Confidentiality Policy

Reviewed & Updated by: Stella Vickers

Date approved by the Board of Trustees: December 2013

Review Date: October 2014

Overview

Application of this policy will be on the basis of equal opportunities regardless of race, colour, nationality, or ethnic origins, age, marital status, gender, sexual orientation, disability, religion or other personal circumstances or disadvantages.

This policy describes the procedures in place to uphold the confidentiality of service users and their children at the Brighton Oasis Project. This includes confidentiality agreements with service users, times at which confidentiality may or must be breached and security measures to safeguard the confidential information kept by the organisation.

Contents

Legislative Framework

Common Law Duty of Confidence
Children's Act 2006
Computer Misuse Act 1990
Crime and Disorder Act 1998
Data Protection Act 1998
Drug Trafficking Act 1994
Human Rights Act 1998
Crime and Disorder Act 1998
The Protection of Children Act 1999
Terrorism Act 2006
Freedom of Information Act 2000
Health & Social Care Act 2012
Sexual Offences Act 2003

National Guidance and Local Protocols

South East Coast Overarching Information Sharing Protocol
Confidentiality: NHS Code of Practice 2003
NTA – Confidentiality and Information Sharing 2013

Other Relevant Policies/ Procedures/ Guidelines

Information Sharing & Data Protection Policy
Staff Code of Conduct

Scope of Policy

- This policy applies to all BOP management, employees, volunteers, recovery champions and service users.
- This policy is applicable both on and off premises during BOP-related activities.

Policy Statement

Brighton Oasis Project is committed to providing a confidential service to its service users and their children within the boundaries of relevant legislation. Any adult or child safeguarding, criminal or substantial concerns about risk to a person's safety, can override any confidentiality agreement.

Brighton Oasis Project believes that principles of confidentiality must be integrated across all aspects of its services and management. Brighton Oasis Project believes its users deserve the right to privacy and confidentiality to protect their interests and safeguard Brighton Oasis Project's services.

The Confidentiality policy applies to all children and young people attending services at Oasis, equally as it applies to adults. It also applies Oasis premises and on outings.

Confidential information about service users and their children at BOP will be kept as secure as possible at all times to ensure that, as far as is reasonably practicable, confidentiality is not breached.

Relevant Procedures & Implementation Guidelines

1. Training & Dissemination of Information

All employees will be made aware at induction of the importance of maintaining confidentiality within the organisation and will be given this policy to read through and have reference to.

Modifications and updates to confidentiality policies, legislation, or guidelines will be brought to the attention of all staff.

Service users will be informed of our confidentiality policy as part of their induction onto a day programme and a signed consent form will be kept with their file.

2. Advice & Consultancy

Where reasonably practical all relevant staff will be consulted on modifications and updates to procedures relating to confidentiality.

The following agencies could also be consulted on specific confidentiality and information sharing matters:

The Information Commissioners Office

3. Definition of Confidentiality & Confidential Information

Confidentiality arises where a person disclosing personal information reasonably expects his or her privacy to be protected, such as in a relationship of trust.

"Confidentiality is the central trust between a service user and a drug treatment service, enabling an open and honest relationship between the service user and the drug service professional. However, information sharing is also central to providing a service user with a seamless integrated service involving other services, to best meet their needs and to reduce the risk of harm to self and others. Information needs to be shared between agencies about service users who are in contact with multiple agencies and those whose care is transferred from one agency to another." NTA – Confidentiality and Information Sharing (2003)

Any of the following information collected in the course of a service user (either adult or child) care will/could constitute person identifiable information:

Name, address, post code, date of birth, NHS No., National Insurance No., carers details, next of kin details, contact details, bank details, lifestyle, family details, artwork or voice and visual recordings.

Further sensitive information that could also be recorded within a service user or child's records includes racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health condition, sexual life, criminal proceedings or convictions.

4. The Caldicott Guardian

A Caldicott Guardian is a senior person responsible for protecting the confidentiality of service user information and enabling appropriate information-sharing. The Guardian plays a key role in ensuring that the NHS, Councils with Social Sevices responsibilities (CSSRs) and partner organisations satisfy the highest practicable standards for handling patient identifiable information. Within BOP the Caldicott Guardian is the director. The key responsibilities of the Caldicott Guardian are as follows:

Strategy & Governance: the Caldicott Guardian should champion confidentiality issues at Board/management team level, should sit on an organisation's Information Governance Board/Group and act as both the 'conscience' of the organisation and as an enabler for appropriate information sharing.

