Information Sharing Agreement

between:

Gloucestershire Care Services – NHS Gloucestershire

Gloucestershire County Council

Document Control

Version History

Issue	Reviewers	Amendments	Date
Draft v1.0	Dee Walker - GCS Kirsty Benzie - GCC	First draft	12.12.11
Draft v2.0	Kirsty Benzie	Second draft	23.02.12
Draft V3.0	Kirsty Benzie Dee Walker	Final draft	13.07.12

Certification

By signing below, the Signatories of the partner organisations accept and agree to be bound by the provisions contained in this Information Sharing Agreement.

Signed
By **[name and position]**
For and behalf of **Gloucestershire County Council**
Date
Data Protection Act 1998 Registration Number:

Signed
By **[name and position]**
For and behalf of **Gloucestershire Care Services (NHS Gloucestershire)**
Date
Data Protection Act 1998 Registration Number

1. Introduction

1.1. This agreement relates to the provision of the Adult Model of Care & Gloucestershire Care Services Support Services Organisational Change Programme, within the context of this agreement Gloucestershire Care Services – NHS Gloucestershire will be the lead health organisation, the lead social care organisation is Gloucestershire County Council.

2. Purpose

2.1 This is an Agreement between the lead Health and Social Care organisations in Gloucestershire as partners to share specified person-identifiable information for the seamless provision of health and social care. This agreement establishes the commitment of health and social care organisations in Gloucestershire to share information to improve the speed and efficiency of health and social care. Specifically for the purposes of:

- Delivering personal Care and treatment
- Assuring and improving the quality of care, treatment and services
- Managing and planning jointly commissioned services
- Joint Strategic Needs Assessment
- Community Profiling
- Health Needs Assessment
- Statistical modelling, analysis and reporting
- Events linkage and/or outcomes
- Risk Management
- Clinical Dashboards
- Community safety partnerships
- Crime and disorder
- Monitoring and protecting public health
- Medical, health or social services research
- Support for clinical governance
- Audit
- Investigating Complaints and notified or potential legal claims
- Contracting for services

2.2 This Agreement has been developed as an operational agreement as established under the terms of the existing overarching Gloucestershire Information Sharing Partnership Agreement (GISPA), for sharing person-identifiable information between partner organisations within Gloucestershire.

2.3 The purpose of this local agreement is to provide a framework for managing the exchange of person-identifiable information in connection with the provision of health and social care, between the participating organisations.

2.4 Operational arrangements for the specific exchanges of person identifiable information to support the purposes identified above, will be detailed in Specific Information Exchange Agreements (SIEA) governed by the Roles & Systems Matrix, which can be found at Appendix 3.

2.5 Section 1 (above) identifies purposes where information may be exchanged under the terms of this Agreement. This does not imply an obligation on partner organisations to exchange information. Such decisions must be made on a case by case basis.

3. Legislation governing and enabling the sharing of Information

3.1 The legal framework for information sharing includes the following areas of law and standards:

- Human Rights Act 1998
- Data Protection Act 1998
- Common Law duty of confidentiality
- Caldicott Principles
- Freedom of Information Act 2000
- Local Government Act 2000

See Appendix 1 for a more comprehensive summary

3.2 The Data Protection Act states that personal data must be processed fairly. Organisations must therefore ensure that individuals are given an explanation of how their data will be used, including details of disclosures to other individuals or organisations.

3.3 Where parties to this Agreement collect personal data directly from individual patients or service users, it is their responsibility to ensure that they have supplied the appropriate 'Privacy Notice' and received explicit consent from the patient/service user to exchanges as envisaged under the terms of this agreement.

3.4 Where parties to this Agreement process information received indirectly via for example the Secondary Uses Service (SUS) there is no requirement to provide the "Fair Processing Information" and obtain consent. This is subject to reasonable assurances that the individual was provided with the necessary fair processing information at the time of their original contact with the initial Data Controller.

4. Consent from Individuals to Share their Personal Information

4.1 Staff should always seek consent from individuals before sharing their personal data and/or sensitive personal data, whenever possible and appropriate. They should record the consent, when given, on their organisation's standard consent documentation, or as a contemporaneous entry into the electronic records system.

Where it is not possible to obtain consent, this could be because:

- the individual does not have the mental capacity to consent

- it may not be safe to seek consent
- it may not be possible to seek consent for some other reason

4.2 In cases where it has not been possible to seek or obtain consent, staff should always record the justification for sharing the information, and how this decision was arrived at.

