

Hampshire & Isle of Wight HEALTH AND SOCIAL CARE INFORMATION SHARING FRAMEWORK

(Version 2.20 September 2016)

Contents

	Section	Page
1	Introduction	3
2	Purpose of the Framework	3
3	Parties to the Framework	4
4	Endorsement	4
5	Effective Date of the Framework	4
6	Structure of Information Sharing between Parties	4
7	Purposes of Operational Agreement	5
8	Information Sharing Covered by the Framework	5
9	Legal Framework	5
10	Notification Under the Data Protection Act 1998	5
11	Fair Processing	6
12	Data Controllers and Data Processors	6
13	Consent	6
14	Information Security Measures	7
15	Complaints	7
16	Staff Awareness	7
17	Subcontractors	7
18	Monitoring	8
19	Non Compliance	8
20	Review of the Framework	8
21	Local Information Sharing Agreement Template	8
22	Equality & Diversity	8
	Appendix A - Government Guidance 'Golden Rules of Sharing'	10
	Appendix B - List of Information Governance Network Contact Details	10
	Appendix C - Privacy Impact Assessment Template	10
	Appendix D - Local Operational Agreement Template	10
	Appendix E – List of Organisations (the parties) who agree to be bound by the Framework	11
	Appendix F – List of the GP practices which have signed the Framework	11
	Appendix G – Table of Legislation	11

1 Introduction

Many organisations are responsible for the provision of a wide range of services to the public which are often undertaken in co-operation with other organisations. One of the most vital resources in accomplishing this is the common availability of relevant information. Whilst there is a public expectation of appropriate sharing of information between organisations providing services to them, the public rightly expect that their personal data will be properly protected. When sharing personal information, organisations must ensure that the Principles of the Data Protection Act 1998, the Human Rights Act 1998, Caldicott Principles (for Health and Social Care) and recommendations contained within the Caldicott Review 2013 and 2016, Freedom of Information Act 2000, Section 22 of the Gender Recognition Act 2004 and the common law duty of confidentiality are upheld.

The members of this group all abide by the legislation referred to in the table in Appendix G

The effectiveness of information sharing relies on good relations and mutual trust but must also comply with legislative, regulatory and ethical demands and needs to be carried out in a consistent manner by all the parties involved. This Framework (“the Framework”) provides the basis for facilitating the exchange of information between the organisations concerned where it is necessary or expedient under the terms of any legislation in order to provide services in the most effective and appropriate way.

It is recognised there will be additional local level information sharing between organisations that are not signatory to the Framework e.g. third party providers; these will be covered by operational agreements. Local operational agreements should be preceded or supported by completion of a Privacy Impact Assessment, an example of which can be found in Appendix C.

To support the Framework guidance can be found in the Appendices of this document.

- DoH Seven Golden Rules of Information Sharing Appendix A
- List of Information Governance Contact Details Appendix B
- Privacy Impact Assessment Template Appendix C
- Local Operational Agreement Template Appendix D
- List of the organisations (the parties) who agree to be bound by the Framework Appendix E
- List of GP Practices who agree to be bound by the Framework Appendix F
- List of legislation – Appendix G

2 Purpose of the Framework

The purpose of the Framework is to facilitate the appropriate exchange of information in order to fulfil the duties imposed upon public authorities and other parties. The Framework is intended to give the participating parties the confidence that when they share information, all parties will be operating to a common standard that complies with relevant legislation and guidance. The Information Governance Network (IGN) is responsible for review and monitoring of this Framework, the group being facilitated by NHS South, Central and West Commissioning Support Unit.

The IG Network will work with the Information Governance Alliance, hosted by NHS Digital and refer to its Information Sharing Map.

3 Parties to the Framework

Many organisations in particular in the NHS and Adult Social Care are able to demonstrate that they have put the required Information Governance framework in place by means of their IG toolkit (IGT), and are achieving an adequate level of performance against these requirements and can be regarded as 'Trusted Organisations' for information sharing purposes where the purpose of sharing is the delivery of care. The parties to the Framework will either have reached a Level 2 'satisfactory' compliance ' within the current IGT or are working towards this with a formalised action plan. The IGN will annually review the parties' compliance with the Toolkit and check that they have submitted a signed IG Assurance Statement. Parties that are unable to demonstrate assurance will have the opportunity to provide other assurance to the IGN for consideration.

Wessex LMC represents GP practices in Hampshire and Isle of Wight. GP practices and the LMC are well aware of the issues around IT and information governance and welcome this work on guidance for information sharing across providers.

Appendix E lists the organisations ("the parties") who agree to be bound by the Framework:

4 Endorsement

The Framework will be signed by the Caldicott Guardian or equivalent from each of the parties who is authorised to endorse the whole of the Framework and commit the organisation.

5 Effective Date of the Framework

The Framework shall become effective at the point at which it is endorsed by an authorised signatory on behalf of the organisation. It will be the responsibility of each organisation who signs the Framework to advise the other signatories of the effective date.

6 Structure of Information Sharing between the Parties

The Framework will be supported and adhered to by local operational agreements.

