

Warrington Information Sharing Agreement (Tier 2)

Arrangements for the sharing of:

Personal and sensitive information to assist in the investigation of, and response to, suspected harm, abuse, neglect or victimisation of adults in Warrington.

From: Warrington Adult Safeguarding Board

To: Warrington Clinical Commissioning Group / Warrington and Halton Hospital Foundation Trust / NHS England Cheshire & Merseyside / Cheshire Fire and Rescue Service / Citizen Advice Bureau / 5 Boroughs Partnership / Cheshire Police / Cheshire Probation / Bridgewater Community Healthcare NHS Foundation Trust / Warrington Borough Council.

Over the period of: 1 April 2016 to 31 March 2018

APPROVAL:

Approving Body 1: Warrington Clinical Commissioning Group
Approved on: 18/04/2016

Approving Body 7: Cheshire Police
Approved on: 19/05/2016

Approving Body 2: Warrington and Halton Hospital Foundation Trust

Approving Body 8: Cheshire National Probation Service

Approved on: 16/05/2016

Approved on: 05/08/2016

Approving Body 3: NHS England Cheshire & Merseyside

Approving Body 9: Bridgewater Community Healthcare NHS Foundation Trust

Approved on: 19/04/2016

Approved on: 14/04/2016

Approving Body 4: Cheshire Fire and Rescue Service
Approved on: 03/08/2016

Approving Body 10: Warrington Borough Council
Approved on: 18/04/2016

Approving Body 5: Citizen Advice Bureau
Approved on: 16/05/2016

Approving Body 11: Golden Gates Housing (Torus Group)
Approved on: 21/06/2016

Approving Body 6: 5 Boroughs Partnership

Approving Body 12: Cheshire & Greater Manchester CRC

Approved on: 13/06/2016

Approved on: 16/05/2016

Version Number: Draft Version
1.3

Effective from: 1 April 2016

Effective to: 31 March 2018

VERSION CONTROL

VERSION	AMENDED DATE	AMENDED BY	MAIN CHANGES
1.0	19 June 2014	Kellie Williams	Changes to sharing with and without consent
1.1	7 August 2014	Kellie Williams	Changes following consultation with WSAB Board Members
1.2	14 August 2014	Kellie Williams	Data Controllers added
1.3	26/01/2016	Rosie Lyden	Name & DOB to be used as specific identifiers and References to 'No Secrets' replaced with Care Act Statutory guidance

For all queries relating to this Agreement please contact:

Rosie Lyden

Adult Safeguarding and Quality Assurance division

Warrington Borough Council

New Town House, Buttermarket Street, Warrington,
WA1 2NJ

Email: ryden@warrington.gov.uk Tel: 01925 442334

Introduction

Sharing information and data is vital to ensure Warrington residents receive appropriate services, care and treatments; we prevent the harm or neglect of vulnerable people; we deliver our statutory functions; and we deliver services in a more effective and efficient way.

This Information Sharing Agreement is part of a set of documentation that together make up the Warrington Information Sharing Framework (see Appendix One), including a Tier One Information Sharing Agreement which includes the signatories of all member organisations of the Framework. These documents can be accessed via the Warrington Partnerships website at http://www.warrington.gov.uk/info/200721/community_support_and_advice/506/warrington_partnership or on Warrington Adult Safeguarding Board website at <https://www.warrington.gov.uk/wsab> under “The Board” page.

This Tier 2 Agreement details the purpose, impact, legislative powers, consent arrangements, procedures and process which underpin the secure and confidential exchange of information between agencies for the purpose of safeguarding adults at risk in Warrington.

Definition

For the purpose of this Tier Two Information Sharing Agreement the term ‘vulnerable adult’, has been replaced with ‘adult at risk’.

The Social Care Institute for Excellence (SCIE) applies the Department of Health definition previously used for ‘vulnerable adult’ as an exact replacement for ‘adult at risk’ as set out below:

“A person aged 18 years or over who is or may be in need of community care services by reason of mental or other disability, age or illness; and who is or may be unable to take care of him or herself, or unable to protect him or herself against significant harm or exploitation.”

