Clinics: client confidentiality and disclosure

Sources of confidentiality rules

The law of confidence is part of the common law (i.e. case law). Clinics and volunteers are also subject to the rules contained in SRA Handbook which contains specific provisions in relation to client confidentiality (see Chapter 4, Confidentiality and disclosure). See also the General Data Protection Regulations (GDPR) which imposes duties as regards the processing of data.

Introduction to confidentiality

Clinics are placed under duty to keep clients' affairs confidential. Volunteer solicitors and barristers are also under a professional duty to keep all clients' affairs confidential – this duty continues long after the clinic's involvement in the client's matter has come to an end and in most circumstances, will continue long after the client's death. The term "client" therefore is not limited to current clients, but also to former clients of the clinic.

All client affairs must be kept confidential unless disclosure is required or permitted by the law, or unless the client consents to the disclosure.

Any third parties should keep all client affairs confidential. Third parties receiving confidential information should be asked to sign a confidentiality agreement (an example of a confidentiality agreement is here).

In certain circumstances the misuse of the client's confidential information by employees / volunteers can mean that clinics are liable to the client for breach of confidence even in the absence of knowledge of the misuse.

What information is confidential?

To be protected by the law of confidence, information must be:

- **Confidential in nature**, meaning that it must have the "necessary quality of confidence". Additionally, it must not be something which is already in the public domain or public knowledge. Examples include: client files, instructions, advice and medical and other sensitive personal information, including certain financial information. [Remember, even if client information is already in the public domain and therefore not protected by the law of confidence, data protection law will still apply, potentially preventing disclosure or other data processing: see LawWorks' data protection guidance].
- **Disclosed in circumstances importing an obligation of confidence.** Advisers, such as solicitors, as well as student volunteers, are subject to strict confidence with regard to client's information by virtue of the solicitor – client relationship.

How to maintain confidentiality

As a general observation, sensitivity should be given when setting up clinics, spatially and otherwise, so as to ensure that clinic clients' privacy and comfort, as well as confidentiality, are maintained.

There are two main ways to protect information under the law of confidence:

- **Information should only be disclosed in circumstances importing an obligation of confidence**.
    - Ensure that employee and volunteer agreements are in writing and contain clear and appropriate confidentiality provisions (see the example of a clinic – volunteer confidentiality agreement below).
    - Certain third parties should be required to enter into confidentiality agreements (see below).
    - It might become necessary (subject to clients' consent) to request copies of clients' medical records, for example from a GP or Hospital and to disclose those records or information to certain third parties. Where disclosure is for a specific, limited purpose, confidentiality may be preserved for all other purposes.
- **Access to information should be managed / restricted**.

  There are a number of practical steps that clinics can take to establish and maintain confidentiality by restricting access:

    - The duty of confidence should be explained to all clinic staff, including volunteers. Clinic staff should be made aware of the practical ways in which clients' confidential information can be protected, as well as the ways in which confidence can be inadvertently breached and the consequences.
    - Ensure that confidential information being held is known about, where it is held and what the consequences would be should that information be inadvertently (or otherwise) disclosed.
    - Make sure that confidential information is communicated on a need-to-know basis only.
    - Give employees and volunteers practical guidance about keeping information confidential, including not to discuss clinic clients outside the clinic, on public transport and to take care when using laptops or mobile devices in public places like trains or cafes.
    - Secure confidential information both physically and electronically, for example (where appropriate and feasible) using firewalls, secure emails or encryption. Consider using techniques to prevent USB keys being used with clinic computers and ensure that there are appropriate

restrictions or policies in place to deal with employee or volunteers using their own devices.

- Keep records that show what matters employees or volunteers have worked on.
- The way(s) in which clients may be contacted should be agreed at the time of the interview and noted on the case record.
- If confidential records are stolen in a break-in or in any other way, the theft must be reported to clinics' coordinators and the police. The report to the police must stress the confidential nature of the records and the importance of them being returned unread if they are found.
- Remind departing employees and volunteers of their obligations of confidentiality and ask them in writing to confirm that they have returned all clinic property.
- Audit security procedures regularly.

There are a number of practical steps to establish and maintain confidentiality in respect of data processed and stored electronically:

- Know what data is held, where it is held and what the consequences would be should that data be lost or stolen.
- Access to systems which are no longer in active use and which contain personal data should be removed where such access is no longer necessary or cannot be justified.
- Passwords used to access PCs, applications, databases, etc. should be of sufficient strength. A password should include numbers, symbols, upper and lowercase letters. If possible, password length should be around 12 to 14 characters but at the very minimum 6 8 characters. Passwords based on repetition, dictionary words, letter or number sequences, usernames, or biographical information like names or dates should be avoided.
- Employees and volunteers who retire from clinics should be removed immediately from mailing lists and any access permission.
- Procedures should be put in place in relation to the disposal of files (both paper and electronic) containing personal data.
- New staff (including volunteers) should receive appropriate training before being allowed to access confidential or personal files.
- Appropriate filing procedures (including, in terms of complying with any relevant professional obligations) - both paper and electronic - should be drawn up by clinics Coordinators and followed. Client files should be systematically and regularly reviewed for confidentiality by Clinic Coordinators.

- Standard unencrypted email should ideally not be used to transmit data of a personal or sensitive nature. Such data should be shared either through file encryption or through the use of a secure email facility which will encrypt the data being sent. Check clinic's email server as to whether and how emails can be encrypted or otherwise secured.
- Data that is accessed via remote access ideally should not be copied to home PCs or to portable storage devices, such as laptops, memory sticks, etc. that may be stolen or lost.
- Clinics should consider whether they require a bring-your-own device policy to cover whether staff are allowed to use their own devices (which may lack up to date institutional antivirus software), in what circumstances and with what safeguards?
- Memory sticks containing client information should be encrypted. Encrypted USB memory sticks are widely available and relatively inexpensive.
- Laptops: portable devices should be password-protected to prevent unauthorised use of the device and unauthorised access to information held on the device. In the case of mobile phones, both a PIN and login password should be used.
- Private, sensitive or confidential data should not be stored on portable devices. In cases where this is unavoidable, all devices containing this type of data should usually be encrypted or otherwise secured.
- Anti-virus/Anti-spyware/Personal Firewall software must be installed and kept up to date on portable devices.
- Laptops must be physically secured if left at the clinic office overnight. When out of the office, the device should be kept secure at all times.

Client access to records

Clients have the right to see their own case records and letters written or received on their behalf. Copies may be given to clients, but the originals should be retained in clinics' files.

Where a client has made a complaint or a claim involving liability for wrong advice against the organisation any records or correspondence relating to the claim or complaint is confidential to the organisation and should be stored separately to the original case record.

Conflict situations

In rare situations the duty of confidentiality and the duty to disclose may come into conflict with each other. If you are in any doubt you should consult the SRA Handbook and contact the SRA ethics line on 0370 606 2577.

Breach management

A breach can happen for a number of reasons, including loss or theft of data or equipment on which data is stored (including break-in to a clinic's premises); human error, such as referring to confidential information outside the clinic environment or other erroneous or mistaken disclosure; inappropriate access controls allowing unauthorised use; equipment failure; access where information is obtained by deceiving the organisation that holds it.

Actual or potential breaches of confidentiality should be notified to clinics' coordinators. Clinics Coordinators must take immediate remedial action, including any necessary action to prevent any further breaches of confidentiality. A breach of confidentiality might also indicate the need for further staff training and/or management.

Clinics coordinators should refer to clinics' insurance policy in the event of a breach of client confidentiality.