



Freedom of Information Act Publication Scheme	
Protective Marking	Not protectively marked
Publication Scheme Y/N	Y
Title	A purpose specific information sharing agreement between Westminster BOCU, Westminster Social Services and CNWL Foundation Trust
Version	1.1
Summary	An agreement to formalise information sharing arrangements between Westminster BOCU, Westminster Social Services and CNWL Foundation Trust
(B)OCU or Unit, Directorate	Westminster BOCU
Review Date	17/01/2013
Date Issued	16/01/2012

<i>Title & Version</i>	A purpose specific information sharing agreement between Westminster BOCU, Westminster Social Services, and CNWL Foundation Trust ,Version 1.1
<i>Author</i>	Pc Lee RISTOW
<i>Organisation</i>	MPS Westminster OCU
<i>Summary/Purpose</i>	An agreement to formalise information sharing arrangements between Westminster BOCU, Westminster Social Service, and CNWL Foundation Trust

ISA Ref: GN51/05/17

Information Sharing Agreement
between
**The Metropolitan Police London Borough
of Westminster,**
Westminster Social Services
and
**Central and North West London (CNWL)
NHS Foundation Trust**
for the purpose of
Mental Health Risk
Assessments

Central and North West London 
NHS Foundation Trust



City of Westminster



Index

Section 1. Purpose of the agreement	Page 1
Section 2. Specific Purpose for sharing	Page 2
Section 3. Legal Basis for Sharing and Specifically what is to be Shared	Page 7
Section 4. Description of Arrangements including security matters	Page 13
Section 5. Agreement Signatures	Page 15

BOCU instructions

The MPS Information Sharing documents to enable information sharing in relation to Mental Health Act Assessments are on the MPS Mental Health intranet pages and in the General Registry docket GN51/05/17. Of all the Information Sharing templates this is the only one that requires completion at a BOCU level to ensure local arrangements are compliant with MPS Information Sharing guidance and agreed to by Social Services.

Section 1. Purpose of the Agreement

This agreement has been developed to:

- Define the specific purposes for which the signatory agencies have agreed to share information.
- Describe the roles and structures that will support the exchange of information between agencies.
- Set out the legal gateway through which the information is shared, including reference to the Human Rights Act 1998 and the common law duty of confidentiality.
- Describe the security procedures necessary to ensure that compliance with responsibilities under the Data Protection Act and agency specific security requirements.
- Describe how this arrangement will be monitored and reviewed.

The signatories to this agreement will represent the following agencies/bodies:

MPS BOCU Westminster
Social Services, London Borough Westminster
Central and North West London (CNWL) NHS Foundation Trust

Section 2. Specific Purpose for Sharing Information

Introduction

As part of their duties Approved Mental Health Professionals (AMHP) undertake assessments of people under the Mental Health Act 1983. In certain circumstances they can request police assistance and obtain a warrant to enter and assess under s135 MHA, further they will also undertake to engage with new or unknown clients.

In order for the AMHP to assess the risks around meeting with services users and the necessity of requesting police assistance when they need to undertake a MH assessment. The police may hold information on an address or an individual that would be critical in assessing risk. This has been recognised in the Multi-Agency Pan London Standards developed with the London Development Centre (LDC-NIHME) and a multi-agency LDC review of this standard (Nov 2005). The Review report and recommendations have been agreed by the LDC Partnership Group, Directors of Social Services, NHS Mental Health Trust Directors and MPS. The report includes recommendations in relation to the risk assessment process and a tool to undertake this.

The agencies that will be involved in this agreement will be London Borough of Westminster Social Services, and CNWL Foundation Trust and their AMHPs. CNWL provides a comprehensive range of health and social care services to people with substance misuse, learning difficulties and mental health difficulties living in central and north west London.

The MPS will be sharing information in relation to people whose mental health is planned to be assessed by an AMHP or new/unknown clients. The information will be details of violence or threats, use or possession of weapons and alcohol/substance misuse. The MPS will also share general information about other risks associated with the venue.

The MPS will receive information to search police data bases to identify the individual (name, sex, date of birth, ethnicity and address).

Objectives

MPS Benefits

By sharing information an informed risk assessment can take place by the Approved Social Worker (AMHPs) before they undertake Mental Health Act (MHA) assessment or engage with clients. By correctly assessing the risk, requests for police assistance can be objectively made and considered. This will support:

- the safety of all those involved
- a proportionate response
- the effective use of resources

The police have a duty to prevent crime. Having officers present when AMHPs undertake high/medium risk MHA assessments will prevent injury and crime (assaults).

