Protecting and maintaining client confidentiality

Issued on 9 January 2015

Who is this guidance relevant to?

This note reminds SRA authorised bodies and persons of their professional duties when dealing with confidential information. This advice does not form part of the SRA Handbook and is not mandatory, but the SRA may have regard to it when exercising its regulatory functions.

Our concerns

There is a risk that confidential information is shared with third parties when clients or prospective clients have not provided informed consent to such sharing. The risk is greater for example, in complex firm structures, particularly global law firms, consisting of group structures, often comprising a number of separate legal entities, typically with common branding and operating in different jurisdictions not all of which are subject to SRA regulation or oversight. Such entities may also have corporate or individual members or directors who are not authorised by the SRA.

There are also a number of circumstances and pressures facing firms where they are allowing third parties, such as other law firms, external funders, consultants, or non-solicitor administrators, access to confidential client information without client consent. This may occur where such third parties are advising the firm on its financial viability or considering a possible merger or acquisition.

In addition, firms should not continue to act for a client(s) where material information cannot be disclosed and such situations give rise to a conflict of interests.

The SRA Principles

The most relevant Principles in relation to your duty of confidentiality are Principles 3, 4 and 6, that you must:

3. not allow your independence to be compromised;

4. act in the best interests of each client; and

6. behave in a way that maintains the trust the public places in you and in the provision of legal services

SRA Mandatory Outcomes

As well as the relevant Principles, you will also need to ensure that you achieve the Outcomes relating to conflict of interest (Chapter 3) and confidentiality and disclosure (Chapter 4) in the SRA Code of Conduct 2011 (the Code). In particular:

- you do not act if there is a client conflict, or a significant risk of a client conflict (O3.5) (unless the circumstances set out in O3.6 or O3.7 apply),
you keep the affairs of clients confidential unless disclosure is required or permitted by law or the client consents (O4.1); and,

you have effective systems and controls in place to enable you to identify risks to client confidentiality and to mitigate those risks (O4.5).

Our expectations

All regulated firms and persons should protect their clients' confidential information. Protection of confidential information is a fundamental feature of your relationship with clients. It exists as an obligation both as a matter of the common law and as a matter of conduct. It is one of the professional principles set out in section 1(3)(e) of the Legal Services Act 2007 [http://www.legislation.gov.uk/ukpga/2007/29/section/1]. The duty arises in relation to the confidential affairs of prospective clients before a formal retainer arises as well as retained clients. This duty continues after the end of the retainer and even after the death of an individual client.

Firms should identify risks to client confidentiality and have in place effective systems and controls to enable them to do so and mitigate any such risks arising from the potential disclosure of information.

Firms and individual practitioners should note the need to distinguish their duties in conduct from the concept of legal professional privilege. Firms must consider the importance of client confidentiality and appreciate that legal professional privilege can only be waived by the client (and not the firm). They should also be mindful of restrictions on the passing of confidential information in particular cases, for example cases involving children.

It should be borne in mind that all members of the firm or in-house practice, including support staff, consultants and locums, owe a duty of confidentiality to all clients.

The duty of confidentiality to all clients must be reconciled with the duty of disclosure to clients. This duty of disclosure is limited to information of which you are aware is material to your client's matter. Where firms cannot reconcile these two duties, then the protection of confidential information is paramount.

Disclosure of confidential information is only allowed where the client consents to it and it is in their interests or is permitted by law. Before approaching a client for consent, firms should consider whether disclosure is essential to proceed with a specific matter.

Consent to disclosure must be informed consent. Information for clients should explicitly set out the circumstances when and to whom information will be made available, why they would need to access information and why disclosure might be necessary. The client should have been given an opportunity to object to disclosure, rather than consent being assumed.

In the case of assessing a firm's financial stability or seeking to acquire a practice, for example, is it necessary for external people to see any client files?

Due diligence or an assessment of a firm's viability should be focused on the firm's financial situation, financial records, accounts, financial forecasts and forward plans. Firms must take steps to minimise the risk of third parties having access to client information.

Where information is to be shared with a third party, for example, with client's consent, firms need to consider:

• What is the purpose of such access and can the purpose be achieved in other ways?

• Should there be limitations on the access?

• Is the firm satisfied that seeking the client's consent to disclosure would not in any way be contrary to the client's best interests?
Is the firm satisfied that the client has genuinely given informed consent?

When firms legitimately share the confidential information of prospective and retained clients with third parties, firms should consider how best they can mitigate the risks and if appropriate, act to protect confidential client information in the hands of such third parties, whether by formal confidentiality agreements between the entities or otherwise. It is advisable that a formal confidentiality agreement should therefore be in place to ensure proper protection and controls. This is additional to obligations placed on a firm by the Data Protection Act 1998 [http://www.legislation.gov.uk/ukpga/1998/29/contents].

**Specific situations**

**Complex firm structures**

Before undertaking conflict checks and other due diligence firms need to actively consider the risks and whether it is in the best interests of that prospective client to share its confidential information with other authorised or non-authorised bodies within a group structure. This applies particularly to those in other jurisdictions, including overseas or connected practices or Verein participants, where they are separate entities. This obligation continues to apply during the course of the retainer.