Confidentiality & Data Protection expertise: the Caldicott Guardian should develop a knowledge of confidentiality and data protection matters, drawing upon support staff working within an organisation's Caldicott function but also on external sources of advice and guidance where available.

Internal Information Processing: the Caldicott Guardian should ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff. The key areas of work that need to be addressed by the organisation's Caldicott function are detailed in the Information Governance Toolkit.

Information Sharing: the Caldicott Guardian should oversee all arrangements, protocols and procedures where confidential patient information may be shared with external bodies both within, and outside, the NHS and CSSRs. This includes flows of information to and from partner agencies, sharing through the NHS Care Records Service (NHS CRS) and related IT systems, disclosure to research interests and disclosure to the police.

5. The Right to Privacy

If a service user requests to speak to a staff member in private, a private space is to be found. If there is no such space available at the time, or it is not possible for that staff member to leave public space, an appointment is to be made when private space and the staff member are available.

6. Consent to Share Confidential Information

Adult services

All information held on service users and their children is confidential to Brighton Oasis Project and cannot be disclosed to third parties without the permission of the individual concerned.

Service users should be made aware of the organisation's confidentiality policy and their rights to access the information that is held on them as soon as is reasonably practicable. This should usually be at the first point of significant contact with an individual, and/or at the point at which a service user joins a day programme at BOP. Their understanding of this should be sought and logged by their signature on a Confidentiality Waiver for each episode of care.

Permission to disclose information must only be accepted from the service user in the form of a signed consent form naming individuals, agencies or organisations to whom information may be given. The Confidentiality Waiver is the primary form of consent used at BOP which describes the organisations and agencies with which it regularly shares information. Service users should be

encouraged to sign confidentiality waivers with regard to other agencies and organisations they are working with, in the interests of optimally managing shared care.

The service user should also be given information (in the form of a leaflet) about what data is recorded and shared with the National Drug Treatment Monitoring System (NDTMS), what this information is used for, information about how their data will be protected and what the implications might be for withholding information. They should also be given an explanation that any consent given can also be withdrawn in the future. If they refuse to share this information, "REFUSED" should be logged on their records. For more information regarding NDTMS data sharing and information for service users see **Appendix B**.

In addition to this a Carer's Confidentiality Waiver can be used when a service user has requested information be shared with another individual involved in their care.

Service users have the right to object to the use and disclosure of confidential information that identifies them, and need to be made aware of this right. Sometimes, if they choose to prohibit information being disclosed to other health professionals involved in providing care, it might mean that the care that can be provided is limited and, in extremely rare circumstances, that it is not possible to offer certain treatment options. Service users must be informed if their decisions about disclosure have implications for the provision of care or treatment.

Staff should check at each new episode of care or normal review stage to ensure that individuals have not changed their mind. It is essential that children, once they gain capacity, are asked to confirm their own choice, as a previously recorded choice regarding consent may have been made by another party, on their behalf, which may not reflect their own choice. It may also be essential to revisit consent at other times e.g. when changes, which impact on how information is used, are introduced. This may be due to changes in service provision or government initiatives. Consent should also be reviewed whenever there are changes to information sharing/disclosure(s) during an episode of care. Any worker disclosing information to a third party without the service user's permission, except in exceptional circumstances (see below) will be subject to disciplinary procedures.

The relationship of a service user is with the organisation and not with an individual staff member, sessional worker or volunteer; therefore information will be shared within the organisation. Line managers have a right of access to all information. Information should be shared with other staff members, sessional workers or volunteers on a need to know basis.

Young Oasis therapeutic service

The Young Oasis Confidentiality Agreement for Therapy must be carefully explained in an age appropriate manner to a child or young person and their Parent/carer before therapy begins. It must be clear that it is understood and signed by themselves and/ or a parent/carer where appropriate. Parent/carer consent must be sought for children below 16yrs of age to access the services.

