Portsmouth Information Sharing Framework

Contents

Version Control

Version	Date amended	Brief description of changes
15	15 May 2014	Version control section - added Summary - added Appendix 1 - sentence added to make it clear PIA is an example. Appendix 1 - Previous PIA from Portsmouth City Council now updated Appendix 11 - new
	10 Nov 2015	List of relevant legislation updated
	10 Nov 2015	New Appendix 5 - Caldicott Principles
	19 Jan 2016	Clarifications in Appendix 2 - Example of operational agreement esp Privacy Impact Assessment,Legal justification for sharing and Fair Processing Information sections
	29 Jan 2016	12.2.4 Government Protective Marking Scheme now called Government Security Classification Policy – wording of this section amended. The addition of a flowchart as Section 18 to inform use of the document by non-IG specialists looking to put in place an operational agreement. Current appendices 1 (Example of Privacy Impact Assessment) & 2 (Example of operational agreement for data sharing between agencies) combined into a single appendix with a part A and a part B. Legal justifications for sharing added to the relevant field in part A of appendix 1. Appendix listing useful websites & guidance added. Glossary added as a penultimate appendix.
	09 Feb 2016	New paragraph at 1.4 re integrated multi-disciplinary services, digital technology, and the framework keeping pace with change.

Summary

Organisations in Portsmouth need to share personal and non-personal information so they can work effectively together to achieve better outcomes. Effective and structured information sharing between partners:

- informs decisions about plans to improve the city
- allow us to understand trends and patterns of activity so we can allocate resources more effectively
- enables us to respond to emergencies and disasters appropriately
- helps us to intervene and support the lives and safety of individuals, families and communities, and
- prevents and detects crime, apprehends and prosecutes offenders, protects life and property and preserves order and fulfils any duty or responsibility arising from common or statute law.

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

This is the overarching Framework setting out the principles for using and sharing personal data amongst agencies working in Portsmouth. It includes templates for privacy impact assessments and information sharing operational agreements which agencies can use in specific circumstances or projects.

1 Foreword

1.1 Portsmouth has a long history of partnership working.[1] Partner agencies work together to deliver better outcomes for our citizens, employees and employers.

1.2 This 'Information Sharing Framework' ('the Framework'), sets out the information sharing requirements which need to be addressed when sharing personal information so that agencies can work effectively together. As a city, we have considerable challenges to overcome and if we want to work together to achieve our agreed outcomes for our citizens, it necessitates the structured sharing of information between all partners. Broadly speaking, effective and structured sharing of information between partners has the ability to:

- inform decisions about plans to improve the city
- allow us to understand trends and patterns of activity
- respond to emergencies and disasters appropriately
- intervene and support the lives and safety of individuals, families and communities, and
- prevent and detect crime, apprehend and prosecute offenders, protect life and property and preserve order and any duty or responsibility arising from common or statute law.

[1] The Vision for Portsmouth (April 2008). Portsmouth Local Strategic Partnership. http://www.portsmouth.gov.uk/yourcouncil/12142.html Accessed 30 October 2013

1.3 In a world of increased information gathering and recording, we have a moral and statutory responsibility to share it carefully and responsibly. Effective use of information will support us in achieving all the ambitions and aspirations we have for our city.

1.4 As integrated multidisciplinary services become an increasingly common model of public service delivery, and organisations embrace digital technology, information sharing will become both more widespread and more easily achievable. The information sharing framework must keep pace with these changes while ensuring that data is always shared in a legally justifiable way that safeguards the individual.

1.5 Within this Framework, justifiable purposes for sharing personal information between the partner agencies include to:

- develop evidence-led policies
- plan and commission more efficient, easier to access services
- improve existing and new services
- manage, report and benchmark performance
- promote accountability to customers, stakeholders, local residents and Government
- ensure that vulnerable children, young people and adults are given the protection they need
- allow organisations to cooperate so they can deliver the care and services that those people with complex needs rely on
- avoid duplication of data gathering
- monitor and protect public health and well being
- audit accounts
- analyse statistics for research and teaching
- prevent and detect crime and promote community cohesion and safety
- investigate complaints or actual/potential legal claims
- plan for and respond to emergencies and civil contingencies across the city
- obtain civil orders for breach of tenancy obligations
- comply with legal responsibilities eg court orders.

1.6 Organisations represented on the Portsmouth Children's Trust, Safer Portsmouth Partnership, the Health and Wellbeing Board as well as individual organisations working in Portsmouth are signed-up to this Framework. Statutory responsibilities remain, as always, with each organisation, but collectively this represents our commitment to sharing data.

1.7 This document is based on Protocols drawn-up by Coventry's Local Strategic Partnership. The template for individual information sharing agreements was drawn up by a pan-Hampshire group of health and social care organisations. We acknowledge, with thanks, the willingness of Coventry LSP and the pan-Hampshire group to help us formulate our Framework and Agreements and their approval for us to use their documents.

2 Introduction

2.1 This overarching Framework sets out the principles for using and sharing personal data among agencies working in Portsmouth.

2.2 Organisations involved in providing services to the public have a legal responsibility to ensure that their use of personal data is lawful, properly controlled and that an individual's rights are respected. This balance between the need to share data to provide quality services and protection of confidentiality can be a difficult one to achieve.

2.3 Uncertainty over the legal position may lead to data not being readily available to those who have a genuine need to know in order for them to do their job properly and provide the services required.

3 Structure

3.1 The Information Sharing Framework has been developed in a two-level framework. There is an overarching Information Sharing Framework (this document) and agencies who 'sign up' to the Framework will agree individual Information Sharing Agreements for specific projects or in particular circumstances.

3.2 The Information Sharing Framework outlines the principles and standards of expected conduct and practice of the signatories and their staff and applies to all sharing of personal and non-personal data. The Framework establishes the organisation's intentions and commitment to data sharing and promotes good practice when sharing personal data. It also contains the legislative standards with which that all types of personal data sharing must comply.

3.3 Specific Information Sharing Agreements set out the detail of what data is to be shared, how it will be shared, how it will be kept secure and who it will be given to. These Information Sharing Agreements also set out the limits to any data sharing and the extent to which it may be passed on to a third party without recourse to the originator of the data. All individual Information Sharing Agreements developed by the participating agencies comply with the principles set down in the overarching Information Sharing Framework. Appendix 1 part B provides model good practice of a specific information sharing agreement.

4 Aims and objectives of this Framework

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

4.2 Specifically, this Framework aims to support appropriate and necessary data sharing between organisations within Portsmouth and includes:

- the general principles of data sharing
- the legal basis for sharing data

- ♦ when it is acceptable to share without consent
- ♦ the common purposes for holding and sharing data
- ♦ broadly, how data will be stored and kept safe.

4.3 It is expected that specific information sharing agreements will be developed separately. These will specify precisely what data is to be shared, how it will be shared and stored and to whom that data will be given for a particular area of activity. Responsibility for producing these specific data sharing agreements rests with the relevant senior managers.

5 What does the Framework cover?

5.1 The Framework applies to the following types of data:

5.1.1 Personal data

"'Personal data' means data which relate to a living individual who can be identified

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual".

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

Certain types of personal data have been classified as **sensitive data,** where additional conditions must be met for that data to be used and disclosed lawfully. The term 'sensitive' personal data means personal data consisting of data as to

(a) the racial or ethnic origin of the data subject,

(b) his political opinions,

(c) his religious beliefs or other beliefs of a similar nature,

(d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),

(e) his physical or mental health or condition,

(f) his sexual life,

(g) the commission or alleged commission by him of any offence, or

(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings."

5.1.2 Anonymised data

Anonymised data is that from which the individual cannot be identified by the recipient of the data. Broadly, data in this category is data about people that has been aggregated or tabulated in ways that, in effect, anonymise the details of individuals. This sort of data can be shared without the consent of the individuals involved. 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 data is combined with other data from different agencies, where the aggregated results produce small numbers in a sample, or where traceable reference numbers are used.

