Information Sharing Agreement

between

Isle of Wight NHS Trust (The Trust)

and

The Isle of Wight Council (IWC)

Table of Contents **Page**

1. Version control.

Protocol Version	Agreement Version	Date	Author	Comment
1.0	1.0	4/4/2013	Tony Martin	
1.1	1.1	29/4/13	Tony Martin	
1.2	1.2	23/4/13	Tony Martin	
1.3	1.3	30/11/2015	Irene Woodford/Julie Adams	

2. Owner/Contact Details (who manages the agreement)

Tony Martin
Information Governance Lead Officer
Isle of Wight NHS Trust

Telephone: 01983 822099 [redacted]
Standard Email: tony.martin@iow.nhs.uk
Secure NHS Mail: tonymartin1@nhs.net

3. Legal basis of this agreement

This agreement is between partner services external to the Trust and therefore each organisation's own Data Protection Act notification applies, and ensures that there is a legal basis for the sharing of the agreed information.

The Data Controllers for this agreement are the Isle of Wight NHS Trust and the Isle of Wight Council

This agreement is also based on the contents of the NHS Act 2006, particularly section 82 covering co-operation between NHS bodies and local authorities.

The NHS and Government's Caldicott Regulations also apply. Caldicott Guardians are responsible for the establishment of procedures governing access to and the use of Person Identifiable Data (PID) within the Isle of Wight Council, and where local flexibilities exist, the transfer of such information from the organisation to other bodies. In agreeing local procedures and policies, the Caldicott Guardians will ensure consistency with any relevant central requirements and guidance.

Fair Processing Information

The partners to this agreement recognise their responsibilities under the Data Protection Act 1998 to provide a fair processing notice to individuals. The sharing of information under this agreement is covered by existing fair processing notices published by the partners to this agreement.

4. Scope of sharing purpose

To enable effective and safe joint working between IWC and The Trust

This service is provided to service users by staff from the Isle of Wight NHS Trust (Trust) and Isle of Wight Council (IWC) either jointly or separately. The services are located in a variety of different work based locations and will also include remote community working. Professionals from both organisations must have access to up-to-date information about service users in order to support;

- effective intervention where a number of professionals contribute to overall care and treatment
- safe working where lone workers are at risk
- safe risk management where service users, carers or public are at risk
- streamlined, aligned and effective service to service users

Extent and type of information to be shared –
The information will be recorded and used by staff from Adult Social Services and IOW NHS Trust from both organisations.
The information will include PID including demographic and sensitive clinical information about individual service users.

5. Privacy Impact Assessment

Prior to drawing up this agreement the partner organisations are required to complete (jointly or separately) a Privacy Impact Assessment (PIA) covering this exchange of information.

A template to be used for this process is attached as a separate document.

6. Summary Description of Process/Pathway

Staff from the IWC will have access to relevant information stored by NHS colleagues on the PARIS patient record system which will be accessed as appropriate.
IWC staff will record information on the PARIS system, which will be accessed by NHS colleagues as appropriate.

IWC Service staff will have access to relevant historical information stored on the SWIFT client record system for the foreseeable future in order to make informed decisions due to the fact that this information will not be migrated to their PARIS system.

7. Relevant Policies and Guidance – (further details in Appendix A)

- Data Protection Act 1998
- Human Rights Act 1998
- Computer Misuse Act 1990
- Mental Health Act 1993

- Mental Capacity Act 2005
- The Carers (Recognition & Service) Act 1995
- The Common Law Duty of Confidentiality
- Care Records Guarantee
- Social Care Records Guarantee
- Information Governance and Risk Policy
- Information Security Management: NHS Code of Practice
- Confidentiality: NHS Code of Practice
- Records Management: NHS Code of Practice Part 1 and 2
- The Caldicott Principles
- IWC Data Protection Policy
- IWC Records Retention Policy
- IWC Access to Information Policy
- IWC Protective Marking Policy
- Acceptable Use Policy

8. Security & Risk Management

Both organisations will be jointly responsible for the safe transfer, storage and retention of the shared information provided. Responsibility for data sharing will be appropriately managed in accordance with the Data Protection Act 1998 and adhering to local policy and procedures for information transfers.