Partner Agency(ies) Benefits

AMHPs take the lead in planning MHA assessments on private premises. Part of this process is for them to undertake a risk assessment. The Pan-London Standard (as developed by NIHME-London Development Centre) requires that this includes information from the police. This information will benefit AMHPs by assisting in the identification of risk and its management.

Citizen Benefits

The person who is the subject of the MHA assessment will benefit as the information sharing will be used to assess the risk and inform the decision as to whether the police need to be involved. Sharing the information will help in ensuring a proportionate response:

- If no/minor risks are identified then the police will not be involved.
- If med/high risks are identified police will be involved to protect subject from injuring themselves/others and staff involved in the assessment.

Rationale

The information shared will be used by the AMHP to undertake a risk assessment as 'the only predictor of future behaviour is past behaviour' (Dr Nigel Eastman consultant forensic psychiatrist-Ritchie 1994:118). A multi-agency project team working under the LDC has developed a joint risk assessment tool that requires information to be shared.

It is clear from public inquiries following homicides involving those with a mental illness that information sharing is critical. Themes from the recommendations made in inquiries after homicide (SCD1 Homicide Prevention-Mental Health) 01/11/04) show:

- From the 69 inquiries considered in the SANE report, 90% reported a breakdown in communication between key agencies
- In the Clunis case, the greatest problem was identified was the 'failure to communicate, pass information and liaise between all those who were or should have been concerned with Clunis' care. (Ritchie 1994)

Clearly information and communication has been identified as an important feature in reducing risk.

The Homicide Prevention Unit have identified a number of high risk factors from their analysis. These include the offenders' failure to take their prescribed medication, their use of illegal drugs, domestic violence and their previous threatening behaviour. Also prevalent are use of weapons, especially knives and the escalation in violent offending behaviour (Mental Health Homicide: Emerging Findings March 2005 HPU).

While these statistics relate to the serious crime of murder the factors will be relevant to those considering risk. The police may have information in relation to risk factors that would not be available to the AMHP.

Information to be Shared

Information in relation to the subject of the assessment in particular:

- History of violence
- Risk of violence
- History of self harm
- Risk of self harm
- Alcohol/substance misuse
- Weapons
- State of mind

This information will be obtained from the following data bases:

- CRIMINT
- CRIS
- PNC
- MERLIN
- NSPIS (custody records)

Information will also be provided if a risk is presented by others at the address in relation to violence and weapons. The information provided would not identify individuals but would identify any additional risks in general.

Section 3. Legal Basis for sharing and what Specifically will be Shared

Lawfully

A public authority must have some legal power entitling it to share the information.

INDICATE: the primary legal power you are invoking to share this information.

AMHPs have legal authority to undertake assessments under the Mental Health Act and in certain circumstances apply for a warrant to enter and assess under s135 of the MHA. There is an implied gateway between the police and Social Services to provide information to assist AMHPs in undertaking this function.

Provision of police information is also directly linked to policing, as it will be used to identify risk, mitigate the risks and so protect all those involved in the assessment and or the engagement with new and unknown clients

Duty of Confidence

If the service has received any information in confidence, you almost certainly have a Duty of Confidence towards the data subject.

INDICATE: How any duty of confidence might be overridden

The duty of confidence might be overridden on the basis of public interest in safeguarding the safety of all those involved in an assessment including the subject. There will likely be disclosure of both certain conviction and none conviction data that is relevant to the risk assessment.

Fair processing

INDICATE: How you will comply with Fair Processing

Exemption under s.29 Data Protection Act 1998

Partners to this arrangement will claim an exemption from this provision. This exemption is permitted by Section 29(1) Data Protection Act 1998. This is based upon the grounds that information is being shared for the prevention and detection of crime and for the apprehension and prosecution of offenders.

The purpose of the arrangement relates to the prevention crime ie: violence towards health professionals involved in the assessment. To comply would be likely to prejudice the purposes of the assessment by alerting the subject too the intention of conducting an assessment and potentially adding to any risk.

It is known from public inquiries (see proposal) that some mentally disordered offenders do not have a complete forensic history due to pre-charge diversions by the police into health care. For this reason none conviction data may be shared to inform the risk assessment.

Legitimate Expectation

An individual's expectation as to how information given to a public body will be used will be relevant in determining whether the first data protection principle has been complied with.

INDICATE: how the information sharing arrangement is consistent with the legitimate expectations of the data subject.

A mental health assessment by an AMHP is enshrined in the MHA. The sharing of information with those involved in a MHA assessment is legitimate in assessing any risk, taking mitigating action to ensure the safety of all those involved. This arrangement will be published on the MPS publication scheme so that members of the public can see in what circumstances information for this purpose will be shared.

Human Rights - Article 8: The Right To Respect For Private Life

There shall be no interference by a public authority with the exercise of this right except such 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.