7. Disclosure of Information without Consent

Adult services

In certain circumstances, confidentiality may be broken without the permission of the client:

- Where there are concerns about the welfare of a child as defined by the Children Act 2006 (see Safeguarding Children Policy)
- When required through a court order, or through a legitimate search warrant
- If a violent situation arises and the service user is endangering the safety of staff, other clients, or others
- Where there are suspicions that a serious crime has or may be committed, e.g. murder, sexual crime (as defined in the Sexual Offences Act 2003), terrorism (as defined in the Terrorism Act 2006), drug trafficking (as defined in the Drug Trafficking Act 1994)
    - Section 115 of the Crime and Disorder Act 1998 gives public bodies the power, *but not a duty,* to disclose information for the prevention or detection of crime
- When disclosures of physical or sexual abuse are made and others may still be at risk from the alleged perpetrator
- When allegations are made of a gross breach of trust or misconduct of a professional worker
- Circumstances where withholding information might result in serious harm to another
- To ensure the service provides a duty of care in a life-threatening situation (e.g. serious illness or injury, suicide and self-harming behaviour). This includes when a service user continues to drive against medical advice, when unfit to do so. In such circumstances relevant information should be disclosed to the medical advisor of the Driver and Vehicle Licensing Agency (DVLA) as soon as possible.

Any adult or child safeguarding, criminal or substantial concerns about risk to a person's safety, can override any confidentiality agreement.

Where it has been judged necessary to share information the clients permission will always be sought unless to do so would endanger them, or another person further. The reasons for sharing the information will be outlined clearly and the risks of not sharing along with the statutory duty of the organization will also be discussed.

There may be cases where it is not possible to contact the client or where the client refuses permission for the information to be shared. Decisions to divulge information about a client to a third party without the client's consent should be discussed by the client's key worker and the Services Care Co-Ordinator/

Director (the designated Caldicott Guardian). The discussion and the decision making process will be recorded on the template 'Information share without consent'. The final decision will be the Services Care Co-Coordinator's/ Director's, or in their absence, the most senior worker's. The decision should be made without delay ensuring compliance with any local agreements for safeguarding vulnerable adults and children The client will be informed of the Project's decision wherever possible..

See Information Sharing & Data Protection Policy for more information.

Children and Young people

A child or young person's confidentiality may be breached where there are safeguarding concerns regarding the child/young person, their parent or carer or where there is a serious threat of harm to another person. The confidentiality policy for safeguarding purposes will be made clear to parents/ carers and to the young person where they attend without an adult, on their initial induction/assessment/ completion of the registration form.

In such cases children/young people's information may be shared with an outside agency.

If there is evidence of probable danger to the client or any other child, eg .when a child has made a disclosure in a creche/ therapy session and is viewed to be at risk, the practitioner is **required** to disclose this according to the BOP safeguarding policy.

In addition to any safeguarding concerns the practitioner is required to report any medical issues about the child to their parent/carer or to the appropriate person in the work setting.

Young Oasis Therapeutic Services

Within the therapeutic service if a child or young person has made or is threatening to harm themselves or make a suicide attempt, the therapist will contact the child's GP. The practitioner **must** therefore obtain the telephone number of the child's GP before the commencement of therapy

The practitioner **must** therefore make the limitations of the confidentiality clear to the child from the outset of the therapy. They should explain that where they believe the child or young person to be in emotional or physical danger they will have to tell someone. This may include disclosing details of actual sessions so that any risks to the child can be managed. The practitioner will endeavor to talk to the child, if possible, before talking to a third party.

Practitioners must keep detailed notes on any disclosure, and write down a verbatim account of what the child said.

8. Data Security

Staff should take all reasonable and practical steps to ensure that information remains confidential. The following should be adhered to by all staff members:

- All identifiable information held on service users must be kept secure – either in written/printed format in locked cabinets on premises, or in electronic format protected by passwords on a BOP computer or on the BOP virtual private network (VPN).

- Referral templates containing sensitive personal information about service users and their children should never be stored alongside forms and templates on the shared drive. If a copy is required for reference then it can be printed and placed on the clients file. In all other cases the completed template should be deleted immediately.