Where relevant, firms should provide present and prospective clients with an explanation of the group structure before seeking their informed consent to the disclosure of confidential information to separate legal entities in the group or non-authorised corporate or individual members or directors.

As part of a retainer, firms may in terms of their engagement, also seek consent from clients to share, during the course of the performance of the retainer, a broader range of client confidential information with other group entities or corporate or individual members or directors who do not form part of the SRA authorised firm. If so, firms should again provide a clear explanation of any group structure and the need for disclosure of information to ensure that such consent is informed consent.

**Case example**

Firm A is part of a group structure with offices across numerous jurisdictions. Externally, the group presents itself as ‘one firm’ with common branding. In fact, Firm A is a limited liability practice ("LLP") incorporated in England & Wales. It has a branch office in Europe. The other 5 offices in the group are separate entities, including a traditional partnership in Hong Kong, a Delaware registered LLP in North America and a separate subsidiary in South Africa. The group has set up a business acceptance unit in Hong Kong, which is staffed by a team of people who conduct money laundering and conflict checks on behalf of all offices. If the unit identifies a potential conflict, it sends details of the matter to the relevant business partners, wherever they are based. The firm’s standard terms of engagement set out details of the separate entities in the group and also explain that there are separate agreements in place between the entities regarding the sharing of confidential client information and personal data.

The partner sends details of his client and the potential acquisition target to the business acceptance unit in Hong Kong who identify a possible conflict. The week after this, stories emerge in the press of an overseas Government agency hacking into law firms’ systems.

In our view, the partner should specifically discuss with the client details relating to the group’s ownership structure and that the initial conflict check will be undertaken and/or shared with other entities. There may be circumstances where material is seen by an office in a foreign jurisdiction and partners should actively consider whether it is in the client's best interests for the client's information to be subject to restricted access.
Mergers and acquisitions

Economic factors and business needs may dictate decisions a firm takes and in certain circumstances, may encourage firms to seek to merge, or acquire in order to achieve their business aims. Firms that are undertaking professional risk due diligence during the merger and acquisition process have a number of issues to consider, including the need to ensure that client confidentiality is not put at risk.

During negotiations sufficient steps need to be taken to protect confidential client information and, where appropriate, to seek clients' consent to any disclosure of confidential information.

Firms also need to have regard to their obligations to protect price-sensitive information relating to the firm and/or their clients.

Case example

Firm A has decided that it will cease trading in the next six months and to ensure continuity of client matters is looking for firms to acquire the business. Firm B is interested in acquiring Firm A and is carrying out the necessary due diligence and insists on reviewing client files despite being aware of need for the client affairs to be kept confidential. Firm A suggests that a non-disclosure agreement is put in place as both firms will be bound by the agreement and their professional obligations.

At the point of disclosure the acquisition has not taken place and due to the deal subsequently falling through, the acquisition does not go ahead.

Confidential information has been shared and despite best intentions and the force of the non-disclosure agreement, Firm B may have acquired knowledge that will damage, or be used against, the relevant client.

In our view, it cannot be argued that no merger or acquisition can be completed without disclosure of client files. A merger or acquisition can take place without making any disclosure that results in a breach of the requirements set out in Chapter 4 of the Code.

Other options to establish the viability of a merger or acquisition should be explored for example, accounting and billing records, records of all active and closed matter, representations and warranties given by Firm A as to the nature, quality and quantity of client matters, and work in progress.

Outsourcing and services provided across different jurisdictions

Where firms outsource services, they will need to consider the arrangements they have in place to ensure adequate protection of clients' confidential information and also the obligations set out in Chapter 7 of the SRA Code of Conduct 2011. Clients may not have agreed or understood that their confidential information may be considered by an unregulated third party and that in certain cases, information will be considered in a foreign jurisdiction.

Firms must consider the electronic security of information held and manage potential vulnerability of electronic information being destroyed or passed to a third party (including separate entities within a group) without the client's informed consent.

Firms should actively consider clients’ best interests before sharing information or in granting rights of access to information held on common IT systems, particularly where information is shared across different jurisdictions.

Cloud computing

Cloud computing may be an attractive concept for a number of firms and may provide benefits
of efficiency, flexibility and high utilisation that, in turn, could result in reduced capital investment costs and lower operational expenditure.

There are many benefits associated with cloud computing but in assessing its value to a firm, it should also consider how best to manage the risks and challenges. These include:

- governance, management and updating of data;
- management of software services;
- monitoring of products and processes;
- reliability and availability of systems and infrastructure; and
- security of information and data.

Confidential client information stored in a cloud, potentially in a foreign jurisdiction may be more vulnerable to disclosure. Firms need to be able to demonstrate that they have considered the risks and that clients have consented to their information being stored in a particular way.

The Data Protection Act 1998 requires that personal information is handled in a manner that ensures that key principles and legal obligations are properly adhered to. There is an obligation for firms to clearly state where client information is being held. However, this may be difficult for firms if service providers themselves are unaware of the exact locations.

**Further help**

If you require further assistance with understanding your obligations in relation to anything please contact the Professional Ethics Guidance Team [contact-us].

Use [www.sra.org.uk/confidentiality](http://www.sra.org.uk/confidentiality) to link to this page.