5.2. There is a general presumption and expectation that anonymised and non-personal information will be shared, unless there are exceptional reasons for this. These may include:

- commercial confidentiality (Section 43 Freedom of Information Act);
- policy formulation (to inform commissioning decisions about services / where a policy is under development and circulation would prejudice its development) (Section 36 Freedom of Information Act);
- legal prejudice (Section 42 Freedom of Information Act); and
- where information is marked protectively under HMG's Protective Marking Scheme and disclosure is not deemed appropriate (refer to your organisation's standards for information classification for further details).

5.3 This Framework applies to elected members, non-executive members, trustees and all employees of partner organisations who agree to be bound by it.

5.4 It also applies to any organisation or agency which has been commissioned to deliver services on behalf of any organisation party to this Framework where permission has been given to the third party organisation to disclose data. This requirement will be included in commissioning agreements, contracts or service level agreements etc.

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

6 Legal responsibility to share

6.1 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 data sharing.

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

6.3 The principal laws, guidance and regulations concerning the protection and use of personal data are listed below:

- Information Commissioner's Data Sharing Code of Practice (May 2011)
- the Children Act 1989 and 2004
- the Data Protection Act 1998
- the Human Rights Act 1998
- the Crime and Disorder Act 1998
- the Freedom of Information Act 2000
- the Health and Social Care Act 2012
- the Health and Social Care Act (Quality and Safety) 2015
- the Care Act 2014
- the Children and Families Act 2014
- No secrets, Department of Health 2000
- Regulatory Investigatory Powers Act 2000
- Police Reform Act 2002
- Criminal Justice Act 2003
- Civil Contingencies Act 2004
- Safeguarding Adults, Association of Directors of Social Services 2005
- Housing Act 1989
- Police and Justice Act 2006
- Guidance on the Management of Police Information 2010
- Working Together to Safeguard Children 2015 Statutory guidance
- Local Government & Public Involvement in Health Act 2007
- the Common Law Duty of Confidence
- Children and Young Persons Act 2008.

6.4 Section 11.7 includes a list of legislation which permits sharing of data without consent. There will also be specific legal bases enabling data sharing to support community safety and safeguarding work.

7 Purposes for which data will be shared

7.1 Data will only be shared for lawful purposes. The specific range of purposes will be identified within the separate and specific information sharing agreements.

7.2 Where the provision of anonymised or pseudonymised data is adequate practitioners must use these as a preferred method.

7.3 The partner organisations will ensure that data is shared or requested 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 data only if the function they are required to fulfil in relation to a particular service user cannot be achieved without access to the data in question. It may not be necessary to disclose all data held regarding a service user and only such data as is relevant for the purpose for which it is disclosed should be passed under the sharing arrangement to the recipient(s).

7.4 Privacy Impact Assessments will be used when considering the risks to individuals in the collection, use, sharing and disclosure of personal information. An example of a template used for Privacy Impact Assessments is at **Appendix 1 part A**. A Privacy Impact Assessment should be completed before using the Operational Agreement at **Appendix 1 part B**.

8 Principles underpinning this Framework

8.1 Seven Golden Rules about data sharing about individuals are at **Appendix 2**. Seven Golden Rules about systematic data sharing are at **Appendix 3**. The Caldicott Principles are at **Appendix 4**. The Health and Social Care Information Centre has also published a Code of Practice[2] and a Guide to confidentiality for handling confidential health and care information[3].

8.2 The partner organisations will:

- share data with each other where it is lawful
- comply with the requirements of the Data Protection Act 1998 and in particular with the eight Data Protection Principles. For more information, please see **Appendix 5**
- inform individuals when and how data is recorded about them and how their data may be used;
- ensure that adequate technical and non-technical security measures are applied to the personal data they hold and transfer;
- develop local Information Sharing Operational Agreements
- promote staff awareness of the Framework;
- promote awareness of the need for data sharing through appropriate communications media.

9 Consent

9.1 Introduction

9.1.1 All consent should be informed. Informed consent can be either explicit or implied.

a) Informed consent

The individual giving consent needs to understand why information needs to be shared, what will be shared, who will see their information, the purpose to which it will be put and the implications of sharing that information. This would include using their information for non-healthcare purposes in an anonymised format. Fair processing notices should be in place (see example at **Appendix 6**).

b) Explicit consent

[2] Health and Social Care Information Centre, 2014. Code of practice on confidential information. http://systems.hscic.gov.uk/infogov/codes/cop/code.pdf Accessed 10 November 2015

[3] Health and Social Care Information Centre. 2013. A guide to confidentiality in health and social care: treating confidential information with respect. http://www.hscic.gov.uk/media/12822/Guide-to-confidentiality-in-health-and-social-care/pdf/HSCIC-guide-to-confidentiality.pdf Accessed 10 November 2015

Consent to share information should be obtained from the individual at the start of the involvement and covers all of the agencies within a multi-agency service but there would be a need to seek additional explicit consent for sharing with practitioners or agencies outside of the service. Obtaining explicit consent for information sharing is best practice and can be expressed either verbally or in writing although written consent is preferable since that reduces the scope for subsequent dispute.

c) Implied consent

Consent can legitimately be implied if the context is such that information sharing is intrinsic to the activity or service and especially if that has been explained or agreed at the outset. Consent could be implied, for example, when a GP refers a patient to a hospital specialist and the patient agrees to the referral. In this situation the GP can assume that the patient has given implicit consent to share Information with the hospital specialist. However, the patient's explicit consent would be required to share information outside the bounds of the original service or setting. Consent can also legitimately be implied in individuals have been fully informed about the nature and purpose of information sharing and that they have a right to object to it, but have not done so.

9.1.2 Individual organisations may have their own procedures for dealing with issues of implicit/explicit consent to allow it to meet its lawful obligations. Please refer to your organisation's procedures.

9.1.3 To give 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).

9.1.4 The person should also be advised of their rights with regard to their information (Principle 6 of the Data Protection Act. See **Appendix 5**). Additionally the individual has the right to

- withhold their consent
- place restrictions on the use of their information
- withdraw their consent at any time.

9.1.5 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 good practice for practitioners to review this as a minimum annually.

9.1.6 If a person makes a voluntary and informed decision to refuse consent for their personal information 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 – eg such as not receiving the right service/amount of support.

9.1.7 Consideration should be given as to whether consent needs to be updated if there are significant changes to the data held or shared.

9.2 Young Persons

9.2.1 Section 8 of the Family Law Reform Act entitles young people aged 16 or 17 years, having capacity, to give informed consent.

9.2.2 The courts have held that young people (below the age of 16 years) 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. Signatory organisations should refer to their own procedures to determine the age at which competency is deemed to be acknowledged.

9.2.3 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.

9.2.4 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 precedent.

9.3 Recording consent

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

9.3.2 An example of permission to share personal data is at **Appendix 7**.

9.3.3 Wherever possible, the individual or their guardian/representative, having signed the consent, should be given a copy for their retention.

9.3.4 The consent form should be securely retained on the individual's file/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.

10 Sharing with consent

10.1 Following best practice, partner organisations should seek to gain informed explicit consent from the individual concerned before sharing his/her personal data in accordance with this Framework - unless there is a specific reason for this not being possible, or where doing this would undermine the purpose of sharing that data.

10.2 Through Privacy Notices (see example at **Appendix 6**) and gaining individual consent, individuals will be made fully aware of the nature of the data that it may be necessary to share, who the data may be shared with, the purposes for which the data will be used, the benefits to the individual and others and any other relevant details including their right to access, withhold or withdraw consent.

10.3 All partner agencies will ensure that the details, including any conditions, surrounding consent (or refused consent) are clearly recorded on the individual's

manual record and/or electronic system in accordance with their agency's policies and procedures.