The Care Act (2014) sets out the statutory requirements where a local authority has reasonable cause to suspect that an adult is at risk of abuse or neglect in cases where the adult:

- a) has needs for care and support (whether or not the authority is meeting any of those needs)
- b) is experiencing, or is at risk of, abuse or neglect, and
- c) as a result of those needs is unable to protect himself or herself against the abuse or neglect or the risk of it.

Purpose of the agreement

This Tier Two Agreement sets out an understanding between the partner organisations that make up the membership of the Warrington Adult Safeguarding Board in order to facilitate and govern the practice of information sharing.

This data will be used for the purposes of:

- a) Identifying ‘adults at risk’ who may be at risk of harm, abuse, neglect or victimisation.
- b) Identifying and apprehending perpetrators of abuse.
- c) Ensuring that organisations that provide services to and commission services for adults are compliant with their statutory duties and are held to account.
- d) Undertaking investigations and reviews including safeguarding and serious incident investigations, Domestic Homicide Reviews, Safeguarding Adults Reviews and Multi Agency Reviews
- e) Working together so that all partners can, at both strategic and operational levels influence continuous improvements in service delivery and better meet the needs of service users.

- f) Ensuring that policy and practice around safeguarding adults is evidence-led.
- g) Ensuring that performance around safeguarding adults is managed effectively and reported to the Health and Wellbeing Board.

The partners to this Agreement may only use the information disclosed as set out as above. They may not regard shared information as intelligence for the general use of their organisation, unless set out above. They may not pass the information on to any third party, without specific amendment and addition to this Tier Two Agreement.

Principles

The Care Act Statutory Guidance, issued by the Department for Health, sets out the principles around the practice of information sharing in the context of working across a range of organisations. The principles are described as below:

- a) information will only be shared on a 'need to know' basis when it is in the interests of the adult
- b) confidentiality must not be confused with secrecy
- c) informed consent should be obtained but, if this is not possible and other adults are at risk of abuse or neglect, it may be necessary to override the requirement
- d) it is inappropriate for agencies to give assurances of absolute confidentiality in cases where there are concerns about abuse, particularly in those situations when other adults may be at risk

Legality

Sharing information in accordance with this Agreement is lawful under the legislation set out below.

a) The Data Protection Act 1998

The Act requires that personal information is obtained and processed fairly and lawfully; only disclosed in appropriate circumstances; is accurate, relevant and is held no longer than necessary; and is kept securely.

The Act allows for disclosure without the consent of the subject in certain circumstances, including:

- The prevention or detection of crime;
- The apprehension or prosecution of offenders; and
- Where failure to disclose would be likely to prejudice those objectives in a particular case.

b) The Human Rights Act 1998

The Act states that everyone has a right to respect for private and family life, his home and his correspondence and that a public authority may share information in accordance with these rights and in the interests of national security, public safety or the economic well being of the country for the prevention of disorder or crime, protection of health or morals or for the protection of rights and freedom of others.

c) Public Interest Disclosure Act 1998

The Act sets out 'protected disclosure' of information under the following criteria:

- A criminal offence has or is likely to be committed;

- A person has failed, is failing or is likely to fail to comply with any legal obligation;
- A miscarriage of justice has occurred, is occurring or is likely to occur;
- The health and safety of any individual has been, is being or is likely to be endangered;
- The environment has been, is being or is likely to be damaged; and
- Information tending to show any matter falling within the any one of the above has been, is being or likely to be deliberately concealed.

d) Crime and Disorder Act 1998

The Act introduced measures to reduce crime and disorder, including a requirement to establish local crime partnerships around local authority boundaries to formulate and implement strategies for reducing crime and disorder in the local area.

