College of Sexual and Relationship Therapists

Practice Guideline 6 – Record Keeping

This document should be read in conjunction with Practice Guideline 2 - Contract for Therapy, Practice, Guideline 5 – Confidentiality, Guideline to Members on preparing a privacy statement and COSRT Data Protection Policy.

The legislation covering this Guideline includes the Data Protection (Subject Access Modification) (Health) Order 2000 and the Data Protection Act 2018.

1. To ensure transparency and accountability in the therapeutic process Members are expected to make and keep accurate and appropriate records of their work with clients.

2. All client records must be adequate, relevant, accurate, not excessive and kept up to date.

3. Records may be kept in any format. Paper notes can be scanned in and stored electronically. If notes are taken in digital form, they should include the same information as paper notes (see paragraphs 8 and 9 below). They should also show who made the record, show revisions and amendments, and have the ability to 'lock' the notes. There is no need to retain paper records as well as digital records, but security, retaining back-ups and having the ability to delete records is even more important with digital notes (and see ICO guidance on cloud computing).

4. Clients must be informed who will make, keep and have access to their records, how they will be kept, the purposes for which their records will be held, for how long they will be retained and for what purposes they may be disclosed. Because data relating to a client's sex life and health is 'sensitive personal data', a client should be asked to consent to their data being retained. This is best addressed in the Contract for Therapy, (see Practice Guideline 2- Contract for Therapy/ link). Members are guided to record any variation of the contract terms as they occur, such as the location, frequency and ending of sessions, payment and cancellation arrangements.

5. Clients have a statutory right to see copies of all personal data about them held electronically or manually (if kept in a structured way) and in relation to which they are identifiable. Clients can make a written Subject Access Request (SAR), which must be responded to within a month, requesting details of what data is being held, how it is being

used and details of any third parties with whom is has been shared. They can also ask for this information to be amended, deleted, or transferred. No charge may be made for this.

6. The exception to the above is contained in the Data Protection (Subject Access Modification) (Health) Order 2000 which provides that this information does not need to be disclosed if this would be likely to cause serious harm to the physical or mental health or condition of the client or another person. However, Members must be careful not to refuse a client access on this ground unless they have consulted the 'health professional' (this term is defined) responsible for the client's clinical care. In the case of couple work, if disclosing such data to an individual would involve disclosing the data of another party, that other party should give their written consent to such disclosure.

7. There should be a clear rationale for the inclusion of lengthy extracts of narrative, dialogue or description, or the names of other individuals, places and dates. Consideration should be given to anonymising or coding data about third parties where this is practical.

8. Session notes provide an aide memoire for and evidence of the content and development of therapeutic work. They should be an authentic, usually brief summary of what was discussed, what interventions were employed and why. Clear distinctions should be made between fact, impressions and opinion. If the client's words are recorded, this should be made clear by the use of quotation marks and care must be taken that they are accurately quoted. Caution should be exercised in the use of prescriptive or diagnostic language unless supported by appropriate knowledge or training. Accurate and specific observations are preferable to interpretation. Members are guided to record risk factors and changes in client functioning or behaviour, CORE-OM, PHQ-9 or BDI-II, (and other measures of distress), score results and any related discussions and actions.

9. Process notes should be written as separate records to session notes. If process notes identify the client by name, or contain data that could identify the client, then they are deemed to be part of the client record and subject to the law and duty of confidentiality and data protection. Process notes that are rendered anonymous and do not contain any sensitive personal data or confidential information may be treated as separate from client records and destroyed when no longer required.

10. Members are guided to address the purpose and content of any client notes made or used for supervisory purposes. If supervision notes identify the client by name, or contain data that could identify the client, then they are deemed to be part of the client record and subject to the law and duty of confidentiality and data protection. Supervision notes that are

anonymous may be treated as separate from client records and destroyed when no longer required. Clients should be made aware that supervisors may have access to their personal data.

11. Members are guided to record in writing any onward referrals and contact or correspondence with GPs or other external services, including telephone conversations.

12. Specific and separate written client consent is required from the client to make, keep, use and dispose of audio or video recordings and for the use of client records for audit or research purposes. For data protection purposes these records are considered to be personal data.

13. Specific and separate written client consent is required for permission to share records with any outside person, organisation, service or agency, including GPs and the police, except where there is a risk of substantial harm to themselves or others, or when it is required by law, (see Practice Guideline 5 – Data Protection and Confidentiality / link). In the case of couple work, written permission must be obtained from both parties.

14. Members should address with the client the question of ownership, storage and disposal of client-generated records, such as letters, artwork, poems, narratives and homework tasks. Any agreement should be recorded in writing.

15. Correspondence with the client, by letter, text, email or telephone form part of the client record and, as such, are subject to the duty of confidentiality. Members are guided to retain accurate records of such correspondence.

16. Client records may refer to a client's present or past medication and any other health interventions, including number and frequency of consultations with health professionals. Any medical records should be treated as sensitive data and Members are guided to maintain them with appropriate care and attention to accuracy.

17. To protect confidentiality, Members must ensure that any records made in whatever form are kept secure, preferably in a locked cabinet, with access restricted only to authorised personnel. Where records are kept electronically, the computer system utilised should comply with current recommended IT security arrangements (see Information Commissioner website) including use of encryption, where appropriate, and strong passwords. There should be particular attention given to security on portable devices, such as phones, tablets and PCs.

18. Personal records should only be kept for as long as necessary and then they must be securely destroyed and disposed of. However, Members should weigh up the need to comply with legal obligations and also to ensure that sufficient records are kept to deal with any future claims. In most cases a retention period of 7 years is considered to be adequate, although this period may be longer in certain circumstances – see separate retention period table appended to this guide. Those working in the NHS will follow their internal procedure and the law.

19. Records of work with clients under 16 should be archived securely for five years after the Client reaches 18 years of age, except in the case of a child protection issue where this period may be longer – see separate retention chart. Note that, for data protection purposes, a child is considered to own their personal data at any age and is capable of giving consent to its use at the age of 13.