BIAN- Confidentiality and Information Sharing

When to use: It is recognised that maintaining confidentiality is crucial to the building of a trusting and respectful working relationship with the service user. It is equally important that all parties recognise that confidentiality is never absolute and service users should be given a clear understanding of the limitations to confidentiality at the outset. All agencies should have appropriate policies and procedures in place to legally allow them to share information.

Protocol Outcomes

1. The service user understands issues relating to confidentiality, including their right to privacy, as well as the limits to confidentiality. The service provider must discuss these issues with the service user to ensure this understanding.
2. The service user is clear about the processes by which they can consent to agreed personal information being shared amongst different parties to the Interagency Care Plan, as well as how to review and withdraw consent.
3. Services agree a definition of what information is considered appropriate and necessary based on the role and responsibility of staff attending and engaged in the interagency care planning process and the role and function of their agencies.

Key Steps

Step 1: All staff participating in the interagency care planning process must be aware of this shared Confidentiality and Information Sharing Protocol, and relevant legislation/ guidelines, as well as any additional policies and procedures from their own agency. Service providers are responsible for ensuring that their staff receive training in all aspects and areas relevant to their role in interagency care planning.

Step 2: Prior to any interagency communication, the key worker/Case Manager should:

- explain the process of interagency care planning to the service user (see Protocol 2)
- complete the Interagency Confidentiality Statement
- ensure written consent via the Interagency Consent for Release of Information Form

Note: Information should only be shared on a need to know basis and where relevant. It has been generally agreed locally that with the service users consent the following information is useful to share:

a) the interagency care plan (to other agencies involved) and information relating to identified needs/progress on the care plan (although the service user should be in attendance and voice their own needs),

b) attendance and engagement (whether a service user attends scheduled appointments or has engaged with other agencies),

c) shared calendar of appointments (so agencies are aware of other scheduled appointments that a service user has).

Step 3: The Interagency Consent for Release of Information Form should be reviewed with the service user at regular intervals of not more than six months by the Case Manager, and if any additional agencies are invited to join the Interagency Care Plan process then the consent of the service user must be obtained beforehand.

Step 4: Service users can withdraw their consent at any time. When this occurs, the Case Manager should try to ascertain why and ask the service user to complete a Withdrawal of Consent Form.
Step 5: Services must ensure that they follow the wishes of the service users in what information they share with other agencies (with reference to the Interagency Confidentiality Statement. Agencies should only request information which is relevant to their own role or that of the agency.
Step 6: Services must train their staff in how to manage potential disclosures[19] at all stages in the working relationship including during interviews to ensure that the service user is fully aware of the limitations to confidentiality before disclosure is made.
Step 7: Where a dispute arises concerning the sharing of information, services should meet to review what information has been requested and why. The requesting agencies should be able to justify their need for the information and its context in relation to their own role with a service user. The Case Manager and/or interagency group should verify the request, discuss the issue with the service user, and agree a collective response. Any actions arising out of the sharing of the information need to be documented on the Interagency Care Plan.
Step 8: Services should have a clear policy on dealing with both formal and informal enquiries relating to service users, and this must be understood by staff, volunteers and service users alike. If it is clear that there has been a breach of confidentiality, whether accidental or not, a follow up process must ensure that the service user is informed and steps taken to ensure the incident is not repeated.
Step 9: The service provider must comply with the requirement to notify the office of the Data Commissioner of breaches of confidentiality as specified by the Data Commissioner

BIAN Shared Policies

a. **Limits of Confidentiality**

It is important to note that confidentiality can never be absolute and absolute confidentiality should never be promised to a service user. Such limits are necessary in the interest of public and/or individual safety. Each participating agency must explain, at the beginning of contact with a service user, that confidentiality doesn't apply in the following situations:

1. A service user clearly indicates his or her intention to:

a. Die by suicide or cause self-harm

b. Injure another person

In this circumstance information may need to be shared with Social Work, An Garda Siochana or a mental health practitioner as appropriate.

2. A service user reveals that they or another/s have abused or currently are abusing a person under the age of 18 years, physically, sexually or by neglect. The agency will then follow the National Guidelines (Children First) in relation to reporting the suspected child abuse to Social Work or An Garda Siochana as appropriate.