10.4 An example of a flowchart of sharing data, including obtaining consent, is at **Appendix 8.**

11 Sharing without consent

11.1 The Data Protection Act 1998 recognises that in certain circumstances the public interest requires the disclosure of personal data without consent. These are:

- disclosures required by law or in connection with legal proceedings or on production of a court order.
- disclosures required for the prevention or detection of serious crime
- disclosures required to protect the vital interests of the individual concerned
- where there is an overriding public interest.

11.2 The decision to disclose under these circumstances must be documented and include the reason for the decision, who made the decision, who the data was disclosed to and the date. A decision not to share data must also be recorded.

11.3 Where data needs to be shared in order to fulfil statutory requirements, but does not comply with the Data Protection Act, these requests will be considered and approved by the appropriate Caldicott Guardians or Senior Information Risk Officers (SIROs) of the partner organisations.

11.4 If you are unsure about whether it is lawful to disclose data without consent, contact your organisation's Data Protection Officer, or seek legal advice.

11.5 An example of a template Record of Disclosure for an individual's record is at **Appendix 9**.

11.6 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.

11.7 Legislation which permits the sharing of data without consent includes:

- 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
- Children's Act 1989 s 47
- 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
- Data Protection Act 1998, schedule 2 and schedule 3
- Terrorism Act 2000 s 19
- Civil Contingencies Act 2004.

11.8 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 agency with influence on policies and procedures. Within health and social care agencies it expected that this person will be the Caldicott Guardian.

11.9 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.

11.10 A record of the disclosure will be made in the service user's case file and the service user 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. See **Appendix 9**.

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

11.12 This situation could arise where the safety of a child/adult, would be jeopardized by informing the service user of such disclosure. In many such situations it will not be a case of never informing the individual., 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 individual's case file, clearly stating the reasons for the decision, and the person making that decision.

12 Organisational and Individual Responsibilities

12.1 Organisations who sign-up to this Framework are responsible for embedding this Framework within their own processes relating to information sharing.

12.2 A number of safeguards are necessary in order to ensure a balance between maintaining confidentiality and sharing data appropriately. Organisations who share data under this Framework will adhere to the following:

12.2.1 Ensure staff are aware of and comply with:

- their responsibilities and obligations with regard to the confidentiality of personal data about people who are in contact with their agency
- know who to contact, and processes to follow, in the event of a breach of confidentiality
- the commitment of the organisation to share data legally and within the terms of an agreed specific information sharing agreement

- ♦ the commitment that data will only be shared on a need-to-know basis
- ♦ the understanding that disclosure of personal data which cannot be justified, whether intentionally or unintentionally will be subject to disciplinary action, and maybe subject to legal sanctions.

12.2.2 Ensure information disclosed is recorded appropriately by:

- ♦ ensuring that all personal information that has been disclosed to them under an agreement is recorded accurately on that individual's manual or electronic record in accordance with the agency's policies and procedures
- ♦ putting in place procedures to record the details of the information shared, the provider and who received the information.

12.2.3 Data security

Party agencies shall have appropriate technical and organisational measures in place to protect the confidentiality, integrity and availability of the data during all stages of processing. It is envisaged that each party will adhere to common standards for data security. Each party shall have formal procedures to:

- ▪ Ensure the security of personal data before, during and after data sharing takes place.
- ▪ Deal with breaches or suspected breaches of legislation or other duty, stated or implied, relating to the confidentiality of personal data, including measures for co-operation between the parties to the Framework.

12.2.4 Where organisations use a security classification scheme (such as the Government Security Classificaton Policy), it is the responsibility of those organisations to apply the appropriate level of security when they are sharing information.

Applying a classification to an information asset expresses the sensitivity of that asset and the impact of disclosure/compromise to unauthorised recipients or users without need-to-know.

Information assets can be any possible format of information carrier, paper and electronic; and when an organisation uses Protective Marking, it should be applied to **all** information assets.

The classification of an information asset:

- defines the protective measures we need to take in the protection of that information asset
- advises on handling, storing, transmitting, processing and destroying the information asset.

Users of this agreement should refer to local guidance on GPMS if they require further guidance.

12.2.5 Data quality

Data shared should be of a good quality and it is recommended that the data shared follows either the Audit Commission's six principles of data quality, or other appropriate guidance used by the organisations sharing the data. The six data quality principles are:

- accuracy
- validity
- reliability
- timeliness
- relevance, and
- completeness.

Further information about these principles can be found in the Audit Commission document entitled "Improving information to support decision making: standards for better quality of data".

12.3 Organisations must ensure that individuals are aware of their personal responsibilities with regard to sharing personal data, and who individuals should contact if queries arise.

13 Access to data

This document is an overarching framework that identifies the guidelines and principles under which sharing of information between signatory organisations will be undertaken, this will ensure that data is managed in accordance with the currently available best practice guidance on the protection and use of confidential information.

Individual Information Sharing Agreements (as at **Appendix 1 part B**) will provide more detail of information/data items to be shared and the associated controls around their use and management.

14 Sharing with organisations who are not signatories to this Framework

If it is necessary to share data with an organisation who is not party to this overarching Framework, consideration should be given on a case by case basis as to whether or not a specific information sharing protocol should be put in place for that information flow.

15 Monitoring and review

15.1 The Joint Strategic Needs Assessment Strategy Group will, in conjunction with partner organisations, review this overarching Framework three yearly unless new or revised legislation necessitates an earlier review.

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

16 Breaches

16.1 All agencies who are party to this Framework 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.

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

- take appropriate steps, where possible, to mitigate any impacts;
- 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.

16.3 On being notified of a breach, the original data provider along with the organisation responsible for the breach, and others as appropriate, will assess the potential implications for the individual whose data 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.

16.4 Where a breach is identified as serious, it may have to be reported to the Information Commissioner's Office. The original data provider, along with the breaching organisation and others as appropriate, will assess the potential implications, identify and agree appropriate action.

17 Complaints

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

17.2 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.

18 Flowchart - setting up operational information sharing agreements / protocols

Staff of partner organisations wishing to put in place a new operational agreement should follow the steps indicated in the following flowchart:

Flowchart - setting up operational information sharing agreements/protocols

As early as possible, contact your organisation's Information Governance (IG) lead to check whether there is an existing protocol/agreement you could use. If not, seek advice and/or help with the process. Ensure that the same discussion is taking place at the agency with which your organisation needs to share data.

⇩

Establish your legal justification for sharing this data (see section 7 and appendix 1 of this document).

⇩

Complete the two-part form in appendix 1 (Example of combined Privacy Impact Assessment (PIA) and Operational Agreement (OA) for data sharing between agencies), asking your IG lead for advice and to review.

⇩

Forward the draft PIA/OA to the organisation/agency with whom you wish to share data to check and ensure that they and their IG lead are happy with the assessment and agreement.

⇩

Each organisation must have the PIA/OA document ratified and signed by an authorised signatory – usually a senior manager with responsibility for IG e.g. the Caldicott Guardian or Senior Information Risk Owner (SIRO)

⇩

You are now able to share data between organisations/agencies for the specific purpose(s) you have specified in the PIA/OA.

⇩

Please send a copy of the combined PIA/OA to joanna.kerr@portsmouthcc.gov.uk so that we have a complete, up-to-date record of agreements being used across Portsmouth.

⇩

All Privacy Impact Assessments/Operational Agreements should be subject to regular review.

Example of a combined Privacy Impact Assessment and operational agreement for data sharing between agencies

PLEASE USE RELEVANT PRIVACY IMPACT ASSESSMENT AND OPERATIONAL AGREEMENT TEMPLATE FROM YOUR OWN ORGANISATION AS APPLICABLE

Adapted with minor amendments from Portsmouth City Council (2014)

PART A

INFORMATION GOVERNANCE IMPACT ASSESSMENT QUESTIONAIRE

Please use black ink and CAPITAL letters if you are not completing this form electronically.