Section 115 of the Act established a power to disclose information, which is central to the Act's partnership approach. This power is not a duty and therefore the requirements set out in the Human Rights Act, Common Law and the Data Protection Act must also be met. Under this Section the Police have a responsibility to disclose information for the prevention, detection and reduction of crime. This is extended to other organisations to disclose information to Police authorities, local authorities, probation committees, health authorities, or to persons acting on their behalf, for the purposes of this Act.

However, there is no requirement to exchange information, rather permission to do so.

e) Common Law Duty of Confidentiality

The 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 individual has been informed about and has consented to. This duty is not absolute but should only be overridden if the holder of the information can justify disclosure as being in the public interest, that is, to protect others from harm.

f) Freedom of Information Act 2000

The Freedom of Information Act 2000 enables any member of the public to apply for access to information held by bodies across the public sector. The Act provides a general right of access to information held by public authorities in the course of carrying out their duties. This right does not extend to personal information, which is largely exempt from the Freedom of Information Act.

The WASB have the responsibility for ensuring that this Agreement is included in the council's Publication Scheme.

All staff involved with this Agreement must be made aware that disclosure of personal information, which cannot be justified on legal or statutory grounds, whether inadvertently or intentionally, could be subject to disciplinary action.

Types of information

Personal data

The Data Protection Act 1998 defines 'personal data' as information relating to a living individual who can be identified:

- from the information, such as name and date of birth;

- from the combination of the information and other information that may be publically available such as address; and
- which affects the privacy of the subject, whether in personal, family, business or professional life.

Sensitive personal data refers to information that provides details of racial or ethnic origin, political opinions, religious beliefs, Trade Union membership, physical or mental health, sexual life, commission or alleged commission of an offence, criminal proceedings or sentence.

The Data Protection Act 1998 does not apply to information about people who have died. However, this information may be considered sensitive and or confidential and is subject to the requirements set out in this Agreement.

Where it is necessary for information to be shared, personal information will be shared on a need to know basis.

Anonymised data

Anonymised data should be aggregated in such a way that it is impossible to identify the individual to which it is relating to. This can be shared without the consent.

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 information 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.

Non-personal data

Non-personal data is information that does not relate to people, such as information about organisations, natural resources and projects, or information about people that has been aggregated to a level that is not about individuals.

Types of data

Types of information and data which may be shared subject to the legal requirements set out in Section 5: Legality may include, but is not limited to information about service users who access statutory or community services, including their name, address, date(s), summary of service use, intervention and support given.

Confidentiality

This Agreement considers the impact on the privacy and confidentiality of service users and their personal information. It is good practice to seek informed consent of service users. However, disclosure without consent is lawful if certain conditions are met. For example, personal information may be shared when anonymised or to ensure the performance of public functions or legal obligations. Consent and advice arrangements are set out in Section 8: Consent.

To support confidentiality and consent arrangements further operational detail of consent forms, guidance for staff and service users, complaints procedures and any other relevant operational procedure documentation is outlined in a Tier Three Operational Arrangement.

Consent

As with all work involving personalised data informed explicit consent should be sought before sharing data in line with statutory duties.

However, this protocol recognises that this may not always be possible or appropriate. For example, meetings across partners whose purpose is to exchange information around shared safeguarding concerns in order to protect them from further harm.

It may be necessary to override the requirement depending upon the circumstance or where doing this would undermine the purpose of sharing that information.

Professionals need to be mindful of the statutory duties and the requirement to be able to explain why the decision not to obtain consent was made.

When it is necessary to seek consent in order to disclose personal information and or data the individual concerned should be made fully aware of:

- the nature of what will be disclosed if this is the appropriate course of action; and
- who the information may be shared with, the purposes for which the information will be used and any other relevant details including their right to access, withhold or withdraw consent.

All partner organisations should ensure that officers handling personal data relating to ‘adults at risk’ are aware of and follow their organisation’s policies and procedures.