- Information Sharing Framework – The parties will adhere to the high level overarching binding agreement setting out the relevant principles
- Operational agreement – Practical implementation of the Framework stating precisely the specific services between whom information is to be shared, the data classes of the relevant information, the exact purposes of sharing the information, the legal basis for the disclosure and how the sharing is to be controlled

Specified people at senior level will assume responsibility for the implementation and control of information sharing defined by operational agreement(s) relative to their management area. These people should also be a source of advice to employees of their organisation. It would be appropriate for the Caldicott Guardian or a person equivalent in seniority in each organisation within this agreement to perform this role.

7 Purposes of Operational Agreements

In respect of each information sharing agreement, information will be disclosed or shared only for the specific purpose(s) defined in the relevant operational agreement, taking into account any restrictions placed upon disclosure by the data subject(s) concerned. Information received will not be used within the receiving organisation for any other purpose than that agreed or required by law.

The parties confirm that they will take appropriate action to deal with staff that use or further disclose information in contravention of the terms of the operational agreement under which the information was received.

8 Means of Information Sharing Covered by the Framework

The Framework covers all sharing of personal information created, collected, stored or transmitted in any format or media type e.g.:

- paper
- microfiche
- video or audio recordings
- electronically
- verbally
- text or images
- It also extends to information known to individuals under the control of any of the parties even if not physically recorded

(This list is not exhaustive).

This Framework also provides the platform for the continued development and implementation of new models of care. Each development will be assessed using the Privacy Impact Assessment process, and detailed via the Operational Agreement.

9 Legal Framework

The parties confirm that they will comply with all relevant legislation (including secondary legislation) currently in force or subsequently enacted in particular the Data Protection Act. The legal basis for processing and sharing personal and personal sensitive information must be established under conditions set out in Schedules 2 and 3 of the Data Protection Act. In fulfilling this obligation, the parties will take into account any official supportive guidance for example The Health & Social Care Record Guarantees and in particular the data sharing code of practice issued by the Information Commissioner's Office published under section 52 of the Data Protection Act. Although the code does not impose additional legal obligations nor an authoritative statement of the law, the code can be used in evidence in any legal proceedings not just under the Data Protection Act. In addition and where applicable the parties confirm that they will adhere to the Caldicott principles and the common law duty of confidentiality.

10 Notification under the Data Protection Act 1998

The parties hereby confirm that their Notifications under the Data Protection Act 1998 will be kept up to date.

11 Fair Processing

When obtaining personal information from a data subject, the parties shall ensure that the following fair processing information is made readily available:

- The identity of the data controller
- The identity of any nominated representative for the purposes of the Act
- The purpose(s) for which the data will be processed
- Any further information necessary, taking into account the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair. Examples of further information are the likely consequences of the processing and whether the personal data may be disclosed to a third party

12 Data Controllers and Data Processors

The identity of the Data Controllers and Data Processors must be established before information may be shared. A Data Controller is a person or organisation who (either alone or jointly or in common with other persons/organisations) determines the purposes for which and the manner in which any personal data are, or are to be, processed. In relation to data controllers, the term jointly is used where two or more persons (usually organisations) act together to decide the purpose and manner of any data processing. The term in common applies where two or more persons share a pool of personal data that they process independently of each other

A Data Processor means any person or organisation (other than an employee of the data controller) who processes the data on behalf of the data controller. Data processors are not directly subject to the Act. However, most data processors, if not all, will be data controllers in their own right for the processing they do for their own administrative purposes, such as employee administration or sales.

Data controllers remain responsible for ensuring their processing complies with the Act, whether they do it in-house or engage a data processor. Where roles and responsibilities are unclear, they will need to be clarified to ensure that personal data is processed in accordance with the data protection principles. For these reasons organisations should choose data processors carefully and have in place effective means of monitoring, reviewing and auditing their processing

13 Consent

Where the individual's consent (in particular with regard to sharing information) is to be relied on as the basis for any processing of personal data, the fair processing information given must be sufficient to allow the individual to make an informed decision whether or not to give consent or to place any restrictions on that consent. Data subjects should be informed that, save as required or permitted by law, their preferences regarding disclosure will be observed. Consent obtained under duress or on the basis of misleading information will not be valid. It is recognised that some individuals may require additional support in order to give informed consent and this will be provided by parties to the framework as required (for example access to a foreign language or sign language interpreter, or easy read information for people with a learning disability, under the Accessible Information Standard).

14 Information Security Measures

The parties shall have appropriate technical and organisational measures in place to protect the confidentiality, integrity and availability of the information during all stages of processing. It is envisaged that each party will adhere to common standards for information security.

Each party shall have formal procedures to:

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

15 Complaints

The parties to the Framework will put in place efficient and effective procedures to address complaints relating to the disclosure or the use of personal information that has been provided under any operational agreement to the Framework.

In the event of a complaint relating to the disclosure or the use of an individual's personal information that has been supplied or obtained under the Framework, the parties will co-operate and assist as appropriate in resolving the complaint.

