police, local authorities, probation service or health authorities (or persons acting on their behalf) where they do not otherwise have the power, but only where it is necessary and expedient, for the purposes of the Act.

Whilst all agencies have the power to disclose, section 115 does not impose a requirement on them to exchange information, and responsibility for the disclosure remains with the agency that holds the information. It should be noted, however, that this does not exempt the provider from the requirements of the second Data Protection principle.

5. Common Law Duty of Confidentiality

All staff working in both the public and private sectors should be aware that they are subject to a Common Law Duty of Confidentiality, and must abide by this.

‘In confidence’…Information is said to have been provided in confidence when it is reasonable to assume that the provider of that information believed that this would be the case, in particular where a professional relationship may exist e.g. doctor/patient, social worker/client, lawyer/client etc.

The duty of confidence only applies to person identifiable information and not to aggregate data derived from such information or to information that has otherwise been effectively anonymised i.e. it is not possible for anyone to link the information to a specific individual.

The duty of confidence requires that unless there is a statutory requirement or other legal reason to use information that has been provided in confidence, it should only be used for purposes that the subject has been informed about and has consented to. This duty is not absolute, but should only be overridden if the holder of the information can justify disclosure as being in the public interest (e.g. to protect others from harm).

Whilst it is not entirely clear under law whether or not a common law duty of confidence extends to the deceased, the Department of Health and relevant professional bodies accept that there is an ethical duty to respect the confidentiality of the dead.

Unless there is a sufficiently robust public interest justification for using identifiable information that has been provided in confidence then the consent of the individual concerned should be gained before disclosure of their information. Schedules 2 and 3 of the Data Protection Act 1998 apply whether or not the information was provided in confidence.

Where it is judged that an individual is unable to provide informed consent (due to age or condition), schedule 2 and 3 of the Data Protection Act 1998 must be satisfied (processing will normally need to be in the vital interest of the individual). 'Public functions' as outlined in schedule 2 and 'medical purposes' as outlined in schedule 3 of the Data Protection Act 1998 are also likely to be relevant.

6. Regulation of Investigatory Powers Act 2000 (www.homeoffice.gov.uk/ripa)

The Regulation of Investigatory Powers Act 2000 primarily deals with the acquisition and disclosure of information relating to the interception of communications, the carrying out of surveillance and the use of covert human intelligence. It is unlikely that this Act will have any implications on the sharing of personal information.

7. Caldicott (http://systems.hscic.gov.uk/infogov/caldicott)

Although not a statutory requirement, NHS and Social Care organisations are committed to the following Caldicott principles which encapsulate the above mentioned statutes when considering whether confidential information should be shared.

Principle 1 Justify the purpose(s) of using confidential information.

Principle 2 Only use it when absolutely necessary.

Principle 3	Use the minimum that is required.
Principle 4	Access should be on a strict need-to-know basis.
Principle 5	Everyone must understand his or her responsibilities.
Principle 6	Understand and comply with the law.
Principle 7	The duty to share information can be as important as the duty to protect patient confidentiality.