Implied consent

Implied consent relates to circumstances where it would be within the reasonable expectations of the individual that information may be shared without needing to obtain explicit consent. It is likely to apply where information is routinely shared and the individual is aware of this or where information sharing is intrinsic to the purpose for which the data subject or confider supplied the information.

Sharing without consent

There are circumstances when it is lawful to disclose personal information about an individual without their consent, whether this has been sought, or sought and withheld.

Decisions regarding the disclosure of information must:

- Be made on a case-by-case basis; and
- Consider if there is a ‘legitimate purpose’ for sharing the information and if it in the ‘public interest’ to share.

Where there is uncertainty around disclosure, consultation with and approval by the appropriate Caldicott Guardian, Data Protection Officer, Information Risk Officer, Freedom of Information Officer or those with similar responsibilities from the partner organisations must be sought.

Legitimate purpose

For the purposes of this agreement a ‘legitimate purpose’ for sharing information would include:

- Preventing serious harm to an adult at risk
- Providing urgent medical treatment to an individual
- Protecting individuals at risk of abuse.

Public interest

The Data Protection Act 1998 recognises that in certain circumstances it is within the ‘public interest’ to share information and creates certain exemptions from the non-disclosure provisions. These include:

- a) Disclosures required by law or in connection with legal proceedings
- b) Disclosures required for the prevention or detection of crime

- c) Disclosures required to protect the vital interests of the individual concerned
- d) Where there is an overriding public interest.

Organisational responsibilities

The partners to this Agreement are responsible for ensuring that they:

- Utilise the full name, D.O.B and address of the individual as the identifiers when sharing information for multi-agency purposes rather than internal codes/references to ensure there is clarity on the individual involved.
- Fulfil their responsibilities and obligations around confidentiality of personal information in line with the statutory requirements (see Section 5)
- Share information legally and within the terms of this Agreement (see Section 5)
- Share information on a need to know basis (see Section 4)
- Understand that disclosure of personal information which cannot be justified, whether intentionally or unintentionally will be subject to disciplinary action, and maybe subject to legal sanctions
- Record all information disclosure in line with their organisations policies and procedures
- Store of all personal information retained within their manual and / or electronic systems securely, such as locked filing cabinets and password protected systems
- Control and restrict access to personal information to those who have a legitimate need
- Transfer personal information and data securely, via encryption (electronic records) or by confidential post
- Retain and dispose of records containing personal information and or data in line with their organisations data retention policy.
- Follow the Audit Commission's six principles of data quality; accuracy; validity; reliability; timeliness; relevance and; completeness
- Have systems and processes in place to ensure that any information that is gathered, retained or shared complies with Principle 7 of the Data Protection Act and is protected by appropriate security.

Involved parties

Each organisation signed up to this Agreement is a member of the Warrington Information Sharing Framework. Each organisation has previously signed the Tier 1 Information Sharing Protocol, which sets out the principles and minimum standards under which information will be shared between organisations. Details of this can be found on the Warrington Partnership website at

http://www.warrington.gov.uk/info/200721/community_support_and_advice/506/warrington_partnership.

The Warrington Information Sharing Framework members involved in this Agreement are:

- a) Warrington Clinical Commissioning Group
- b) Warrington and Halton Hospital Foundation Trust
- c) NHS England Cheshire & Merseyside
- d) Cheshire Fire and Rescue Service

- e) Citizen Advice Bureau
- f) 5 Boroughs Partnership
- g) Cheshire Police
- h) Cheshire Probation
- i) Bridgewater Community Healthcare NHS Foundation Trust
- j) Warrington Borough Council.
- k) Golden Gates Housing Trust
- l) Cheshire & Greater Manchester CRC

This Agreement is owned equally by all participating members and is coordinated and administered on their behalf by:

Adult Safeguarding Board Manager of Warrington Borough Council

The Data Controllers for 1.3 above are:

- a) **John Wharton** (Chief Nurse & Quality Lead) of Warrington Clinical Commissioning Group
- b) **Angela Madigan** (Deputy Director of Nursing) of Warrington and Halton Hospital Foundation Trust
- c) **Dr Kieran Murphy** (Medical Director), NHS England North (Cheshire and Merseyside) of NHS England Cheshire & Merseyside
- d) **Mike Anderson** (Group Manager Prevention Team) of Cheshire Fire and Rescue Service
- e) **Steve Cullen** (Chief Executive) of Citizen Advice Bureau
- f) **Jeanie Hedley** (Information Governance Manager) of 5 Boroughs Partnership
- g) **Jane Shaw** (Information & Compliance Manager) of Cheshire Police
- h) **John Davidson** (Head of Cheshire LDU) of Cheshire National Probation Service
- i) **Jan McCartney** (Head of Information Governance) of Bridgewater Community Healthcare NHS Foundation Trust
- j) **Jo Hodgkinson** (Care First Coordinator) of Warrington Borough Council.
- k) **Gill Healey** (Group Head of Social Investment) of Golden Gates Housing Trust (Torus Group)
- l) **Donna Yates** (CRCCGM Executive Community Director) Cheshire & Greater Manchester CRC

This protocol also relates to those organisations that are contracted to provide services for adults in Warrington by the partners to this agreement.

Information security

The partners to this Agreement will ensure the security for the exchange of information which will be achieved through the use of encrypted devices and secure email.

Security for the storage of information will be achieved through password protected systems and lockable filing cabinets, both of which will have restricted access.

Security for the disposal of information will be the responsibility of each partner organisation in line with their Data Retention Policy.

To support information security further operational detail of data transfer, storage and disposal is outlined in a Tier Three Operational Arrangement.

Monitoring and review

This Agreement will be reviewed on an annual basis.

It is agreed by all signatories that either organisation listed in this Agreement, or the Warrington Partnership Information Governance Board, may request a review of compliance at any time, either delivered themselves, or via a third party. All requests will be adhered to unless under exceptional circumstances which prevent either party involvement.

Approval

The signatories below confirm

- Their organisation is signed up to the Warrington Tier 1 Information Sharing Protocol.
- Resources and trained personnel are in place to fully maintain the procedures set out in the Agreement above.
- This Agreement will be registered via the Warrington Partnerships website.
- Review periods have been agreed and will be upheld.

Appendix One:

Organisation 1: Warrington Clinical Commissioning Group

Senior Information Risk Owner (SIRO):

Name: Nick Armstrong

Job title: Chief Operating Officer

Email address:

Nicholas.armstrong@warringtonccg.nhs.uk

Phone number: 01925 843 636

Signature:



Date: 18/04/2016

Caldicott Guardian (where available):

Name: John Wharton

Job title: Chief Nursing & Quality Lead

Email address:

john.wharton@warringtonccg.nhs.uk

Phone number: 01925 843 690

Signature:



Date: 18/04/2016

Data controller

Name: Not applicable to Warrington CCG

Job title: N/A

Email address: N/A

Phone number: N/A

Signature: N/A

Date: N/A

Organisation 2: Warrington and Halton Hospital Foundation Trust

Senior Information Risk Owner (SIRO):

Name: Angela Madigan

Job title: Deputy Director of Nursing

Email address: angela.madigan@whh.nhs.uk

Phone number: 01925 662112

Signature:



Date: 16/05/2016

Caldicott Guardian (where available):

Name: Simon Constable

Job title: Medical Director

Email address: simon.constable@whh.nhs.uk

Phone number: 01925 662298

Signature:



Date: 16/05/2016

Data controller

Name: Angela Madigan

Job title: Deputy Director of Nursing

Email address: Angela.Madigan@whh.nhs.uk

Phone number: 01925 66 2112

Signature:



Date: 16/05/2016

Organisation 3: NHS England Cheshire & Merseyside

Senior Information Risk Owner (SIRO):