Data systems and/or external processes this piece of work links to			
		To be completed by Project Manager	
	Data system/external process	Separate IA Completed	Known Risks Y/N
1			
2			
3			

To be completed by Project owner			
Date received	All information provided (Y/N)	Risk Score	Signed off by Project Owner (Date and name)

To be completed by IG Administration			
Date received	All information provided (Y/N)	Risk Score	Signed off by IG Team (Date and name)

Work package details			
Project		Point of contact for this work (name, role, phone, email)	
Specific area concerned (e.g. which pilot)			
Project summary			
Brief description of overall activity			
Has anything similar been undertaken before			
Is there a reason why an			

Impact Assessment is not required for this piece of work			
Stakeholder(s) / Organisation(s) involved			
Sponsor (e.g. Project Board)		Activity period	

Information

What information will be collected – be specific (Person Identifiable Data (PID), Corporate, Sensitive etc)		
Why is information being collected		
How information is being collected	Verbal ☐ Paper questionnaire ☐ Other ☐→	Electronic form ☐ Electronic (automated) ☐
How information is to be stored	Paper ☐ Other ☐→	Electronic ☐
Where information will be stored (including back ups and copies)		
How information is to be edited or deleted		
How data is to be quality checked		
Who is responsible for the information		
What are the benefits to the individual and professional		
Is the use of Cloud technology being considered either by PCC or 3rd party supplier?	CLOUD ICO Questions_MASTERCC	

Sharing and access

What information is shared	
Who are you sharing with	
How information is to be transported	
Which roles will have access? Is there any restrictions based on different roles	
How is it accessed	
How access is to be monitored (audit, logs)	
What security measures will be in	

place	
What information sharing protocols and operational agreements will be in place	
What training is planned to support this piece of work	
What is the process for obtaining and recording consent/dissent (how, where, when, by whom)	
What is the legal justification for sharing? (See relevant section of part B)	
Will reports be generated from this information? If yes, will the information be identifiable or anonymous (will the reports be used for research)	
How can the individual access the information	
Retention	
How long data is to be retained	
What is the process for start-up and closing down this piece of work	
If the organisation/service ceases what will happen to the information	
Risks, issues and activities	
Any known risks or issues	
Any known activities that will have a direct affect on this piece of work	

Comments from Information Governance	
Comment	**Date/author**

Part B - Example of operational agreement for data sharing between agencies

Scope and Purpose

This is an Operational Agreement (OA) for data sharing between signatories of the Portsmouth Information Sharing Framework. As signatories to the Framework, the participating partner organisations agree to operate within a framework of data sharing that accords with best practice guidance set out in the Framework.

This OA is supplementary to the Framework and has been agreed between the participating partner organisations to support the regular sharing of personal data for the purpose of [Insert details here].

This OA covers the exchange of data between [Insert a brief description of the partner organisations]

It supports the data sharing partner organisations involved and the people it impacts upon. It details the specific purposes for sharing and the personal data being shared, the required operational procedures, consent processes, and legal justification that underpins the disclosure/exchange of data.

Partners may only use the data disclosed to them under this OA for the specific purpose(s) set out in this document.

Privacy Impact Assessment

[Select one of the following:]

A Privacy Impact Assessment has been completed to determine if this new process poses any new or emergent privacy concerns. Any privacy risks identified have been addressed in this Operational Agreement. [The information from the PIA should be used to populate the sections of this agreement]
OR
This Operational Agreement describes the formalisation of a pre-existing and lawful process and presents no additional privacy concerns to necessitate a privacy impact assessment. It has been determined in this case that the Operational Agreement addresses the privacy points.

Objectives

The objectives of sharing the data covered by this agreement are

- [Insert details here in bullet point form of the objectives of the data sharing covered under this agreement.]

Individuals Impacted by this OA

The residents/clients/service users and/or carers which this OA relates to include:

- [Insert details of the residents in bullet point form here].

The benefits to the people include:

- [Insert details here in bullet point form of how the ISP will benefit residents].

Legal Justification for Sharing

Please note: Staff should not hesitate to share personal data in order to prevent abuse or serious harm, in an emergency or in life-or-death situations. If there are concerns relating to child or adult protection issues, the relevant organisational procedures must be followed.

Data Protection Act, 1998 Principle 1 – Lawful Conditions

Processing, therefore sharing, of any personal data must be necessary for one or more condition of Schedule 2 of the Data Protection Act 1998. The relevant conditions are as follows:

[Complete the appropriate paragraph below and delete the one that does not apply]

- **Consent**: The sharing of personal data covered by this OA is based on informed consent from the data subject or carer. [Continue by describing the form of consent (explicit/implied) and how obtained and recorded; e.g. client signs consent form, implied consent assumed on referral, verbal consent given etc
- **Contract**: Where the agreement between data controller and data subject.
- **Legal obligation**: Where the sharing is mandated by the rule of law, for example, a Court Order.
- **Vital Interests** of the Data Subject: The sharing is necessary to prevent "life and limb" harm to the data subject, considered to be risk to life or immediate risk of serious harm.– i.e. severe or fatal.
- **Administration of justice:** Where the sharing is necessary for the functioning of the judiciary, for example the trial, finding and sentencing.
- **Legal gateway** The sharing of personal data under this protocol [is not / is not always] carried out with informed consent. In the absence of consent the legal justification for sharing is [Describe other legal or statutory basis which allows sharing, implicitly or explicitly]:
    - o
- **For a public duty in the public interest** – where the individual's right to confidentiality is outweighed by the public interest in sharing the information for the public good if there is a risk of harm. To make this assessment a Public Interest Test must be carried out on a case by case basis. Where all alternatives have been considered the public interest balance should be considered and approved by a senior officer.
- **Legitimate interests** of any party. Where the disclosure is necessary and compatible with legitimate aims of the information sharing partners to xxxxx; and where this is not unwarranted in any particular case by reason of prejudice to the rights and freedoms, or legitimate interest of the data subject. It is anticipated that disclosure will be warranted should xxxxx.

Where the Sensitive personal data will be shared under this agreement, the sharing must satisfy one or more of the following conditions of schedule 3 of the Data Protection Act. This list is not exhaustive, but the relevant conditions are as follows.
[Complete the appropriate paragraph below and delete the one that does not apply]

- No sensitive personal data will be shared under this arrangement
- Explicit and informed consent of the data subject has been obtained. The data subject must be fully aware of the scope of what they are consenting to.

- To protect the vital interests of the data subject or another person, where consent cannot reasonably be obtained or has been withheld unreasonably where the vital interests of a third party are at stake.
- The sharing is necessary for the purpose of, or in connection with, legal proceedings – (these must be directly compatible with a common law purpose to prevent public authorities acting *ultra vires*).
- The sharing of the information is necessary for:
    - the administration of justice
    - the exercise of any functions conferred on any person by or under an enactment
- The processing is necessary for medical purposes – specifically when it is necessary for the provision of care and treatment and the management of health care services
- The sharing of the information is necessary for the exercise of any functions conferred on a constable by any rule of law – this covers the use of common law powers to meet the policing purpose.

Data provided by partner organisations will not be released to any third party without the permission of the owning partner organisation.

Data to be Shared

Only the **minimum necessary** personal data consistent with the purposes set out in this document must be shared.

The data to be shared consists of [Describe or list data to be shared. [If possible include a full list of data items to be shared here or enclose as an appendix to the agreement]

Data Controller

The responsibility of Data Controller for the data subject to this agreement is held by [insert appropriate details here]:

> [Explain who is/are the data controller(s) for the data disclosed/exchanged. The responsibility may be shared (data controllers in common) or passed from one organisation to another in line with the flow of data.]

Data Quality

Personal data will only be collected using approved collection methods, ensuring the required data is complete and up-to-date.

All reasonable steps must be taken to ensure that anyone who has received data is notified of any relevant changes and if any inaccuracies are found the necessary amendments will be made.

Fair Processing Information

The Data Protection Act requires the fair processing of information unless an exemption applies. In particular, fairness involves being open with people about who is processing their data and how their data is being used. Put simply, a data subject should not be 'surprised' by their information being shared between the signatories.