3. A staff member of a participating agency has a child protection concern. The agency will then follow the National Guidelines (Children First) in relation to reporting the suspected child abuse to Social Work or An Garda Siochana as appropriate.

4. A staff member/agency is ordered by a court of law to submit a report or is subpoenaed to give evidence then the requested information should be shared with the courts.

From a data protection perspective, sharing of personal data, including sensitive personal data by an organisation (a data controller) can take place in one of three main ways:
1. With explicit consent of the data subject.
2. Where the organisation holding the personal information is under a legal obligation such as a court order to release the information.
3. Where the release of information is in the vital interests of the individual or another individual

b. Acquiring consent/ Release of Information and Review/ Withdrawal of same

Acquiring consent- the Key Worker/Case Manager should explain the Interagency Confidentiality Statement, the process of interagency care planning, and ensure written consent via the Interagency Consent for Release of Information Form for the sharing of agreed information. This should occur before any interagency communication takes place.

Release of Information review-The Interagency Consent for Release of Information Form should be reviewed with the service user at regular intervals of not more than six months by the Case Manager. If any additional agencies are invited to join the Interagency Care Plan process, then the consent of the service user must be obtained beforehand.

Withdrawal of Consent to Share Information-Service users can at any time withdraw consent to share information and their participation in the collaborative process. It is important that the Key Worker/ Case Manager tries to ascertain why the service user wants to disengage from collaborative working. If possible, concerns or issues that have lead the service user to request disengagement should be addressed by the organizations concerned. However, the service user has the final say and if they want to disengage, then the Withdrawal of Consent Form (see FORM 3) should be signed and returned to their assigned Key Worker/ Case Manager.

c. **Report Writing and Recording of Case Notes**

1) Written records should be clear and brief.
- All records should be written in a way that the service user is able to understand
- Records should include only essential and relevant details
- Records should use complete sentences

2) Written records should be timely. Where possible, they should be recorded shortly after the event. Case notes should also be recorded regularly, staff should aim to complete notes at least on a weekly basis.

3) Written records should be accurate and complete. Records should be clear, unambiguous and include the date (day/month/year)

4) Events should be described sequentially

5) Where notes have been made in a written form and used in a meeting (i.e. case meeting) these should include the printed name and signature of the persons completing the records.

6) Any alterations should be made by striking a line through the incorrect information and initialing and dating. The use of correction fluid is not permitted.

7) Records must be objective and factual and describe what is observed/ evidenced. If an

incident has not been observed, but is relevant to service user care, then it must be clearly stated i.e. 'the service user reports that….'. If for some reason a more subjective statement needs to be made, the recorder should acknowledge that this is a subjective opinion.
8) Where possible records should use the service users own words
9) Written records should be readable and written legibly, preferably in black or blue ink.
10) The following common errors in record keeping should be avoided
- Dates, time and signature omitted
- Illegible handwriting
- Ambiguous abbreviations. Abbreviations should not be used unless approved in advance by management
- Phone calls not recorded
- Use of correction fluid
- Completion of records many days after the event
- Unprofessional terminology, colloquialisms, jargon and clichés
- Opinions mixed with facts
- Lack of detail/too much detail.

d. **Secure Storage of Personal Data: Hardcopy and Electronic**

All notes relating to contact between staff and service users must be held in a locked filing cabinet in a locked room. This cabinet must only be used for holding service user files. Only workers who deal directly with service users and the manager/coordinator of the agency may have keys for the cabinet or access to the files. Similarly, where notes are retained on computer systems, these are closed systems that are protected by double entry security passwords and are only accessible to relevant staff and kept in a locked room.

e. **Sharing Information within each Agency**

Issues discussed between a staff member and service user may be discussed with other members of the team as appropriate and/or necessary. It is important to note that confidentiality is between the service user and the organisation rather than between the service user and any particular member of staff. Following this, case specific information will be shared with the staff team as relevant and necessary. This provides workers with a forum to discuss in a professional manner, issues that may be difficult and complex for the worker (as well as for the service user) and allows the team to offer support and guidance to the worker.
Service users indirectly benefit from the combined experiences of the team. Shared confidentiality also means that the whole team is aware of issues facing the service user, enabling other workers to offer appropriate interim support if the service user's key worker is not available. The service user benefits from a uniform response from all team members. The Key Worker should inform service users of their agencies policy on sharing information when they first engage with the service.