Name: N/A

Signature: N/A

Job title: N/A

Email address: N/A

Date: N/A

Phone number: N/A

Caldicott Guardian (where available):

Name: Dr Kieran Murphy

Signature: (Email confirmation)

Job title: Medical Director

Email address: jaynejones1@nhs.net

Date: 19.04.2016

Phone number: 01138252774

Data controller

Name: N/A

Signature: N/A

Job title: N/A

Email address: N/A

Date: N/A

Phone number: N/A

Organisation 4: Cheshire Fire and Rescue Service

Senior Information Risk Owner (SIRO):

Name: Andrew Leadbetter

Signature: Email Confirmation

Job title: Head of Legal and Demographic
Services

Date: 03/08/16

Email address:

andrew.leadbetter@cheshirefire.gov.uk

Phone number: 01606 868456

Caldicott Guardian (where available):

Name: N/A

Signature: N/A

Job title: N/A

Email address: N/A

Date: N/A

Phone number: N/A

Data controller

Name: Mike Anderson

Signature: Email Confirmation

Job title: Group Manager Prevention Team

Email address

Date: 03/08/16

mike.anderson@cheshirefire.gov.uk

Phone number: 01270 254907

Organisation 5: Citizen Advice Bureau

Senior Information Risk Owner (SIRO):

Name: Steve Cullen

Signature: (email confirmation)

Job title: Chief Executive

Email address:

Date: 16/05/2016

manager@warrington.cabnet.org.uk

Phone number: 01925 246970

Caldicott Guardian (where available):

Name: N/A

Signature: N/A

Job title: N/A

Email address: N/A

Date: N/A

Phone number: N/A

Data controller

Name: N/A

Signature: N/A

Job title: N/A

Email address: N/A

Date: N/A

Phone number: N/A

Organisation 6: 5 Boroughs Partnership

Senior Information Risk Owner (SIRO):

Name: Gail Briers

Signature:



Job title: Chief Nurse and Executive Director
of Operational Clinical Services

Date: 09//06/2016

Email address: gail.briers@5bp.nhs.uk

Phone number: 01925 664 007

Caldicott Guardian (where available):

Name: Louise Sell
Job title: Medical Director
Email address: louise.sell@5bp.nhs.uk
Phone number: 01925 664 007

Signature: 

Date: 10/06/2016

Data controller

Name: Jeanie Hedley
Job title: Information Governance Manager
Email address: jeanie.hedley@5bp.nhs.uk /
G5BP@5bp.nhs.uk
Phone number: 01925 664 485

Signature: 

Date: 10/06/2016

Organisation 7: Cheshire Police

Senior Information Risk Owner (SIRO):

Name: Janette McCormack
Job title: Deputy Chief Constable
Email address:
Janette.McCormick@cheshire.pnn.police.uk
Phone number: 01606 362090

Signature: (email confirmation)

Date: 19.05.16

Information Compliance Department:

Name: Jane Shaw
Job title: Information & Compliance Officer
Email address:
Jane.Shaw@cheshire.pnn.police.uk
Phone number: 01606 363620

Signature: (email confirmation)

Date: 19.05.16

Data controller

Name: N/A
Job title: N/A
Email address: N/A
Phone number: N/A

Signature: N/A

Date: N/A

Organisation 8: Cheshire National Probation Service

Senior Information Risk Owner (SIRO):

Name: John Davidson

Signature: (Email confirmation)

Job title: Head of Cheshire LDU

Email address:

John.Davidson@probation.gsi.gov.uk

Phone number: 01928 713555 / 01244 665100

Date: 05/08/2016

Caldicott Guardian (where available):

Name: N/A

Signature: N/A

Job title: N/A

Email address: N/A

Date: N/A

Phone number: N/A

Data controller

Name: N/A

Signature: N/A

Job title: N/A

Email address: N/A

Date: N/A

Phone number: N/A

Organisation 9: Bridgewater Community Healthcare NHS Foundation

Trust

Senior Information Risk Owner (SIRO):