INDICATE: how the Article 8 of the Human Rights Act is to be satisfied

- In pursuit of a legitimate aim

The information is shared to assist AMHPs in undertaking their lawful function. Sharing information will assist in managing risk and ultimately preventing/minimising violence. It will ensure the safety of all those involved.

- Proportionate

Not sharing information could lead to a dis-proportionate response in that if AMHPs are not fully informed when planning the assessment they may be inclined to routinely ask for police assistance. The Review identified a wide range of police involvement depending on borough. A robust process is being implemented as a result of the review that includes joint risk assessment. This will set out clear criteria for the involvement of police and support a more proportionate response.

- Appropriate and necessary to a democratic society

The conducting of mental health assessment are provided for in the MHA.

Schedule 2, Data Protection Act 1998

In addition to the legal criteria set out above, the information sharing arrangement must satisfy **at least one** condition in Schedule 2 of the Data Protection Act in relation to personal data.

INDICATE: the Schedule 2 Condition(s) Satisfied

Schedule 2 Data Protection Act 1998 requirements and, in brackets, where it appears in the schedule

The data processing is necessary for:

- The purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms of legitimate interests of the data subject [6(1)]

The information sharing is to support the legitimate interests of AMHPs. By sharing information an informed risk assessment can take place by the Approved Social Worker (AMHPs) before they undertake Mental Health Act (MHA) assessment or undertake a new client. By correctly assessing the risk, requests for police assistance can be objectively made and considered. This will support:

- the safety of all those involved
- a proportionate response
- the effective use of resources

The police have a duty to prevent crime. Having officers present when AMHPs undertake high/medium risk MHA assessments will prevent crime (assaults).

Schedule 3, Data Protection Act 1998

If the information is “sensitive” (that is, where it relates to the race, ethnic origin, political opinions, religion or belief system, membership of a trades union, physical/mental health or sexual life, the commission or alleged commission of any offence, proceedings relating to the offence) you must satisfy at least one condition in Schedule 3.

INDICATE: How the Schedule 3 Condition is satisfied

Exercise of Powers Conferred under Statute [7]

An implied gateway exists to support the exercise of AMHPs in their lawful role under the MHA.

Vital Interest [3]

The person subject to a MHA assessments vital interest is being served as the purpose of the assessment is their health care.

A MHA assessment would normally be considered when other methods have been tried and failed or likely to fail. It is unreasonable to obtain the consent of the data subject as this could frustrate the assessment process, impact on the safety of those involved by forewarning the subject.

Second Principle

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

INDICATE: how the agreement complies with the second data principle

This information was obtained for Policing purposes. Under this arrangement it will not be processed in any manner contradictory to that purpose.

Third Principle

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

INDICATE: how the agreement complies with the third data principle

The MPS information to be shared will be in relation to the subject of the assessment in particular:

- History of violence
- Risk of violence
- History of self harm
- Risk of self harm
- Alcohol/substance misuse
- Weapons
- State of mind

This information will include specific details to evidence the particular risk.

Information will also be provided if a risk is presented by others at the address in relation to violence and weapons. The information provided would not identify individuals but would identify any additional risks in general.

Fourth Principle

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

INDICATE: how the agreement complies with the fourth data principle

This information comes from MPS corporate systems and is subject to our normal procedures and validations intended to ensure data quality. Any inaccuracies should be notified to the SPOC.

It will be the responsibility of the new data controller(the partner) to maintain it in future. If so, insert a statement to that effect.

Fifth Principle

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

INDICATE: how the agreement complies with the fifth data principle

The information can be retained as part of the Social Services records in relation to the assessment and the individual concerned and should be

retained as part of Social Services records management policies (Paul find out)

Sixth Principle

Personal data shall be processed in accordance with the rights of data subjects under this Act.

INDICATE: how the agreement complies with the sixth data principle

- Partners to this arrangement will respond to any notices from the Information Commissioner that impose requirements to cease or change the way in which data is processed.
- Partners will comply with subject access requests in compliance with the relevant legislation.
- The MPS reserves the right to withdraw right of use of the data at any time.

Seventh Principle

Appropriate technical 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.

INDICATE: how the agreement complies with the seventh data principle

Measures to satisfy the Seventh Principle are detailed in the Baseline Security Assessment document.

Eighth Principle

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 of the rights and freedoms of data subjects in relation to the processing of personal data

INDICATE: how the agreement complies with the eighth data principle

The information is not intended for transfer outside the European Economic Area.

The Caldicott principles

The Caldicott Principles are guidelines that are followed by Social Care and Health professionals regarding the use of person-identifiable and confidential

information. The Caldicott principles are set out below. These principles apply in addition to the requirements of the Data Protection Act 1998. The Caldicott principles are supported by the appointment of Caldicott Guardians, members of staff in the NHS and Councils with Social Services Responsibilities with a responsibility to ensure patient-identifiable data is kept secure.