5. Data Controller

5.1 Each partner organisation will remain the "Data Controller" of their own individual databases and systems unless specifically referenced as "Controllers in Common".

6. Role and Responsibilities of Gloucestershire Care Services and Gloucestershire County Council

6.1 This Agreement requires each participating partner organisation to have a nominated senior professional (e.g. Caldicott Guardian) who is responsible for:

- Agreeing who in their organisation has access to the shared information
- Agreeing amendments to the Agreement
- Ensuring mechanisms are in place to monitor its operation and ensure compliance

6.2 Partners are responsible for ensuring;

- All information received under this Agreement will only be used for the purposes defined and listed in the Agreement.
- The information shared between partners will consist of the minimum amount of personal information necessary to correctly identify a person.
- All data must be accurate, valid, reliable, timely, relevant and complete; the responsibility for ensuring this remains with the partner holding the original information.
- Information received under this Agreement will not be disclosed to another agency/organisation without the agreement of the agency/organisation that provided the information in the first place and the explicit consent of the patient/service user.
- Information will be retained no longer than is necessary and in accordance with each organisation's respective retention schedules. Information will be protected by security measures equal to those stipulated in the sections (below) on access and security.

7. Method for Information Sharing

7.1 Information may be shared in the following ways:

- Information accessed in situ, via provision of access to organisational databases or records.
- In written information transferred by secure e-mail or via a 'trusted link'. (See 9 below)
- In written communications transferred by fax to Safe Haven faxes
- In written communications, transferred in hard copy through approved internal or external mail services.
- Verbally i.e. face to face, in wider meetings or on the telephone.

Examples of written information/communications include alert/referral forms, letters, statements, reports or spreadsheets.

8. Secondary Use of Information

8.1 Partner organisations must always seek to use anonymised personal data for secondary uses. Where identifiable data is needed for particular analyses, organisations must ensure there is a secure legal basis for use and disclosure, either through statute or consent.

8.2 Where there is a statutory basis for processing the data, there is still an obligation to inform individuals about how their data is being used, ideally at initial collection, and, other than where processing is mandatory, patient dissent must be respected.

8.3 Both the transitional and proposed new arrangements will give rise to new issues and conflicts of interests for clinicians and social workers. Staff should consult their respective Information Governance or Caldicott Leads to manage these to ensure they do not result in detriment to patients or service users.

8.4 Where possible, NHS numbers will be used within Adult Social Care to aid the ongoing development of closer working between health and social care.

9. Security

9.1Secure transfer of Information

When any of the following transfer methods is used, it is essential to consider security in both the access, processing and recording of information, and also throughout transit and delivery. Information should be appropriately secured in transit, and transferred by approved methods agreed by the respective partner organisations.

9.1.1 Verbal Transfer:

Verbal conversations and interviews should be recorded in a statement that is agreed by the information giver. Care must be taken to record and denote information clearly as fact, statement or opinion and to attribute any statement or opinion to the owner. All information should be recorded in such a way that it can be used as evidence in court, should that be required at a later date. Minutes of meetings which involve the exchange of personal and sensitive

information, e.g. case conferences, should be anonymised as much as possible and agreed by all participants present.

9.1.2 Written communications:

Written communications containing confidential information should be transferred in a sealed envelope marked "Private & Confidential" and addressed by name to the designated person within each organisation. Alternatively, confidential information can be sent by fax, providing it is sent to a 'safe haven' fax. This is a fax machine that is managed in such a way that you can be confident that information can be transferred to it in the knowledge that safeguards are in place to ensure its security and that access is restricted to assure confidentiality.

Written communications containing sensitive personal information sent to patients/service users by post should be done via Recorded Delivery.

9.1.3 Email communications:

When confidential information is sent by e-mail, it should be sent and received using secure domain e-mail addresses, or via Trusted Links to ensure encryption of information in transit. Secure e-mails include the following e-mail address domains:

- NHS (*.NHS.net)
- GSi (*.gsi.gov.uk)
- CJX (*.police.uk or .pnn.police.uk)
- GSE (*.gse.gov.uk)
- GSX (*.gsx.gov.uk)
- GCSX (*.gcsx.gov.uk)
- SCN (*scn.gov.uk)
- CJSM (*cjsm.net)
- MoD (*.mod.uk)

Secure email is reliant on BOTH the sender AND recipient using one of the e-mail domains listed above. In the absence of this, the SENDER will need to encrypt the content of the e-mail using additional authorised software, e.g. Winzip.

