

Confidentiality

COSRT.ORG.UK INFO@COSRT.ORG.UK TWITTER: @COSRTNEWS

Confidentiality

1. Respecting confidentiality is a fundamental requirement for keeping trust and respecting service user autonomy. The professional management of confidentiality concerns the protection of personally identifiable and sensitive information from unauthorised disclosure. Disclosure may only be authorised in the following circumstances:
 - where the person to whom the duty of confidentiality is owed has given explicit consent;
 - where there is an overriding public interest in disclosure; or
 - where sharing is required by a court order or by other legal obligation.
2. Any disclosures of service user's confidences should be undertaken in ways that best protect the service user's trust and respect their autonomy.
3. Service users should be advised that, whilst confidentiality and privacy is extremely important, there may be exceptional circumstances that may prevent the Member from seeking Service user consent to a breach of confidence due to the urgency and seriousness of the situation, for example in order to stop the Service user causing serious harm to themselves or others, or where a serious crime is involved (e.g. murder, manslaughter, rape, kidnapping, child abuse). In such circumstances the Member has an ethical responsibility to act in ways that balance the Service user's right to confidentiality against the need to communicate with others.
4. If disclosure is required by the courts, care needs to be taken to limit disclosure of information to the terms of the relevant order and the precise information requested. It is permitted to make ethical objections but, if the order is not changed, it will be necessary to provide the information or the Member will be in contempt of court.
5. When only one partner of a couple consents to the release of information, the Member may only release information relating to the consenting Service user and should protect the identity and the confidentiality of all information deriving from the non-consenting Service user. This should be the guiding principle even where a court order is in place relating to one of the parties. Appropriate redaction can be used, as well as coding and anonymisation, where appropriate.
6. Different rules apply for the family courts and child protection cases and generally disclosure must be made in these circumstances.
7. Where Members are asked to assist police with information in relation to a serious crime, it will depend upon whether the relevant statute requires or only permits disclosure. In the absence of a requirement to disclose, there must either be explicit consent or a robust public interest justification (usually determined by the court). Where disclosure is justified it should be limited to the minimum necessary to meet the need and Service users should be informed of the disclosure unless it would

defeat the purpose of the investigation, allow a potential criminal to escape or put persons at risk. However, a Member must not give misleading information as this would constitute an offence.

8. Service users should give their express consent to any disclosure of information. However, there are certain situations where it is not possible to advise the Service user of a disclosure. For example, within the provision of the Children Act 1989, the Children (Scotland) Act 1995, the Terrorism Act 2000 (as amended) and the Drug Trafficking Act 1994 (and such other legislation which may from time to time come into force), the law forbids the Member informing the Service user that confidential information has been passed to the authorities.
9. Breaking confidentiality with the full consent of the service user does not constitute a breach of confidentiality. Service user consent is the ethically preferred way of resolving any dilemmas over confidentiality with the exception of the conditions described in clause 8.
10. Confidential information about Service users may be shared within teams where the Service user has consented or knowingly accepted a service on this basis.
11. Informed written consent must be obtained before any information from the clinical work may be used for publication, training or research.
12. Service user confidentiality must be maintained in supervision. When psychosexual and relationship therapy, supervision and training in a group format is offered, the Member must recognise the increased difficulty in maintaining confidentiality and discuss this with potential participants.
13. If a Member is accused formally by a service user of wrongful conduct, then the need for the Member to divulge information about this service user is recognised. The breaking of confidentiality will be kept to a minimum in consultation with advisers.
14. The Member will continue to have regard for the wellbeing of the service user. Service users should be notified of this as part of the contract.
15. Working online raises specific issues of confidentiality. In particular a secure method of payment must be used and Members must be clear about this to service users.
16. The obligation to maintain confidentiality continues after the therapeutic relationship has ended.
17. Members should expect to be ethically accountable for any breach of confidentiality to their Service user and to COSRT for their management of such disclosure.
18. Members should follow COSRT guidance on data protection and ensure that they have in place a privacy statement which is shared with their Service users. They should follow the requirements for obtaining, storing and processing personal data securely. Particular attention should be paid to sensitive personal data. The rights of data subjects should always be respected.
19. Members should ensure that any breach of personal data is notified to COSRT and to the Information Commissioner's office where appropriate.
20. Records should be kept securely for seven years or as long as required by the insurer, normally 7 Years.

21. If in doubt on any of the above issues, seek advice from COSRT or from a legal professional.