- Justify the purpose for using identifiable information;
- Only use identifiable information when absolutely necessary;
- Use the minimum identifiable information that is required;
- Restrict access to identifiable information on a need-to-know basis;
- Ensure that everyone handling identifiable information is aware of their responsibilities; and
- Understand and comply with the law.

Section 4. Description of arrangements including security matters.

Designated Single Point of Contact

The Designated single point of contact in relation to information sharing for mental health risk assessments will be the Westminster BMHLO contactable via the group email [MHL-CW@ Met.pnn.police.uk](mailto:MHL-CW@Met.pnn.police.uk), or 02073219451

Methods of Requesting/Transferring/Recording

Please describe how information will be requested and then transferred between partners and how it will be recorded when received; include reference to Data Retention and Future Use Policy. Take into account any current recording methods and any Information Technology impact; e.g. in electronic or hard copy format.

At Meetings

Information may be shared at meetings a representative from each group will attend. This exchange could be paper based, disk based or CCTV tape. These representatives will perform the role of a designated officer – they will be responsible for bringing information to the meeting and taking information away. They will record what personal information they shared at the meeting and the date it was shared. Similarly, when they take information away from the meeting and share this with their team members, they will record what has been shared and the date of sharing.

Outside Meetings

Outside of formal meetings information sharing may be done via the request process, it can be paper based, disk based, CCTV tape based, or could be verbally in person by phone or fax or via secure email. The recording procedures will follow the model in the above paragraph, staff will record what information they shared with who and what information they received, together with the date.

Requesting Process

Requests for disclosure of information will be via a modified MPS form 3315a which has been circulated to partners, the request will be made via secure email to MHL-CW@Met.pnn.police.uk using the 3166a request form or in exceptional circumstances via fax having confirmed that the BMLO or a named member of the mental health unit is aware and can collect the fax upon arrival. The signed copies of the request will be retained in the subjects files along with the subsequent disclosure

Right of Access to Information

Please describe who will have a right of access to the information provided as a result of this arrangement and what procedures are in place to prevent unauthorised access/disclosure.

Only staff employed by the agencies listed on the front cover will have access to the information that is shared. All members of staff will be responsible for securely retaining the information supplied to them. In practical terms this will translate to keeping the information in a secure office to which only staff employed by these agencies have access or in a locked drawer/cupboard. If information is stored on a computer, access must be by password which is accessed by individually assigned passwords. The information will only be used on a 'need to know basis', Any Security breaches will be reported to the MPS and covered by Trust/Social Services disciplinary procedures. The managers of each team in Social Services and the Trust will ensure AMHPs are aware of the above security provisions

Consent

Please describe the procedures in place for ensuring that clients have given their prior explicit consent to the sharing of agreed information between partners; include how this consent is captured and shared between partners and for how long it remains valid.

Partners to this agreement are not relying upon the consent provisions of Schedule 2 and Schedule 3 to the Data Protection Act. Information sharing will satisfy Schedule 2 and 3 by the statutory power to share information through the s135 of the Mental Health Act 1983 and by the processing condition of being in the data subjects vital interests.

Process

The information will be shared using the following process:

- 1) The AMHP will complete a risk assessment using the joint tool and fax (or secure e-mail) this to the BOCU single point of contact (SPOC).
- 2) The SPOC or member of the Mental health Unit will undertake checks of police data bases and complete the police part of the risk assessment.
- 3) The SPOC will retain a copy of the risk assessment and fax (secure e-mail) to the AMHP.
- 4) The AMHP will retain the information securely with their documentation in relation to the subject.
- 5) The AMHP will use the information to undertake their risk assessment and their decision as to whether to request police assistance with the assessment.

The AMHP can:

- Use the information for risk assessment
- Retain the information as part of their agencies records in relation to the assessment and the individual concerned.
- Retain as part of Social Services records managements policies

- Use the information to brief participants in the MHA assessment

Section 5. Agreement to abide by this arrangement

The agencies signing this agreement accept that the procedures laid down in this document provide a secure framework for the sharing of information between their agencies in a manner compliant with their statutory and professional responsibilities.

As such they undertake to:

- Implement and adhere to the procedures and structures set out in this agreement.
- Ensure that where these procedures are complied with, then no restriction will be placed on the sharing of information other than those specified within this agreement.
- Engage in a review of this agreement with partners at least annually.

We the undersigned agree that each agency/organisation that we represent will adopt and adhere to this information sharing agreement:

Agency	Post Held	Name	Signature	Date