- Staff members should not give out person-identifiable information over the telephone unless they have satisfied themselves that they know the identity of the requestor.

- Breaching confidentiality is not just restricted to paper or computer records. Staff members should take care when discussing pertinent cases with their colleagues that the conversation is not being overheard.

- Staff members should ensure confidential information is destroyed as confidential waste as opposed to being placed in the waste paper bin or standard recycling.

- Staff members should change passwords at regular intervals and must never write them down, nor share them with any other person, whether a close colleague or otherwise.

- Computer hard drives and storage shall be disposed of securely when no longer required. Confidential information shall not be leaked to outside persons through inappropriate disposal

9. Requests for Confidential Information

Under the Data Protection Act 1998 (see **Appendix A**), service users have the right to access person-identifiable information that is held about them at BOP. There is a process for this, including the receipt of appropriate signed consent from the client, and a certain editorial process that may omit details made available to the service user under the grounds that it may cause serious harm to their (or others) mental or physical state, or that it contains information about a third party. See the NHS guidance on Access to Health Records in the references section for more information on this.

There are certain circumstances under which another party may request access to confidential information. If these parties are not covered by the Confidentiality

Waiver, or legislation, then information may only be shared with proof of consent from the client. This could be faxed or posted to the organisation.

The following guidance should be followed when sharing information with other agencies or workers:

"*Ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those people who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely*." (Information Sharing: Guidance for Practitioners and Managers (2008) – see References)

If a service user is over 16 years of age information would only be disclosed to relatives, friends or carers if the service user has given written consent.

10. Confidential Information and Service Contracts/Agreements

All partnership agreements must include confidentiality, both in the contract and the service protocols. Confidentiality clauses must be consistent with Brighton Oasis Project's Confidentiality Policy.

Responsibilities

The Board / Management Committee

- Has overall responsibility for the policies and procedures at BOP, so far as is reasonably practical.

The Director

- To ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff.
- Take the role of Caldicott Guardian for the organisation, championing the use of appropriate information sharing and a culture within the organisation which promotes and maintains confidentiality.
- To ensure that adequate resources and training is made available to staff on the subject of confidentiality.

Line Managers/Care Co-ordinators

- To ensure that staff members are adequately informed about confidentiality procedures at induction and that this becomes part of the working culture at BOP.

Staff Members

- To act with due care and attention for the confidentiality of the clients and their children. (Both within and outside the workplace) and be aware of how and when confidentiality may be waived.
- To discuss any queries or concerns they may have about disclosures with a line manager or senior staff member.

- To ensure that the information they record or access is appropriately stored in secure cabinets or securely on computers.
- To ensure that they verify the authorisation of another person to ensure information is only passed on to those who have the right to see/hear it.
- Not to discuss confidential matters outside of work.
- To dispose of any confidential information in a secure manner (i.e. confidential shredding service, or emptied computer recycle bin).
- Not to access any confidential records/databases/files for personal reasons.
- To attend appropriate training as required.
- To keep passwords secure e.g. do not write them down or share them with anyone else.
- To enter information in manual and computer records accurately and clearly.
- To make sure terminal screens cannot be seen by clients and visitors unless it is part of the client care process.
- To log out of systems/databases when not using them.

References

Information Sharing: Guidance for Practitioners and Managers (2008) - http://www.everychildmatters.gov.uk/_files/116ABBC875E8FEE7BC1E03F534A1EFAA.pdf

Confidentiality: NHS Code of Practice (2003) - http://www.dh.gov.uk/dr_consum_dh/groups/dh_digitalassets/@dh/@en/documents/digitalasset/dh_4069254.pdf

NTA – Confidentiality and Information Sharing (2003) - http://www.nta.nhs.uk/publications/documents/nta_confidentiality_and_info_sharing_2003_dsp1.pdf

NTA – Data Protection and Record Sharing (2003) - http://www.nta.nhs.uk/publications/documents/nta_data_protection_and_record_sharing_2003_dsp2.pdf

NTA – Confidentiality Toolkit (2008) - http://www.nta.nhs.uk/areas/outcomes_monitoring/docs/confidentiality_toolkit.pdf