The security and access of the information is the responsibility of the relevant partner requiring the information and it must not be copied or transferred into any other media or disclosed to anyone outside of the remit of the agreement without approval from the agreement owner.

The designated employees of the contracted services who will have access to the information will abide by the security and data management restrictions as defined within section 7 – Relevant Policies and Guidance

- All manual records will be subject to both parties respective Records Management policies and processes
- Any information held electronically will be transferred via the NHS and local authority secure private fibre link by secure e-mail or in accordance with the IWC Protective Marking Policy
- The Local Authority will exchange all information in accordance with the IWC Protective Marking Policy. For example, where personal data is included, the loss of which may cause harm to an individual(s). This will be marked as “PROTECT – PERSONAL”.
- The Isle of Wight NHS Trust does not currently have a Protective Marking Policy

in place however will respect any documents that they receive that are protectively marked accordingly.

- All staff who have direct contact with service users, will have appropriate access to manual records, PARIS and SWIFT. All staff with access to these are subject to the Acceptable Use Policy.

All NHS staff must complete the appropriate mandatory Information Governance Training module via Training Tracker.

All Local Authority staff must complete The Corporate Information Governance training.

9. Consent

Information will only be shared if:

a) the purpose for the sharing has been explained to the client and the client has either given consent or

b) that there is a legally justified purpose for sharing without consent as defined within the DPA 1998

10. Requests for Information

The Trust and the IWC have clear guidelines on their respective intranets and websites on 'How to make an information request' and 'How to recognise and process an information request'. This applies for:

- Freedom of Information
- Environmental Information Request
- Data Protection Act
- In addition the Trust may also process requests under The Access to Health Records Act 1990.

The information that is processed on PARIS will include information from Trust and IWC staff. However, each organisation is separately responsible as the Data Controller for the information. Any Subject Access Requests (SARs) or Freedom of Information (FOI) requests received under any of the Acts must therefore take all usual data protection considerations into account.

11. Sharing Criteria

As Section 4. Scope of sharing purpose summary' :

IWC will be permitted access to relevant information stored by NHS colleagues on the PARIS patient record system.
IWC staff will record information on the PARIS system, which can then be accessed by NHS colleagues.

Due to the fact that not all historical information will not migrated to the PARIS system IWC staff will in addition be able to access relevant and proportionate historical

information stored on the SWIFT client record system for the foreseeable future in order to make informed decisions.

Access to information will be authorised on a role based basis in order to support contact with service users, carers and other professionals.

a) **Demographic and assessment information -** shared with all staff within the Trust and Local Authority's Mental Health Services who have legitimate access in order to carry out their function within their respective organisations. The teams would consist of :

IWC Teams	IOW NHS Trust teams

12. Information to be Shared:

PID and sensitive personal data as defined within the Data Protection Act 1998 will be required for the purpose of this agreement.

Owing to the variety of legitimate purposes that the information will be shared it is not possible to list specific details within this agreement, however in line with the Data Protection Act any information shared must always be justified and proportionate for the purpose.

13. Network Connectivity Utilised

IOW NHS Trust Network and IW Council Network

The link between the IOW NHS Trust network and the IW Council network is a secure private fibre link.

There are aspects of the Council network (the BT LES circuits (Lan Extension Service)) which are less secure. These will be strengthened when the Council complete migration to Office 2010 which implements Transport Layer Security (TLS).

The alternative route for secure emails is the nhs.net to gcsx.gov.uk which provides secure connection to government / local government agencies.

14. Applicable Controls:

All PARIS users will receive appropriate training to their role.

Controls in place will include

- Role based access
- User name
- Password

15. Specific Sharing Constraints

This agreement must operate within the constraints of the purposes listed within this document in order for the lawful sharing of the information to exist.

16. Information Risk Ownership

Each service must appoint a Designated Point of Contact

For the Council this role will be fulfilled by the Corporate Information Unit (CIU).