Name: Gareth Davies

Signature: (Email confirmation)

Job title: Director of Finance

Email

Date: 14/04/16

address: gareth.davies@bridgewater.nhs.uk

Phone number: 01942 482064

Caldicott Guardian (where available):

Name: Dr Karen Slade

Signature: (Email confirmation)

Job title: Medical Director

Email

Date: 14/04/16

address: Karen.slade@bridgewater.nhs.uk

Phone number: 01942 482754

Data controller

Name: Jan McCartney

Signature: (Email confirmation)

Job title: Head of Information Governance

Email

Date: 14/04/16

address: jan.mccartney@bridgewater.nhs.uk

Phone number: 01925 867704

Organisation 10: Warrington Borough Council

Senior Information Risk Owner (SIRO):

Name: Margaret Macklin

Signature:

Job title: Head of Service

Email address: mmacklin@warrington.gov.uk

Date: 18/04/2016

Phone number: 01925 444291

Caldicott Guardian (where available):

Name: Steve Peddie

Signature: 

Job title: Operational Director for F&WB

Email address: speddie@warrington.gov.uk

Date: 18/04/2016

Phone number: 01925 444251

Data controller

Name: Jo Hodgkinson

Signature: (Email confirmation)

Job title: Social Care Records Management

Team Manager

Date: 18/04/2016

Email address: jhogkinson@warrington.gov.uk

Phone number: 01925 443573

Organisation 11: Golden Gates Housing Trust (Torus Group)

Senior Information Risk Owner (SIRO):

Name: Cath Phillips

Signature: (Email confirmation)

Job title: Group Head of Legal and

Governance

Date: 21/06/2016

Email address:

cath.phillips@wearetorus.co.uk

Phone number: 01744 417607

Caldicott Guardian (where available):

Name: N/A

Signature:

Job title: N/A

Email address: N/A

Date:

Phone number: N/A

Data controller

Name: Gill Healey

Signature: (Email confirmation)

Job title: Group Head of Social Investment

Email address: gill.healey@wearetorus.co.uk

Phone number: 01744 417622

Date: 21/06/2016

**Organisation 12: Cheshire & Greater Manchester Community
Rehabilitation Company**

Senior Information Risk Owner (SIRO):

Name: Gavin Emberton

Signature: (Email confirmation)

Job title: Head of Corporate Services

Email address:

Date: 16/05/2016

gavin.emberton@cgm.probation.gsi.gov.uk

Phone number: 03000 479 000

Caldicott Guardian (where available):

Name:

Signature:

Job title:

Email address:

Date:

Phone number:

Data controller

Name: Donna Yates

Signature:

Job title: CRCCGM Executive Community

Director



Email address:

Donna.Yates@cgm.probation.gsi.gov.uk

Phone number: 01244 665100

Date: 16/05/2016

Appendix Two: Framework

Table 1 – Warrington Information Sharing Framework	
<p>Tier 1 - Information Sharing Protocol and Declaration of Acceptance and Participation (DAP)</p>	<p>A signed statement of willingness from organisations across Warrington to enter into information sharing agreements. This sets out the principles and minimum standards under which information will be shared between organisations.</p> <p>Approval level: Senior accountable officer, SIRO and Caldicott Guardian (where available).</p>
<p>Tier 2 - Information Sharing Agreement</p>	<p>Sets out the detail of what information will be shared, why, between who and the legal basis under which it will be shared. Provides an overview of the procedures involved in data transfer, storage and disposal.</p> <p>Approval level: SIRO, Caldicott Guardian, Data Asset Owner and relevant strategic manager (for example, Assistant Director)</p>
<p>Tier 3 – Operational Arrangement</p>	<p>These include the specific processes involved in the transfer, storage and disposal of data to ensure it complies with legal requirements, including details of consent documentation.</p> <p>Approval level: Data Asset Owner and Operational manager.</p>
<p>Guidance notes</p>	