Therefore so that individuals are not deceived or misled partners to this agreement should issue whenever possible a fair processing notice, either in writing or verbally. In some cases, it is in our interest to be open as to how data is shared.

[If existing fair processing notices do not adequately cover this information sharing arrangement additional measures will need to be taken and should be detailed in this section. If appropriate refer to specific leaflets etc that provide the information.]

Principle 2 – Secondary Processing

Data provided by partner organisations will not be released to any third party without the permission of the owning partner organisation.

Principle 3 – Adequate, relevant, not excessive

Only the **minimum necessary** personal data consistent with the purposes set out in this document must be shared.

The data to be shared consists of:

[Describe or list data to be shared. [If possible include a full list of data items to be shared here or enclose as an appendix to the agreement]

Principle 4 - Adequate, relevant, not excessive

Personal data will only be collected using approved collection methods, ensuring the required data is complete and up-to-date.

All reasonable steps must be taken to ensure that anyone who has received data is notified of any relevant changes and if any inaccuracies are found the necessary amendments will be made.

Principle 5 - Retention and Disposal

Personal data disclosed under this agreement will not be held for longer than necessary to fulfil the purpose for which it was collected and will be disposed of securely in accordance with national guidance and each organisation's local information retention and disposal policy.

[If it is possible to agree a set retention period for information shared under this agreement insert the details in this section.]

Principle 6 - Subject Access and Freedom of Information

If a party to this agreement receives a subject access application under section 7 of the Data Protection Act 1998 and personal data is identified as having originated from another signatory partner, it will be the responsibility of the receiving agency to contact that partner to determine whether the latter wishes to advise use of any statutory exemption under the provisions of the Data Protection Act 1998, or to consider further sharing on live matters. Disputes as to accuracy, damage or distress relating to the data processing will be passed promptly to the relevant Data Controller to resolve.

Participating partner organisations acknowledge a duty to assist one another in meeting their individual responsibilities under the Data Protection Act 1998 and the Freedom of Information Act 2000 to provide information subject to this agreement in response to formal requests.

Principle 7 – Technical and Organisational Security

Partners agree to ensure the reliability their employees through appropriate training around principle 7. As a bare minimum this should involve making staff aware of the processes outlined within this sharing agreement.

The information must be stored securely and is the responsibility of all partners to ensure that adequate security arrangements are in place in order to protect the integrity and confidentiality of information shared.

Each party agrees to apply appropriate security measures, to meet the requirements of principle 7 of the Data Protection Act to the data. That is, to make accidental compromise, loss or damage unlikely during storage, handling, use, processing, communication, transmission or transport; deter deliberate compromise or opportunist attack, and promote discretion in order to avoid unauthorised access. Any loss of data by a recipient partner must be notified to the originating partner at the earliest opportunity.

Only nominated representatives can access, request information, and make disclosure decisions and they should adhere to the 'need to know' principle when obtaining or disclosing information.

Principle 8 – Transfer outside of the EEA

Personal data supplied under the agreement will not be transferred outside the EEA.

Operational Procedures for Sharing

[Describe in this section the detailed procedures to be followed to allow data to be shared. This may be a simple as providing access to staff in one organisation to an existing information system hosted in another organisation or a more defined data transfer process. Consider the following questions if appropriate:

- Will data be requested or is an automatic data flow being set up?
- If data is being requested what is the procedure to do this?
- What will be the frequency of the data exchange?
- If setting up an automatic data flow how will data be transferred?
- If setting up an automatic data flow what are the security arrangements for the data in transit?
- Who is authorised to view/use the shared data and how?
- What systems are involved in the extraction, transfer and storage of the data?
- Could the data to be shared be transferred using the safe haven arrangements already in place in partner organisations?
- Do any arrangements need to be agreed for the return of data at the end of a contract term or agreed period of service provision?

Consider if the inclusion of a diagram or flow chart describing the sharing process will aid clarity.]

Retention and Disposal

11. Personal data disclosed under this agreement will not be held for longer than necessary to fulfil the purpose for which it was collected and will be disposed of securely in accordance with national guidance and each organisation's local information retention and disposal policy. [If it is possible to agree a set retention period for information shared under this agreement insert the details in this section.]

Subject Access and Freedom of Information

12. Participating partner organisations acknowledge a duty to assist one another in meeting their individual responsibilities under the Data Protection Act 1998 and the Freedom of Information Act 2000 to provide information subject to this agreement in response to formal requests.

Breach of Agreement

13. Any breach of this agreement should be reported and investigated in line with each partner organisation's incident reporting and management procedure and any relevant statutory guidance.

Complaints

14. Each partner organisation has a formal procedure by which individuals can direct, their complaints regarding the application of this OA.

Contacts

15. The primary contact for matters relating to the operation and management of this OA are:

Data Sharing Partner Organisations	Responsible Person
[Insert organisation details here]	[Insert job title and contact details here]
[Insert organisation details here]	[Insert job title and contact details here]
Insert rows below as necessary	

Review

16. This OA will be subject to local approval and reviewed [Insert agreed date for review here] or sooner if appropriate.

Authorised Signatories

In signing the document each signature is an undertaking to adopt the Agreement on behalf of their organisation

Signed on behalf of: .....

Signature: ..... Date: .....

Designation: ..... Role: .....

Name: ..... Title: .....

Signed on behalf of: .....

Signature: ..... Date: .....

Name: ..... Title: .....

[Add additional signature blocks as required]

Appendix 2

Seven Golden Rules of data sharing on an individual basis

1. Remember that the Data Protection Act is not a barrier to sharing data but provides a framework to ensure that personal data about living persons is shared appropriately

2. Be open and honest with the person (and/or their family where appropriate) from the outset about why, what, how and with whom data will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.

3. Seek advice if you are in any doubt, without disclosing the identity of the person where possible.

4. Share with consent where appropriate and, where possible, respect the wishes of those who do not consent to share confidential data. You may still share data without consent if, in your judgement, that lack of consent can be overridden in the public interest. You will need to base your judgment on the facts of the case.

5. Consider safety and well-being: Base your data sharing decisions on considerations of the safety and wellbeing of the person and others who may be affected by their actions.

6. Necessary, proportionate, relevant, accurate, timely and secure: Ensure that the data you share is necessary for the purpose for which you are sharing it, is shared only with those people who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely.

7. Keep a record of your decision and the reasons for it - whether it is to share data or not. If you decide to share, then record what you have shared, with whom and for what purpose.

Source: Guidance for Practitioners and Managers, 2008. Department for Children, Families and Schools

Appendix 3

Seven Golden Rules of data sharing on a systematic basis

1 Remember that the Data Protection Act is not a barrier to sharing data but provides a framework to ensure that personal data about living persons is shared appropriately

2 Assess the potential benefits and risks to individuals and/or society of sharing or not sharing.

3 Keep a record of your decision and the reasons for it - whether it is to share data or not. If you decide to share, then record what you have shared, with whom and for what purpose.

4 Necessary, proportionate, relevant, accurate, timely and secure: Ensure that the data you share is necessary for the purpose for which you are sharing it, is shared only with those people who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely.

5 Is there a legal obligation to share data (for example a statutory requirement or a court order.

6 Share with consent where appropriate and, where possible, respect the wishes of those who do not consent to share confidential data. You may still share data without consent if, in your judgement, that lack of consent can be overridden in the public interest. You will need to base your judgment on the facts of the case.

7 Agree common retention periods and process for secure deletion of the data.

Source: ICO Guidance: Data Sharing checklist – systematic data sharing

Appendix 4

The Caldicott Principles

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.

2. Don't use personal confidential data unless it is absolutely necessary

Personal confidential data 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).

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 transferred or accessible as is necessary for a given function to be carried out.

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 mean introducing access controls or splitting data flows where one data flow is used for several purposes.

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 confidentiality.

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.

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.