For the Trust this role will be the Information Asset Owner/Administrator (IAO/IAA) for the relevant department.

The function of these roles will be to assume responsibility for data protection, security and confidentiality and compliance with all relevant legislation. Specific responsibilities are as follows but not limited to:

- Ensuring that all sections of this agreement are adhered to.
- Ensuring that all designated officers and other staff are fully aware of their responsibilities.
- Ensuring the agreement is accurate, up to date and adequate for the purpose for which it is intended.

The CIU - for the IW Council - and the Information Governance Lead Officer - for the NHS - will provide governance advice and guidance where appropriate particularly in the review of this agreement and with regard to any potential information governance related incidents.

17. Breach and Escalation Rules

Any data breaches or Information Governance related incidents must be reported by

the Trust on the DATIX incident reporting system. Any incident involving IWC data must be reported to the Corporate Information Unit.

All incidents will be investigated in line with the incident reporting policies of each partner agency. For NHS incidents the Information Governance Lead Officer will determine the appropriate IG grading in line with the HSCIC (Health & Social Care Information Centre) Guidance. Where it is determined that the incident is an Information Governance (IG) level 2 or above, the Head of Nursing & Quality in the relevant Clinical Business Unit must be notified, so that a decision can be made as to whether the incident is SIRI reportable. under the Serious Incidents Requiring Investigation (SIRI) procedure..

18. Complaints

Each partner organisation is responsible for any complaints or appeals process.

The CIU or the appropriate IAO/IAA for each agency must be notified immediately of any of the above.

For the NHS, all complaints must be acknowledged in writing and dealt with under the NHS Complaints procedure.

For the Council, all complaints must be acknowledged in writing within two days and, wherever possible, dealt with within twenty eight days. Any disciplinary proceedings will be implemented according to the IW Council's policies.

19. Data Quality

PID must only be collected using approved and agreed collection methods, ensuring that the required information is complete, accurate and up to date.

All reasonable steps must be taken to ensure that anyone who has received information is notified of any relevant changes and if any inaccuracies are found that all amendments required are made

20. Retention and Disposal

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

NHS Records will be retained in line withRecords Management Code of Practice for Health and Social care 2016

Council records will be retained in accordance with the Council's Records Retention Policy.

21. Audit and Review Date

To be reviewed twelve months after the date of signing of this agreement and annually thereafter.

22. Closure or termination of agreement

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

This agreement may be terminated if there is a serious breach of confidentiality, e.g. where information provided under this agreement is used for purposes other than set out in this agreement or information is passed to a third party other than with the agreement of the agreement owner.

The CIU and IAO/IAAs must exercise caution when processing information specified within this agreement and whether their decision will stand up to scrutiny at a later stage. This should not, however, be a barrier to the disclosure of information in appropriate circumstances, but will necessitate maintaining records of disclosure and the justification. It is the responsibility of the CIU and IAO/IAAs to review this agreement. Initially this will be twelve months after the date of signing this agreement, and then annually thereafter to ensure that information is being processed in the correct manner.

23: Parties & Signatures

_____ _____

Name **Information Asset Owner** **Date**

Isle of Wight NHS Trust

_____ _____

Name **Caldicott Guardian** **Date**

Isle of Wight Council

24. Appendix A

24.01 NHS Act 2006 (S75 and S82 Partnership Arrangements)

New powers to enable health and local authority partners to work together more effectively came into force on 1st April 2000. These were outlined in Section 31 of the 1999 Health Act. These partnership arrangements were applicable for health bodies, such as Strategic Health Authorities, Primary Care Trusts, (now replaced by Commissioning Support Units and Clinical Commissioning Groups) together with any health-related local authority service such as social services, housing, transport, leisure and library services, community and many acute services.

Section 31 of the Health Act 1999 has since been repealed and replaced, for England, by Section 75 of the National Health Service Act 2006, which has consolidated NHS legislation. The Act provides funding so that partnerships can be formed to provide efficient services between the NHS and Social Care. It permits the exchange of information to assist with the arrangements, but does not say what information, nor how the exchange should be managed. Section 82 covers co-operation between NHS bodies and local authorities in order to secure and advance the health and welfare of England and Wales.