NTA – Confidentiality Toolkit (2013) - http://www.nta.nhs.uk/uploads/ndtmsconfidentialitytoolkitv6.3.pdf

NHS – Access to Records (2003) - http://www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/Patientconfidentialityandcaldicottguardians/DH_4084411?IdcService=GET_FILE&dID=17820&Rendition=Web

NHS – Caldicott Guardians - http://www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/Patientconfidentialityandcaldicottguardians/DH_4100563

NHS – Data Protection: What do we do with your information http://www.bsuh.nhs.uk/EasysiteWeb/getresource.axd?AssetID=360239
Children's Act 1989 – http://www.opsi.gov.uk/Acts/acts1989/Ukpga_19890041_en_1.htm
Children's Act 2006 - http://www.legislation.gov.uk/ukpga/2006/21/contents

Computer Misuse Act 1990 - http://www.opsi.gov.uk/acts/acts1990/UKpga_19900018_en_1.htm

Drug Trafficking Act 1994 - http://www.opsi.gov.uk/ACTS/acts1994/ukpga_19940037_en_1

Data Protection Act 1998 - http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1

Human Rights Act 1998 –
http://www.opsi.gov.uk/ACTS/acts1998/ukpga_19980042_en_1

Crime and Disorder Act 1998 –
http://www.opsi.gov.uk/acts/acts1998/ukpga_19980037_en_1

The Protection of Children Act 1999 –
http://www.opsi.gov.uk/ACTS/acts1999/ukpga_19990014_en_1

Terrorism Act 2000 –
http://www.opsi.gov.uk/acts/acts2000/ukpga_20000011_en_4#pt4-pb3-l1g39

Terrorism Act 2006 -
http://www.legislation.gov.uk/ukpga/2006/11/contents

Freedom of Information Act 2000 -
http://www.opsi.gov.uk/Acts/acts2000/ukpga_20000036_en_1

Health & Social Care Act 2001 –
http://www.opsi.gov.uk/Acts/acts2001/ukpga_20010015_en_1

Health & Social Care Act 2012 -
http://www.legislation.gov.uk/ukpga/2012/7/contents

Sexual Offences Act 2003 –
http://www.opsi.gov.uk/acts/acts2003/ukpga_20030042_en_1

Appendix A - THE DATA PROTECTION ACT 1998

THE EIGHT PRINCIPLES

For personal data held in any format

1. The information to be contained in personal data shall be obtained, and personal data shall be processed, fairly and lawfully.

2. Personal data shall be obtained only for one or more specified lawful purpose(s). Personal data held for any purpose or purposes shall not be further used or disclosed in any manner incompatible with that purpose or purposes.

3. Personal data held for any purpose or purposes shall be adequate, relevant and not excessive in relation to that purpose or purposes.

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

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

6. Personal data shall be processed in accordance with the rights of the individual under this Act. An individual shall be entitled:

- At reasonable intervals and without undue delay or expense:
    - To be informed by any data user whether he or she holds personal data of which the individual is the subject, and
    - To access any such data held by the data user, and
- Where appropriate to have such data corrected or erased

7. Appropriate security measures shall be taken against unauthorised or unlawful access to, or alteration, disclosure or destruction of, personal data and against accidental loss or destruction of or damage to personal data.

8. 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 for the rights and freedoms of individuals in relation to the processing of personal data.

Appendix B – NDTMS Data and Confidentiality Guidance

Guidance for Sharing Data with the National Drug Treatment Monitoring Service (NDTMS)

CONFIDENTIALITY GUIDELINES FOR STAFF HELP SHEET 1

NHS Code of Practice

Sharing information is part of good communication and is vital to the health care process. Nevertheless it has to be done with due consideration for client/patient confidentiality. The Department of Health has produced a code of practice for NHS staff that addresses confidentiality issues. Voluntary and private drug and alcohol treatment services may also find this code useful to inform their own policies. The document 'Confidentiality: NHS Code of Practice' can be found on the Department of Health website.
Search 'NHS confidentiality code of practice' or 'Patient Confidentiality' for this and other information. The website also provides details of how to apply for hard copy publications.