Source: Department of Health: Information: To Share or Not to Share – Government Response to the Caldicott Review – September 2013

Appendix 5
Eight Data Protection Principles

The Data Protection Act 1998 governs the protection and use of personal data. It sets out standards which must be satisfied when obtaining, recording, holding, using or disposing of personal data. These are summarised by the eight Data Protection Principles. Under the key principles of the Act, personal data must be:

Principle 1 - processed fairly and lawfully. There should be no surprises – data subjects should be informed about why data about them is being collected, what it will be used for and who it may be shared with.

Principle 2 - obtained and processed for specified purposes. Only use personal data for the 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).

Principle 3 - adequate, relevant and not excessive. Only collect and keep the data you require. It is not acceptable to collect data that you do not need. Do not collect data 'just in case it might be useful one day'.

Principle 4 - accurate and kept up to date. Have in place mechanisms for ensuring that data is accurate and up to date. Take care when inputting to ensure accuracy and have local procedures in place to manage requests for data to be amended.

Principle 5 - not kept for longer than is necessary. The legislation within which area you are working in, will often state how long documents should be kept. Data should be disposed of in accordance to your organisation's disposal policy.

Principle 6 - processed in accordance with the rights of the data subject under the Act. These rights include the right to:

- Make subject access requests
- Prevent the processing of data which is likely to cause them substantial
- damage or substantial distress
- Prevent processing for the purposes of direct marketing
- Be informed about automated decision making processes that affect them
- Prevent significant decisions that affect them from being made solely by automated processes
- Seek compensation if they suffer damage or distress through contravention of the Act
- Take action to require the rectification, blocking, erasure or destruction of inaccurate data
- Request an assessment by the Information Commissioner of the legality of any processing that is occurring.

Principle 7 - protected by appropriate security. This can be broken down into two elements:

- Practical – for example:
  - Internal and external postal arrangements
  - Verbal communications (phone, meetings etc)

- Electronic mail – such as what personal data can and cannot be sent via electronic mail, secure destruction of electronic mail
- Ensuring the confidentiality of faxes by using Safe Haven /secure faxes,
- Keeping confidential papers locked away,
- Ensuring confidential conversations cannot be overheard
- Ensuring data is transported securely
- Having procedures for access by their employees and others to personal data held in manual or electronic systems, and to ensure that access to such data is controlled and restricted to those who have a legitimate need to have access
- Storage of portable media
- Having procedures for the retention and disposal of records containing personal data
- Clear desk policies if appropriate

♦ Organisational (not an exhaustive list) – all organisations should have their own security policies:
- good information management practices
- guidelines on IT security
- procedure for access to personal data
- a retention and disposal policy for confidential data.

Principle 8 - not transferred to a country or territory outside the EEA without an adequate protection. If sending data outside the EEA, ensure consent is obtained and it is adequately protected. Consider carefully what is posted on websites or sent via email. Where appropriate, obtain approval from the data controller.

Appendix 6
Example of Privacy/Fair Processing Notice
Source: Based on NHS Hampshire Privacy Notice, May 2012

Privacy notice.

How we use your information
This privacy notice tells you what to expect when (Name of organisation) collects personal information. It applies to information we collect about:

- visitors to our websites
- complainants and other individuals in relation to a data protection or freedom of information complaint or enquiry
- people who use our services, e.g. application for additional healthcare funding or a specialist service.
- job applicants and our current and former employees

Visitors to our websites
When someone visits (website) we collect standard internet log information and details of visitor behaviour patterns. We do this to find out things such as the number of visitors to the various parts of the site. We collect this information in a way which does not identify anyone. We collect identifiable information from visitors to our website who register in order to comment on forum threads or to receive further information on specific topics. This information is held securely and only used for the purposes provided.

We do not make any other attempt to find out the identities of those visiting our website. We will not associate any data gathered from this site with any personally identifying information from any source. If we do want to collect personally identifiable information through our website, we will be up front about this. We will make it clear when we collect personal information and will explain what we intend to do with it.

YouTube cookies
We embed videos from YouTube channels using YouTube's privacy-enhanced mode.

People who make a complaint to us
When we receive a complaint from a person we make up a file containing the details of the complaint. This normally contains the identity of the complainant and any other individuals involved in the complaint.

We will only use the personal information we collect to process the complaint and to check on the level of service we provide. We do compile and publish statistics showing information like the number of complaints we receive, but not in a form which identifies anyone.

We usually have to disclose the complainant's identity to whoever the complaint is about. This is inevitable where, for example, the accuracy of a person's record is in dispute. If a complainant doesn't want information identifying him or her to be disclosed, we will try to respect that. However, it may not be possible to handle a complaint on an anonymous basis.

Appendix 6 continued

We will keep personal information contained in complaint files in line with our retention policy. This means that information relating to a complaint will be retained for 6 years from closure. It will be retained in a secure environment and access to it will be restricted according to the 'need to know' principle.

Similarly, where enquiries are submitted to us we will only use the information supplied to us to deal with the enquiry and any subsequent issues and to check on the level of service we provide.

People who use our services
(Name of organisation) offers various services to the public. For example, we send out publications and decide on requests for healthcare funding.

We have to hold the details of the people who have requested a service in order to provide it. However, we only use these details to provide the service the person has requested and for other closely related purposes. For example, we might use information about people who have requested a publication to carry out a survey to find out if they are happy with the level of service they received. When people do subscribe to our services, they can cancel their subscription at any time and are given an easy way of doing this.

Job applicants, current and former employees
When individuals apply to work at (Name of organisation), we will only use the information they supply to us to process their application and to monitor recruitment statistics. Where we want to disclose information to a third party, for example where we want to take up a reference or obtain a 'disclosure' from the Criminal Records Bureau we will not do so without informing them beforehand unless the disclosure is required by law.

Personal information about unsuccessful candidates will be held for 12 months after the recruitment exercise has been completed, it will then be destroyed or deleted. We retain de-personalised statistical information about applicants to help inform our recruitment activities, but no individuals are identifiable from that data.

Once a person has taken up employment with us, we will compile a file relating to their employment. The information contained in this will be kept secure and will only be used for purposes directly relevant to that person's employment. Once their employment with (Name of organisation) has ended, we will retain the file in accordance with the requirements of our retention schedule and then delete it.

Complaints or queries
(Name of organisation) tries to meet the highest standards when collecting and using personal information. For this reason, we take any complaints we receive about this very seriously. We encourage people to bring it to our attention if they think that our collection or use of information is unfair, misleading or inappropriate. We would also welcome any suggestions for improving our procedures.

This privacy notice does not provide exhaustive detail of all aspects of (Name of organisation) collection and use of personal information. However, we are happy to provide any additional information or explanation needed. Any requests for this should be sent to the address below.

Appendix 6 continued

Access to personal information
(Name of organisation) tries to be as open as it can be in terms of giving people access to their personal information. Individuals can find out if we hold any personal information by making a 'subject access request' under the Data Protection Act 1998. If we do hold information about you we will:

- give you a description of it;
- tell you why we are holding it;
- tell you who it could be disclosed to; and
- let you have a copy of the information in an intelligible form.

To make a request to (Name of organisation) for any personal information we may hold you need to put the request in writing addressing it to the Information Governance Manager, writing to the address provided below.

If we do hold information about you, you can ask us to correct any mistakes by, once again, contacting the Information Governance Manager.

Disclosure of personal information
In many circumstances we will not disclose personal data without consent. However when we investigate a complaint, for example, we will need to share personal information with the service concerned and with other relevant bodies.

You can also get further information on:

- agreements we have with other organisations for sharing information;
- circumstances where we can pass on personal data without consent for example, to prevent and detect crime and to produce anonymised statistics;
- how we check that the information we hold is accurate and up to date.

Links to other websites
This privacy notice does not cover the links within this site linking to other websites. We encourage you to read the privacy statements on the other websites you visit.

Changes to this privacy notice
We keep our privacy notice under regular review. This privacy notice was last updated on 12 October 2011.