24.02 The Data Protection Act 1998

Data Protection Principles

Anyone processing personal data must comply with the eight enforceable principles of good practice. They say that data must be:

a) Fair and lawful

   Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless certain conditions are met. Also the processing must adhere to the fair processing code

b) Use for specified purposes

   Personal data shall be obtained only for one or more specified purposes, and shall not be further processed in any manner incompatible with that purpose or purposes.

c) Adequate, relevant and not excessive

   Personal data shall be adequate, relevant and not excessive in relation to the purpose

d) Accurate and up to date

   Personal data shall be accurate and, where necessary, kept up to date.

e) Do not keep longer than necessary

   Personal data processed for any purpose or purposes shall not be kept longer than is necessary for that purpose or those purposes.

f) Rights given under the act

Personal data shall be processed in accordance with the rights of the data subject under this act.

g) Security appropriate and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data

h) Disclosure outside Europe

Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection.

Personal data covers both facts and opinions about the individual. It also includes information regarding the intentions of the data controller towards the individual, although in some limited circumstances exemptions will apply. With processing, the definition is far wider than before. For example, it incorporates the concepts of 'obtaining', 'holding' and 'disclosing'.

Schedule 2 and Schedule 3 Conditions

Condition for processing personal data is that one condition in Schedule 2 should be met.

Condition for Processing sensitive personal data is one condition in Schedule 2 and a condition in Schedule 3 should also be met.

Schedule 2: Personal Data

Information which relates to a living individual who can be identified from that data, or from that data and other Information which is, or is likely to come into, the possession of the data controller. This includes opinions about the individual and any indications of the organisation's intentions in respect of that individual.

The data subject has given consent, or the processing is necessary for:

- A contract
- Legal obligation
- Protection of the vital interests of the data subject
- Public function
- In the public interest
- A statutory obligation
- Legitimate interests of the Data Controller

Schedule 3: Sensitive Personal Data

Is 'personal data' that contains Information as to an individual's racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical/mental health, sexual life, or criminal offences.

The data subject has given explicit consent, or the processing is necessary for:

- Employment related purposes
- The purpose of, or in connection with legal proceedings
- Protection of vital interests of the individual (where consent cannot be obtained)
- Made public by the data subject
- Substantial public interest
- Prevention or detection of an unlawful act
- Legitimate interests of a non-profit making organisation
- Medical purposes

24.03 Human Rights Act 1998

This Act became law on 2 October 2000. It binds all Trusts and health care professionals treating NHS patients to respect and protect an individual's human rights. This includes an individual's right to privacy (under Article 8) and a patient/individual's right to expect confidentiality of their information at all times. Article 8 of the Act provides that 'everyone has the right to respect for his private and family life, his home and his correspondence'. However, this article also states "there shall be no interference by a public authority with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others". Each organisation must act in a way consistent with these requirements. It must take an individual's rights into account when sharing personal information about them.

24.04 The Common Law Duty of Confidentiality

The Common Law Duty of Confidentiality requires that unless there is a statutory requirement to use Information that has been provided in confidence, it should only be used for purposes that the subject has been informed about and consented to. In certain circumstances, this also applies to the deceased. The duty is not absolute but should only be overridden if the holder of the Information can justify disclosure as being in the public interest i.e. to protect others from harm.