16 Staff Awareness

The parties hereby make a commitment to train staff appropriately via the [IG Training tool](#) or face to face or other online training approved by the appropriate body to ensure that they understand their responsibilities regarding the protection of personal data and the circumstances in which personal data may be shared. Additionally there is a requirement for some organisations to achieve 95% of its entire staff to be trained in information governance.

17 Subcontractors

In the event that any of the parties, as a data controller, engages a sub-contractor to process information covered by the Framework:

- The subcontractor whenever processing information must be required to provide sufficient guarantees in respect of the technical and organisational security measures
- The data controller must take reasonable steps to ensure compliance with those measures
- The processing must be carried out under a contract evidenced in writing which requires the subcontractor to act only on instructions from the data controller and to comply with obligations equivalent to those imposed on a data controller by the Seventh Principle of the Data Protection Act 1998

As required by the data controller a specific confidentiality agreement should be put in place

18 Monitoring

Each party shall have in place mechanisms to monitor compliance with the terms of the Framework and supporting operational agreements. The Caldicott Guardian and/or Senior Information Risk Owner (SIRO) or equivalent shall be responsible for ensuring that information sharing is monitored.

19 Non Compliance

Instances of non-compliance with this Framework and associated Operational Agreements will be reported to the Caldicott Guardian and/or SIRO in respective organisation(s). Each incident will be dealt with promptly in accordance with agreed information governance / operational policies and procedures.

In addition, where non-compliance is likely to amount to professional misconduct as defined by an appropriate regulatory body; then it is expected that it will be reported to that regulatory body.

Any contracts or service level agreements between parties must make provision for dealing with incidents of non-compliance in line with this framework.

20 Review of the Framework

It will be the responsibility of the IGN to review this framework annually or sooner if required and republished on a three year cycle. Each party shall raise with the relevant signatories any issues that may affect the Framework.

An amendment may be recommended by any party but must be agreed by the IGN and formally documented before coming into force. Thereafter the Framework will operate as amended and the supporting operational agreement(s) will take the amendments into account. Each signatory will ensure that changes are promulgated throughout his/her organisation.

21 Local Operational Sharing Agreement Template

A template for completing a local operational agreement detailing the detailed operational arrangements for a specific information sharing process between signatories to this Framework is enclosed at Appendix E.

22 Equality and Diversity

Most parties to this information sharing framework have a legal duty under the Public Sector Equality Duty to have due regard to the need to eliminate unlawful discrimination, promote equality of opportunity, and foster good relations between people of diverse groups. This duty has a number of implications for the way this framework is implemented:

- So that health and social care organisations can meet their proactive duty to make reasonable adjustments for people with a disability, parties to this framework will ensure that relevant information about a patient's or carer's disability is shared so that equality of access and outcome can be facilitated
- Parties will have due regard to the NHS England Accessible Information Standard <http://www.england.nhs.uk/ourwork/patients/accessibleinfo-2/>

- That patients, service users, or carers may be asked to identify their protected characteristics by way of an anonymous equalities monitoring questionnaire so that the service provider can monitor equality of access and outcomes for diverse communities

Under Section 22 of the Gender Recognition Act 2004 *'It is an offence for a person who has acquired protected information in an official capacity to disclose the information to any other person.*

Appendix A

Seven **Golden Rules** for Information Sharing

1. **Remember that the Data Protection Act is not a barrier to sharing information** but provides a framework to ensure that personal information 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 information 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 information. You may still share information without consent if, in your judgement, that lack of consent can be overridden in the public interest. You will need to base your judgement on the facts of the case.
5. **Consider safety and well-being:** Base your information sharing decisions on considerations of the safety and well-being of the person and others who may be affected by their actions.
6. **Necessary proportionate, relevant, accurate, timely and secure:** Ensure that the information 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 information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

Appendix B - Information Governance Contact Details



Appendix B to
Information Sharing F

Appendix C – Example of a Privacy Impact Assessment Template



20170327 PIA
Template v2.0 approved

Appendix D – Example of a Local Operational Sharing Agreement Template



Appendix D -
Example of Operator

Appendix E – List of the Organisations which have signed or are in the Process of Signing the Framework



APPENDIX E to
Health and Social Car

Appendix F - List of the GP Practices which have signed or are in the Process of Signing the Framework



Appendix F -
Register of Signatory

Appendix G – Table of Legislation

Access to Health Records Act 1990
Access to Medical Reports Act 1988
Computer Misuse Act 1990
Crime and Disorder Act 1998
Criminal Justice and Immigration Act 2008
Data Protection Act 1998
Freedom of Information Act 2000
Health and Social Care (Safety and Quality) Act 2015
Human Rights Act 1998
Privacy and Electronic Communications Act 2000
Protection of Children Act 1999
Regulation of Investigatory Powers Act 2000

Additional Guidance:

Organisation	Website
IG Toolkit	https://www.igt.hscic.gov.uk/
Information Commissioner	https://ico.org.uk
NHS Digital	digital.nhs.uk
IG Training Tool	https://www.igtt.hscic.gov.uk/igte/
Information Governance Alliance	http://systems.digital.nhs.uk/infogov/iga