How to contact us
Requests for information can be emailed to (the relevant person)
or by writing to:

The Information Governance Manager
Etc
Etc

Appendix 7 - Example of permission to share personal data

[Insert name/logo of organization]

Private and Confidential
Permission to View and Share

Name:	**DOB/Gender:**
Address:	**Telephone:**
Email Address:	**NHS Number:** **Paris Number**

Collecting, Viewing and Sharing Information

By recording information we aim to offer you a service that is right for you at the right time to meet your needs.

This information will be stored electronically on computer and possibly on paper. It will:

- Help us to understand what's happening in your own life and in your family.
- Tell us, about what services you are already receiving.
- Give you the opportunity to share anything you consider to be useful for us to know.

We aim to work with as many organisations as possible to be effective in our provision of services. This will be done in accordance to the Data Protection Act 1998.

In an emergency, safeguarding, or life threatening situation, there may be circumstances when we need to view and share information about you, without your consent, for the safety of yourself and others.

It is your choice who your information is shared with. You should let us know if you wish to review or change your consent and this can be updated and recorded at any time.

Are you willing for us to share your information with:

Personal

Immediate Family	**Yes/No**
Guardian	**Yes/No**
Next of Kin	**Yes/No**
Do any of these have lasting or Enduring power of attorney?	**Yes/No**

Carer	**Yes/No**
Appointee	**Yes/No**
Advocates	**Yes/No**
Religious Leader	**Yes/No**

Which of these is your preferred contact? .....

Who else would you like? .....

Care Worker / Personal Assistant

Employed/paid carer	**Yes /No**
Care agency	**Yes /No**
Supported Living Worker	**Yes/No**
Other	**Yes/No**

Who else supports you? .....

GP Surgery **Yes/No**

Anyone involved in my treatment and care

Hospital

Anyone involved in my treatment and care **Yes/No**

Community Health

Anyone involved in my treatment and care **Yes/No**
eg District Nurse, Dentist

Health & Social Care Team

Anyone involved in my treatment or care **Yes/No**

Mental Health Services

Anyone involved in my treatment and care **Yes/No**

Other Organisations

Housing Department/ Association	**Yes/No**
Private Health providers	**Yes/No**
Independent Providers	**Yes/No**
DWP - Department of Work and Pensions	**Yes/No**
Legal professionals	**Yes/No**
School/ Education	**Yes/No**
Employment Services	**Yes/No**
Blue Badge Service	**Yes/No**

Please list any others not on this list that are important to you

.....

.....

Emergency Services

Fire	**Yes/No**
Police - Local / International/Coast Guard	**Yes/No**
Ambulance Service	**Yes/No**

DO NOT SHARE WITH (please list)

....

.....

Declaration of Permission to Share Information

"I understand that information about me will be stored on computer and possibly paper. This will only be used in accordance with the Data Protection Act (1998). I agree to information about me being viewed and shared as indicated above where this is necessary in order to assess my needs and arrange and provide services."

Signed: ……..…… Date: ...…….....

Print Name: ……..……

<u>If signing on behalf of someone</u>

Signed: ……..…… Date: ...…….....

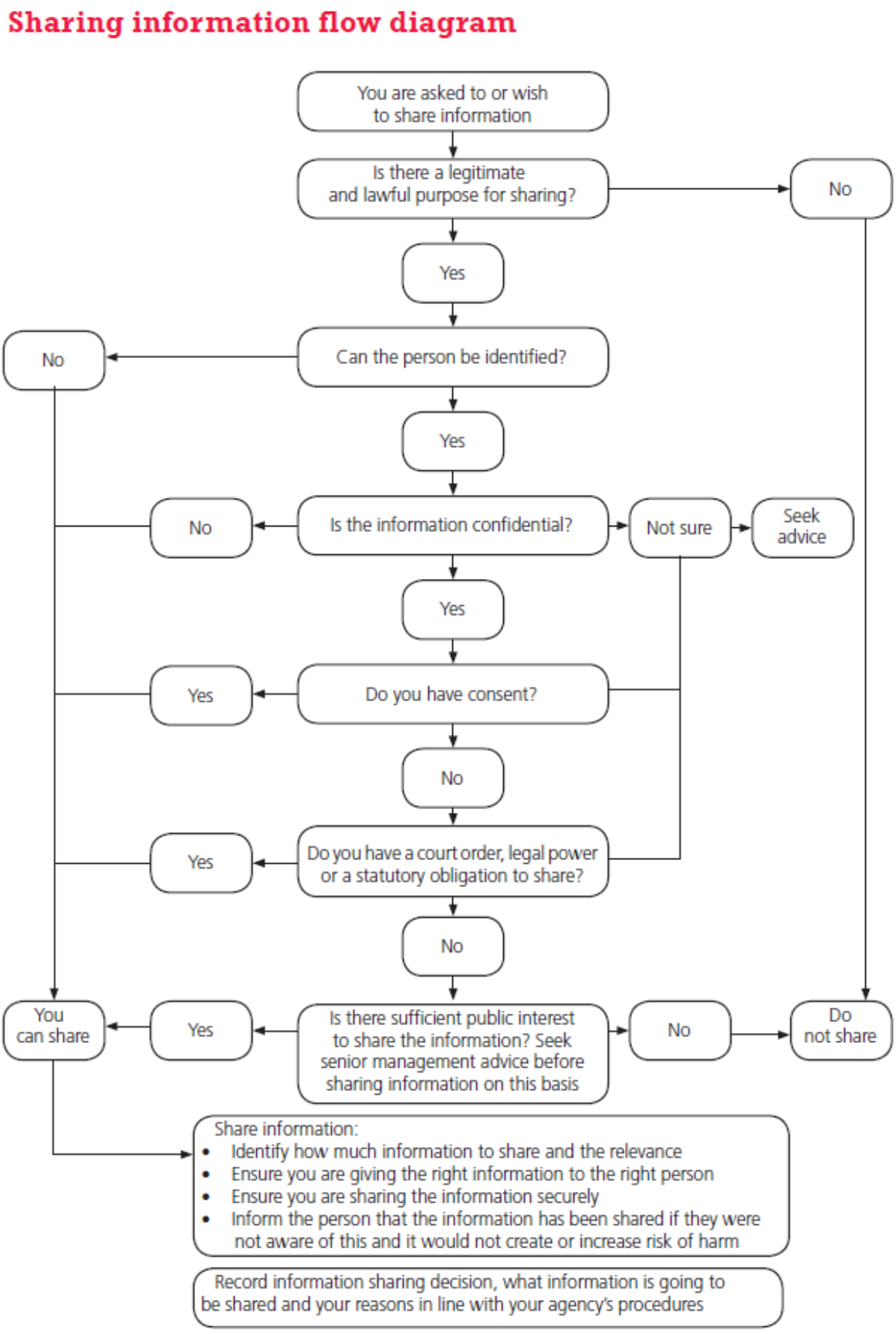
Print Name: ……..……

<u>Witnessed by</u>

Signed: ……..…… Date: ...…….....

Print Name: ……..……

Appendix 8 – Example of a sharing information flow diagram



Appendix 9 - Example of a Record of Disclosure formConfidential Record of Disclosure

Service user name	
Service user date of birth	
Local record identifier	
NHS number (if relevant)	
Description of data disclosed	
Reason for disclosure	
Recipient(s) of the data	
If disclosure is made without	
consent, please state reasons	
Reasons for refusal/limited	
disclosure (if appropriate)	
Disclosing organisation	
Disclosed by	
Authorised by	
Date of disclosure	

A copy of this disclosure record should be retained on the service user's file.

Appendix 10 – Useful websites and guidance

Data Protection Act 1998
http://www.legislation.gov.uk/ukpga/1998/29/contents

Health and Social Care (Safety and Quality) Act 2015
http://www.legislation.gov.uk/ukpga/2015/28/contents/enacted

Health & Social Care Information Centre – Information sharing
http://systems.hscic.gov.uk/infogov/iga/resources/infosharing
Includes a guide to The Health and Social Care (Safety and Quality) Act 2015 and other guidance to support sharing.