24.05 The Caldicott Principles

The Caldicott Committee (which reported in 1997) carried out a review of the use of

patient identifiable Information. It recommended a series of principles that should be applied when considering whether confidential Information should be shared. All NHS organisations and social services departments are now required to apply the Caldicott principles. These principles relate to the use of patient-identifiable Information and are detailed below:

1. Define Purposes - Every proposed use or transfer of patient-identifiable Information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed, by an appropriate guardian.
2. Use anonymised Information if possible - Patient-identifiable Information items should not be included unless it is essential for the specified purpose. The need for patients to be identified should be considered at each stage of satisfying the purpose.
3. Use the minimum Information necessary.
4. The minimum amount of identifiable Information should be transferred or made accessible that is necessary for a given function to be carried out.
5. Access to personal Information on a need to know basis - Only those individuals who need access to patient-identifiable Information should have access to it, and they should only have access to the Information items that they need to see. This may mean introducing access controls or splitting Information flows where one Information flow is used for several purposes.
6. Staff must be aware of their responsibilities - Action should be taken to ensure that those handling patient-identifiable Information - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.
7. Use only when lawful - Every use of patient-identifiable Information must be lawful.

All Health and Social Services organisations are required to nominate a senior person to act as a Caldicott Guardian responsible for safeguarding the confidentiality of patient Information.

24.06 Computer Misuse Act 1990

This Act makes it a criminal offence to access any part of a computer system, programs and/or data that a user is not entitled to access. Each organisation will adhere to the requirements of the Computer Misuse Act 1990 by ensuring staff are made aware of their responsibilities regarding the misuse of computers for personal gain or other fraudulent activities. Any member of staff found to have contravened this Act would be considered to have committed a disciplinary offence and be dealt with accordingly.

24.07 The NHS Confidentiality Code of Practice

The Confidentiality Code of Practice is to ensure that information given by the patient

is treated as confidential information and only to be divulged on a need to know basis. All staff are obliged to adhere to this procedure.

24.08 The Mental Health Act 1983

The 1983 Act is largely concerned with the circumstances in which a person with a mental disorder can be detained for treatment for that disorder without his or her consent. It also sets out the processes that must be followed and the safeguards for patients, to ensure that they are not inappropriately detained or treated without their consent. The main purpose of the legislation is to ensure that people with serious mental disorders which threaten their health or safety or the safety of the public can be treated irrespective of their consent where it is necessary to prevent them from harming themselves or others.

24.09 Mental Capacity Act 2005

From 1 October 2007 this Act was fully in force in England and Wales. It impacts on all staff working with or caring for adults (16+) who lack mental capacity (or have impaired capacity) to make their own decisions about health, social care and financial matters.

The Act makes clear who has authority to make decisions in certain situations and sets out statutory principles which must guide decision-making.

Doctors have a legal duty to have regard to the Code of Practice in their day to day decisions about the treatment and care of incapacitated patients. So it is important that doctors take steps to familiarise themselves with the legal principles, and the provisions of the Code which are of most relevance to their areas of practice.

24.10 The Carers (Recognition & Service) Act 1995

Carers' needs are recognised in this legislation. It gives the right to have their needs taken into consideration when services are being assessed under the NHS and Community Care Act for an individual they care for.

24.11 Care Records Guarantee

The NHS Care Record Guarantee for England sets out the rules that govern how patient information is used in the NHS and what control the patient can have over this. It is based on professional guidelines, best practice and the law and applies to both paper and electronic records. Whilst not a legal document, the Guarantee could be used as the basis for a complaint.

The NHS Care Record Guarantee includes information on:

- people's access to their own records,
- how access to an individual's healthcare record will be monitored and policed and what controls are in place to prevent unauthorised access,
- options people have to further limit access,
- access in an emergency,
- what happens when someone is unable to make decisions for themselves.

The delivery of joined up care requires effective and accurate sharing of information between health and social care. The NHS Care Record Guarantee for England and the Social Care Record Guarantee for England together form a basis for transparent, legal and secure information sharing.

24.12 Social Care Record Guarantee

Your local authority has a range of duties to support and care for those most in need in the community. To do this we provide a range of services, such as:

- assessing your, or your and your carer's, needs;
- providing care in your home;
- taking steps to protect you if you are at risk of harm;
- paying someone to help care for you;
- supporting you in a residential home; and
- providing a foster carer (if you need one).

To do this, we must hold records about you, your personal circumstances and the care you are receiving or may need to receive in the future.

This guarantee is our commitment that we will use records about you in ways that respect your rights and promote your health and wellbeing.