f. **Sharing Information with Other Agencies**

Agencies may only disclose the information agreed with the service user on receipt of the signed Interagency Consent for Release of Information Form. For communication outside of BIAN agencies, the same process should be adhered to. Best practice recommends that the service user should view court or similar reports before they are provided to a consented third party. Where 3rd party medical information is included (such as family

history of addiction), if identifying information is included then this should be removed before circulating the information to other agencies.

g. **Sharing Information with Family Members**
Information should only be shared with the service user consent.
h. **Informal Enquiries**
Information should not be shared without the service user consent. Staff members must be careful when dealing with informal enquiries relating to service users as it is possible to identify someone as a service user without meaning to do so.
i. **Under 18's**
All agencies must adhere to the HSE policy on the treatment of service users who are under 18 years. For example, service users under 18 requesting treatment (e.g. methadone, needle exchange) must be referred to the HSE Outreach Team. The HSE Northern Area will require parental consent before a treatment can start.

Consent/ Parental involvement
The involvement of parents in an under 18's care, in general, results in better outcomes for both the individual and family. Services should be aware of the potential additional vulnerability of service users aged under 18. The service will always seek to obtain parental / guardian consent. Where consent to engage parents has not been provided by the under 18, or the parents refuse to provide consent, the service will liaise with the person under 18 and a relevant clinical governance provider to ensure that duty of care has been adequately provided.
Competence (to consent) will be specifically assessed for all 16yrs old to 18yr olds where parental consent can not be provided. In the case of under 16s the service will seek approval from the HSE Consultant Child and Adolescent Psychiatrist prior to engaging in treatment. Certain aspects of the assessment and treatment plan will require specific written consent, these are:
a) Refusal to involve parents in assessment of treatment
b) Sharing of information with other people or agencies (see standard consent to share information forms).
c) Willingness to be contacted after treatment for service evaluation or research purposes.
j. Modes of Communicating Personal Information
Sharing information by telephone- Staff members must be careful when dealing with telephone enquiries relating to service users as it is possible to identify someone as a service user without meaning to do so. The staff member must establish and be satisfied with the identity of anyone requesting information as many service users will not give permission to supply information, for example, to parents or partners. Callers must be told that a confidentiality policy is in place and that direct information cannot be given. If you are unsure, then take a message and ascertain if the information is to be shared with the service user and call the person back. The number can also be checked and this could possibly help to confirm the identity of the person.

Fax usage- Faxed messages containing sensitive case information should only be sent to specified individuals at confirmed numbers while the recipient waits at the fax machine. All faxes should contain cover sheets stating the person whom the fax is intended for.

Receipt of fax should be confirmed by phone.

Email usage- Any information from which a client could be identified should not be sent via email.

k. **Dealing with Accidental, Planned, or Deliberate Disclosure without Permission**

Wrongful disclosure can occur in at least two ways. It can be by either act or omission. The first would be where confidential information is deliberately passed on to a third party. The second would be where confidential information is disclosed to a third party through negligence.

The follow up process must ensure that the service user is informed and steps taken to ensure the incident is not repeated. The service provider must comply with the requirement to notify the office of the Data Commissioner of particular breaches of confidentiality as specified by the Data Commissioner. (see Data Security Breach Code of Practice).

l. ***Service Users' Access to files***

Service users and in some cases, their significant other/s have the right to view information/files relative to the service user (see Freedom of Information Act 1997; Data Protection Act 1988; and individual agencies policy on information management).

All requests should be made in writing. Service users should be supported with their application by their Key Worker, if requested.

Under section 4 of the Data Protection Acts, an individual is entitled, upon making a written request to an organisation, to obtain the following:

a) a copy of the personal data,

b) a description of the purposes for which it is held,

c) a description of those to whom the data may be disclosed and d) the source of the data unless this would be contrary to public interest.

The service user has a right to receive a copy of his/her personal data under the Data Protection Acts within a period of 40 days from receipt of the request and upon payment of a maximum fee of €6.35.