Health & Social Care Information Centre – Information Governance support and guidance
http://systems.hscic.gov.uk/infogov

Information Commissioner's Office – guidance for organisations
https://ico.org.uk/for-organisations/

Information Commissioner's Office – key definitions
https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/

Information Governance Alliance – *Enabling information sharing: a user's map for health and social care* (Draft for consultation, Oct 2015)
http://systems.hscic.gov.uk/infogov/iga/consultations/nhsenframework.pdf

Information: To share or not to share - The Independent Information Governance Oversight Panel's report to the Secretary of State for Health (Jan 2015)
https://www.gov.uk/government/publications/iigop-annual-report-2014
This is the first annual report of the Independent Information Governance Oversight Panel, chaired by Dame Fiona Caldicott. It looks at whether health and social care organisations are sharing information wisely and preventing improper disclosure of personal data.

Information: To share or not to share? The information governance review (2013)
https://www.gov.uk/government/publications/the-information-governance-review
Dame Fiona Caldicott's independent review of information sharing, aimed at ensuring that there is an appropriate balance between the protection of patient information and the use and sharing of information to improve patient care.

Appendix 11 - Glossary

Anonymised data – information from which in practice the data subject cannot be identified by the recipient of the information, and where the theoretical probability of the data subject's identity being discovered is extremely small

Aggregated data – data which has been reduced to such an extent that it is no longer possible, by any means, to identify any individual. Typically this will include information for statistical returns at both local and national level.

Caldicott Guardian – is the representative responsible for agreeing and reviewing internal protocols governing the protection and use of patient-identifiable information by the staff in their organisation.

Confidentiality – respect for the privacy of information - one of the principles that underpin all health and social care practice. Information about a person is generally held under legal and ethical obligations of confidentiality. With certain important exceptions, information provided in confidence must not be used or disclosed in a form that might identify the person concerned without their consent.

Common law duty of confidentiality – a common law duty of confidentiality is owed to individuals who have been told that a matter will be dealt with in confidence or have discussed a matter under circumstances in which they might reasonably expect that it would remain confidential. This duty can only be broken if the public interest requires it. Statutory provisions on disclosure override common law provisions.

Consent – is one of the lawful bases for processing patient data. As long as you have given patients a fair choice that they understand (called informed consent) about how you will use their data if they say "yes", then it is a solid base to support the use of data. Consent is applicable to the Data Protection Act as well as the common duty of confidentiality. Remember, consent cannot be overridden in most instances (you cannot give people a choice then say "we have found a basis in law and are going to do it anyway") and can be withdrawn. Explaining to patients the benefits and consequence of both consent (saying "yes") and dissent (saying "no") is crucial.

Explicit consent – can be given in writing or orally (and then recorded) agreeing that information can be used purposes described.

Implied consent – is where the person has been informed about the information to be shared, the purpose for sharing and that they have the right to object; their agreement to sharing has subsequently been signalled by their behaviour rather than orally or in writing.

Data – is information recorded in a form in which it can be processed automatically in response to instructions; information recorded as part of a relevant filing system or an accessible record.

Data controller – a person who (alone, jointly or in common with other persons) determines the purposes for which and the manner in which personal data is processed.

Data Protection Act 1998 – the main UK legislation which governs the handling and protection of information relating to living people.

Data sharing – the disclosure of data from one or more organisations to a third party organisation(s), or the sharing of data within an organisation. Sharing can take the form of systematic, routine data sharing where the same data sets are shared between the same organisations for an established purpose; and exceptional, one off decisions to share data for a range of purposes.

Data (personal) – anything which is capable of identifying a living individual, e.g. name, address, CCTV image, telephone call recording, e-mail address, postcode, photograph etc.

Sensitive personal data – information about:

- racial and ethnic origin
- political opinions
- religious beliefs
- physical and mental health
- sexual life
- trade union membership
- criminal convictions and proceedings.

De-personalised data – is data about an individual from which all personally identifying information has been removed, including any unique identifiers such as a computer reference number.

Data processing – this has a very broad definition and includes:

- obtaining, recording or holding information or data
- organisation, adaptation or alteration of data
- retrieval, consultation or use of data
- disclosure of data
- alignment, combination, blocking, erasure or destruction of data

Data subject – a person who is the subject of personal data:

- they must be a living individual
- they need not be a UK national or resident
- organisations cannot be data subjects

Disclosure – this is the divulging or provision of access to data.

Duty of confidentiality – everyone has a duty under common law to safeguard personal information.

Fair processing – is a term that comes from the Data Protection Act. The first requirement of the Act is being fair and lawful in our use of patient data. That means telling them who we are and what we are doing with their data. We have to do this in a way that they understand. The Information Commissioner's Office (ICO), see below, refers to this process as 'Privacy Notices' but the concepts are rooted in the same law. Patient Notification (not patient communication) is a subtly different concept that relates to Section 251 applications (and the Regulations which permit the lawful flow of data when the Secretary of State approves).

Fair Processing Notice (also called Privacy Notice) – this is issued to children, young people, adults and their families to inform them what information is being collected and recorded about them, the reasons for doing so, under what circumstances it might be shared and why, and their right of access to the data.

Information Commissioner – the independent public official who reports to Parliament and whose principal duty is to enforce DPA 1998 and to educate organisations, businesses and individuals about the legislation.

Information Commissioner's Office (ICO) – is the regulator (they judge whether organisations are meeting both the letter and the spirit of the law) for Data Protection and Freedom of Information. They provide useful guidance on understanding the Data Protection Act and implementing Fair Processing or Privacy Notification as they call it. Remember, while the ICO have a view of "lawful" processing, this focuses on the Data Protection Act and they are not the ombudsman for the common law duty of confidentiality (there isn't one). The ICO will take account of the requirements of the Human Rights Act (HRA) and the Common Law duty of confidentiality, when determining what is lawful and fair.

Lawful basis – in order to use patient data (both the confidential data and that without a duty of confidentiality) organisations must have a lawful basis. For health data the standard is set by the Data Protection Act (statute), the common law duty of confidentiality (set by precedent and expectations) and the Human Rights Act (statute). This same standard will also often apply to social care data. For health and social care, this is a high standard for using patients' data. Using patient information well starts at the point where patients give us their information and what we tell them, at that time, about how we'll use it.

Need to know – sharing of information should only be with those who need to know and, even then, only the information that is actually required to provide any appropriate service.

Privacy impact assessment (PIA) – is a comprehensive process for determining the privacy, confidentiality and security risks associated with the collection, use and disclosure of personal data.

Public Interest – is the interest of the community as a whole, a group within the community, or an individual other than the data subject.

Purpose – the use / reason for which information is stored or processed.

Recipient – the person(s) to whom the data is disclosed.
Definitions have been drawn from the draft Information Governance Alliance guidance *Enabling information sharing: a user's map for health and social care* (http://systems.hscic.gov.uk/infogov/iga/consultations/nhsenframework.pdf; consulted upon in October 2015 and due to be published this year), and Essex Partnership's *Information Sharing Protocol Standard No 8 - Glossary of Terms* (http://www.essexpartnershipportal.org/content/information-sharing-protocol-standard-no-8-glossary-terms).

Appendix 12

Organisations signed up to this Framework as at 9th February 2016

Organisation	Information governance generic contact points
Portsmouth City Council	foi@portsmouthcc.gov.uk
NHS Portsmouth Clinical Commissioning Group	SOUTHCSU.IG-Enquiries@nhs.net
University of Portsmouth	Adrian Parry, Director of Corporate Governance
Hampshire Constabulary	Information.management@hampshire.pnn.police.uk
Portsmouth Hospitals NHS Trust	James Taylor, Information Governance Manager
Solent NHS Trust	SNHS.SolentIGTeam@nhs.net

Organisations intending to sign up to this Framework as at 9th February 2016

National Probation Service	Sarah Beattie
Purple Futures (Hampshire Community Rehabilitation Company)	Barbara Swyer