National Drug Treatment Monitoring System (NDTMS)

CONFIDENTIALITY GUIDELINES FOR STAFF HELP SHEET 2

Treatment Service Confidentiality/Data Handling Policies

All drug and alcohol treatment services must have a clear confidentiality/data handling policy, which is understood by all members of staff. If you have not seen such a policy, ask where it is located.
The policy should be presented and clearly explained to the client/patient, both verbally and in written form, before assessment for treatment begins. It should be explained on the client/patient's first visit and must describe:

- what information will be collected by the treatment service
- when and what information will be shared with any other services and
- organisations involved in their care
- who the information will go to and why
- in what circumstances confidentiality may be breached.

For services within NHS Trusts, the policy may be part of a general Trust policy, but it should be adapted if it does not include the above information.
The policy itself may be outlined in the form of a simple leaflet and/or notice displayed within the treatment service, however the patient/client MUST be given the NDTMS information sheet alongside the treatment service's confidentiality policy/leaflet.
Help sheets 4, 5 and 6 may help you to devise a policy if you do not already have one.
Help sheets 5, 6 and 7 outline the when, what, who and why as far as sharing with the National Drug Treatment Monitoring System (NDTMS) is concerned - but you will doubtless have other services and organisations with whom you may be sharing data.
The information on Help sheet 8 can be communicated to clients/patients as is, or can be incorporated into your treatment service policy. It describes why client information is needed, both by a treatment service and for the NDTMS.

National Drug Treatment Monitoring System (NDTMS) CONFIDENTIALITY GUIDELINES FOR STAFF HELP SHEET 3

Sharing Drug and Alcohol Data with the NDTMS

Local confidentiality policies may differ due to the different needs and practices of drug and alcohol treatment services but, in the case of information collected and shared with the NDTMS on behalf of Public Health England the following should provide some guidance.

- A client/patient's initials, date of birth, gender and postcode (partial unless there is local consent) are used by the NDTMS. Although not fully identified data, these items of information still make it necessary to obtain explicit consent from the client/patient before collecting data to send to the NDTMS.

- Explicit consent can be given orally or in writing. It should be given freely in circumstances where the client has been appropriately informed. There should be an understanding of available options and any concerns and queries should be addressed.

- Ideally, this consent would be part of the process of obtaining consent in general, when explaining local data collection policies.

- The patient/client MUST be given the NDTMS information sheet (see help sheet 8), alongside the treatment service's confidentiality policy/leaflet, which explains what the information will be used for.

- If the client/patient refuses consent, this should be recorded in the clients' case notes and clinical information system.

- If a treatment service has not previously provided data to the NDTMS but begins to do so for the first time, the service should seek retrospective consent from any existing clients. Where consent cannot be obtained, then mark the record as 'no consent'.

- Most clients/patients are reassured when they know why their data is collected and how it is shared. Become aware of the reasons for collecting various data items and how information is used within your service so that your clients/patients are fully enabled to make an informed decision.

National Drug Treatment Monitoring System (NDTMS) CONFIDENTIALITY GUIDELINES FOR STAFF HELP SHEET 4

Data Sharing Protocols

Having data sharing protocols in place, that outline how and why data is shared within and between organisations, is good practice.

It may be that local collection procedures involve third parties (e.g. Partnerships) to make use of jointly procured software. This may necessitate information sharing across treatment services and/or Drug and Alcohol commissioners. It may be that certain treatment services share software across all their sites and information is therefore shared within these sites and/or beyond the region.

It may be important, for one reason or another, for treatment services to share client/patient data if there is more than one service simultaneously providing treatment, irrespective of the Partnership or the software used. This is relevant for example, to Treatment Outcome Profile (TOP) data where a treatment service should, subject to permissions and data sharing protocols, send copies of the TOP information to other services.

If identifiable patient data is to be shared more widely than with Public Health England (e.g. with Health and Wellbeing Board staff), Service Managers should ensure that appropriate consent and data sharing agreements are in place, as this is the responsibility of the treatment service that is collecting the data. They should also take care to ensure that clinical and administrative staff are fully aware of, and understand, the way in which data is used and shared (See Helpsheet 6). In turn, this information should be passed on to clients/patients who should feel reassured about the confidential nature of the data collection and sharing processes.