In all transfer scenarios, the onus is on the SENDER to ensure that:

- Information is transferred securely
- The chosen method is acceptable to and workable by the recipient
- Information has reached the required recipient

In the event that a recipient receives information by an unsecured route, it is the responsibility of the recipient to advise the sender and agree a secure route for future transfers of information. Further information on secure methods of transfer is available from http://staffnet.gloscc.gov.uk/index.cfm?articleid=13561

9.2 Storage & Data Management

All patient/service user information will be stored securely and shall be protected by appropriate technical and organisational measures; this includes the use of physical and virtual security, and role based access controls.

All data requiring de-identification for secondary purposes will be stored within the Safe Haven of either Gloucestershire Care Services of Gloucestershire County Council.

9.3. Access Controls

Access to data will be controlled by the respective system owner or records manager (Information Asset Owner).

Authorisation of specific roles on Smartcards (where used) for individual members of staff will be managed through the Registration Authority (RA) process as agreed by GCS & GCC.

- Each Role will be established with a nominated sponsor.
- Access will be subject to approval by the Information Asset Owner (IAO).
- Addition and removal of Roles will be undertaken by Systems administrators (Information Asset Administrators) following approval by the IAO.

Details of roles and access authorisations as applied by partner organisations will be available on request.

10. Information Quality

10.1 Partner organisations are individually responsible for the quality of the data under their control in line with their respective Data Quality and Record Management policies.

10.2 When receiving information, partner organisations are responsible for applying relevant quality checks before using the information. If the information is found to be inaccurate, it is the responsibility of the organisation discovering the inaccuracy to notify the relevant partner.

10.3 Both partner organisations have a responsibility to ensure that all information is adequate, relevant and not excessive for the purpose of processing it.

11. Retention & Disposal of Information

11.1 The Data Protection Act (1998) requires that personal data and sensitive personal data is not retained for longer than necessary. Partner organisations will have their own organisational, legal or procedural requirements for records retention and disposal. These retention schedules should be observed and applied at all times.

12. Breaches of Security

12.1 Any breaches in security should be reported and monitored within each organisation following their own incident reporting policies, and relevant partner organisations should be informed.

13. Subject Access Requests

13.1 Under the Data Protection Act 1998, individuals have a right of access to information held about them unless an exemption applies.

13.2 Any subject access request received from, or on behalf of, a service user or appropriate person will be dealt with according to the existing Data Protection Policy of the organisation who "controls" the data.

14. Complaints Procedures

14.1 Any complaints will be dealt with under the Local Authority Social Services and National Health Service Complaints (England) Regulations 2009.

14.2 Any complaint received from, or on behalf of, a service user or appropriate person relating to inappropriate disclosure of information, will be dealt with via the relevant complaints procedure(s) of the organisation to which the complaint relates.

15. Training

15.1 Each partner organisation will expect all staff requiring access to their respective systems to have undertaken annual mandatory Information Governance training alongside any specific system-related training.

16. Indemnity

16.1 A partner organisation (i.e. Gloucestershire County Council or Gloucestershire Care Services) will not be liable for any financial or other costs incurred by the other partner organisation to this Agreement, as a result of any information being wrongly disclosed by the other as a result of any neglect, act, default or omission by them.

16.2 Each partner organisation shall indemnify the other partner organisation to this Agreement and keep them fully and effectively indemnified against all direct losses, claims, damages, liabilities (whether criminal or civil), costs, charges, expenses (including legal fees and costs), demands, proceedings and actions which the other partner organisation may incur and which in any case arises out of:

- Any breach by a partner organisation, its employees, servants or agents, of any of the provisions of this Agreement,
- Any processing by a partner organisation, its employees, servants or agents, of personal data received, for purposes other than the originating purpose, or

- Any breach by a partner organisation, its employees, servants or agents, of any law in respect of its processing of personal data received by reason of a disclosure made by the other partner organisation.

16.3 Each partner organisation shall be under a duty to mitigate against all losses which it may incur.

17. Freedom of Information

17.1 This Agreement is not confidential and will be made available for anyone to view. It is recommended that the Agreement is published through the Freedom of Information Publication Scheme for each partner organisation.