If your service does not already have data sharing protocols in place, there are useful websites at www.justice.gov.uk and at www.ico.gov.uk. These are the websites for the Ministry of Justice and the Information Commissioners Office respectively. Guidance and example protocols are also easily accessible using internet search engines by typing in ‘data sharing protocols’ for guidance, or ‘NHS data sharing protocols’ to produce a list of example protocols currently being used by different NHS organisations.

National Drug Treatment Monitoring System (NDTMS) CONFIDENTIALITY GUIDELINES FOR STAFF HELP SHEET 5

Why Information is needed for the NDTMS

The drug and alcohol treatment information that you provide to the NDTMS is used for several purposes. Primarily it is used to:

- Assess the number of individuals attending drug and alcohol services in order to monitor the progress of the national drug and alcohol strategies.

- Evaluate the efficiency and effectiveness of drug and alcohol treatment provision, including treatment outcomes for clients/patients.

- Monitor the use of resources. This helps ensure equitable funding of drug and alcohol treatment services nationally.

- Provide a local and regional picture of drug and alcohol users and their needs, which will assist service commissioners Health and Wellbeing Boards and Local Authorities in planning and developing better drug and alcohol treatment services that are more appropriate to their geographical area.

- Monitor the effectiveness of the government drug and alcohol strategies.

- Produce statistics and to support research on drug and alcohol use, treatment or general public health.

National Drug Treatment Monitoring System (NDTMS) CONFIDENTIALITY GUIDELINES FOR STAFF HELP SHEET 6

How Information is handled within NDTMS

Familiarise yourself with the information below and share its detail with clients/patients who wish to have more information about Public Health England and the way in which they handle and use data.

- Public Health England (PHE) is an Executive Agency of the Department of Health. The functions of the National Treatment Agency were transferred to PHE on 01/04/2013.

- The information is passed monthly to NDTMS teams working in regional Public Health England offices. It may go via a third party (e.g. service commissioners). However, the help sheets do not cover the consent arrangements required for any local data collection arrangements. These are the responsibility of, and should be managed by, the local third party body collecting the data.

- To minimise double counting, it is necessary to be able to identify if clients/patients have attended more than one service. For this purpose the initials, date of birth, gender, postcode (partial unless there is local consent), and local authority of residence are recorded. These data items are stored on a database in a secure environment.

- Care is taken at the NDTMS regional centres and Public Health England to ensure that data cannot be accessed unless it is for a clearly authorised purpose.

- The law strictly controls the sharing of very sensitive personal information. Anyone who receives information from the database is under a legal duty to keep it confidential.

- Any information published by the DoH, or Public Health England is always in the terms of total numbers of people.

- Any research that would involve the use of data would be closely scrutinised by the NDTMS Regional Centre and/or PHE. Where appropriate, research proposals would also have to obtain ethical approval.

- Data is matched from the NDTMS with other government datasets to produce statistics which help evaluate the success of treatment programmes.

- All data matching is conducted by Public Health England, and at no point is any identifiable information about clients passed onto other government departments. Data-sets that are used in this way include (but are not necessarily limited to)

    - Drug Intervention Programme

    - Police National Computer

    - Department of Work and Pensions. Other routine health data-sets (e.g. Hospital Episode Statistics)

- Under no circumstances is potentially identifiable data made public or provided to other government departments.

- Data is not placed on any register of addicts – no central register exists.

National Drug Treatment Monitoring System (NDTMS) CONFIDENTIALITY GUIDELINES FOR STAFF HELP SHEET 7

The type of information collected for NDTMS and the time it is retained

It is important that the NHS offers the right treatment at the right time. It is also essential that treatment meets the different needs of the various local and regional populations. For this reason, Public Health England seeks several data items. These include the dates of referral, treatment start and discharge. The list incorporates information on the type of treatments offered, as well as the outcomes of treatment. In addition, the main and secondary problem substances are collected, and Public Health England also need to know about demographics including gender and ethnicity.

The information helps Public Health England and/or those who commission services, to use resources more appropriately to improve drug and alcohol treatment throughout the country.

The NDTMS will hold client/patient information for at least 8 years.

Signature of Service User: …….Date: ……..

Witnessed by……. Date: ……..