18. Review

18.1 This information sharing agreement will be reviewed on a six monthly basis.

Appendix 1

Legislation relevant to sharing personal data

Legislation	Section Description
Children Act 1989	**Section 17** – general duty of local authorities to safeguard and promote the welfare of children within their area who are in need, and so far as is consistent with that duty, to promote the upbringing of such children by their families. **Section 47** – where a local authority is informed that a child who lives, or is found, in their area is the subject of an emergency protection order or is in police protection or there is reasonable cause to suspect that a child who lives, or is found, in their area is suffering, or is likely to suffer, significant harm, there is a duty to investigate.
Children Act 2004	**Section 10** – promote co-operation to improve wellbeing. **Section 11** – arrangements to safeguard and promote welfare.
Crime and Disorder Act 1998	**Section 17** – duty of each authority to exercise its functions with due regards to the likely effect of the exercise of those functions, and the need to do all that it reasonably can, to prevent crime and disorder in its area. **Section 115** – any person who apart from this section would not have power to disclose information to a relevant authority or to a person acting on behalf of such an authority, shall have the power to do so in any case where the disclosure is necessary or expedient for the purposes of this act.
Criminal Justice and Courts Services	**Section 67** – the authority for each area must establish arrangements for the purpose of assessing and managing the risks posed in that area by relevant sexual or violent offenders and other persons who have committed offences who are considered by the authority to be persons who may cause serious harm to the public. **Section 68** – interpretation of who is a relevant sexual offender.
Data Protection Act 1998	**Section 29(3)** – where disclosure is required for the prevention or detection of crime of the apprehension or prosecution of offenders.

	Section 35(1) – where the disclosure is required by or under enactment, by any rule of law or by the order of a court.
Education Act 2002	**Section 175 –** a local education authority shall make arrangements for ensuring that the functions conferred on them in their capacity as a local education authority are exercised with a view to safeguarding and promoting the welfare of children.
Local Government Act 1972	**Section 111(1)** – a local authority shall have the power to do anything which is calculated to facilitate, or is conducive to or incidental to, the discharge of any of their statutory functions.
Local Government Act 2000	**Section 2(1) –** a local authority shall have the power to do anything which they consider is likely to achieve the promotion or improvement of the social well-being of their area.
National Health Service Act 2006	**Section 82 –** in exercising their respective functions NHS bodies and local authorities must co-operate with one another in order to secure and advance the health and welfare of the people in England and Wales. Section 201(3)(d) – a disclosure of information may be made if it is for the purposes of any criminal investigation or proceedings. Section 201(6) - Information to which this section applies may be disclosed in accordance with section 201(3) despite any obligation of confidence that would otherwise prohibit or restrict the disclosure.

Appendix 2
Definitions:

There are two distinct classifications of data covered by the Data Protection Act (1998): Personal data and sensitive personal data.

Personal data includes data relating to a living individual who can be positively identified from the data, or from the data and other information which is at the disposal of other individuals or is in the public domain. Personal data includes obvious identifiers such as names, addresses, dates of birth, as well as NHS or National Insurance numbers. Facial photographs and CCTV footage are also regarded as personal data, as are descriptions or photographic records of unique scars, tattoos or other markings.

Sensitive personal data includes data relating to racial or ethnic origins, religious beliefs or similar belief systems, political opinions and affiliations, trade union membership, physical or mental health (including disabilities), sexual life, the commission or alleged commission of offences, and criminal proceedings

Schedule 2 *– one or more of these conditions must be met when sharing personal data*

Condition 1 - the data subject has provided their consent to the sharing
Condition 3 - the sharing is necessary to comply with a legal obligation
Condition 4 - the sharing is necessary to protect the individual's life or protect them from serious harm
Condition 5 - the sharing is in the public interest and is necessary for the disclosing organization *or* another organization to undertake its official duties
Condition 6 - the sharing is necessary for a legitimate and lawful purpose and does not cause unwarranted prejudice to the data subject

Schedule 3 *– one or more of these conditions must be met when sharing 'sensitive' personal data, as well as at least one condition from Schedule 2*

Condition 1 – the data subject has provided their 'explicit' consent to the sharing
Condition 3 – the sharing is necessary to protect the life of the individual or someone else or to protect them from serious harm
Condition 7- the sharing is necessary for the disclosing partner to undertake its official duties
Condition 8- the sharing is necessary for medical purposes including preventative medicine, medical research and the management of healthcare services
Condition 9- the processing is of sensitive information as to racial or ethnic origin and is necessary for identifying or reviewing the existence or absence of equality of opportunity or treatment, with a view to enabling such equality to be promoted or maintained

Sensitive Personal Data Order 2000 *- one or more of these conditions must be met when sharing 'sensitive' personal data, as well as at least one condition from Schedule 2*

Condition 1(a) – the sharing is in the substantial public interest
Condition 1(b) – the sharing is for the prevention or detection of an unlawful act

Appendix 3