IALS INSTITUTE OF ADVANCED LEGAL STUDIES | SCHOOL OF ADVANCED STUDY UNIVERSITY OF LONDON

THE LEGAL RECORDS AT RISK (LRAR) PROJECT

Project patrons: William Twining, Professor of Jurisprudence Emeritus, UCL and Avrom Sherr, Emeritus Professor, IALS

Project Director: Clare.cowling@sas.ac.uk

http://ials.sas.ac.uk/research/areas-research/legal-records-risk-lrar-project

Legal Records at Risk Guideline 4: advice to legal institutions on confidentiality and research access to records

Contents

Legal records and historical research

Private sector "legal" records have never been collected systematically in the UK other than by a very small number of specialist archives[1]. Collecting in the public archives sector has tended to be ad hoc (ie as and when individuals or legal bodies such as law firms decide to clear out some of their records). As a result research using legal records is inevitably weighted towards the pre-twentieth century study of government policy, legislation and the courts, producing a historical picture of the UK's legal framework and legal services which is skewed towards the policies and actions of central government. One reason for this dearth of private sector legal records may be the legal profession's legitimate concerns about record confidentiality and a mistrust of or misunderstanding about how archival repositories respect and manage this, plus the reluctance of archives to accept deposits of records with unfeasibly long closure periods. These issues, and how to resolve them, are discussed below.

Legal records and confidentiality

The Legal Records at Risk project seeks to broaden the concept of "legal" records from the traditional definition of them as court records or formal documents such as deeds to the

[1] Such as the Archives of the Inns of Court, the Law Society and the Records of Legal Education Archives. Not to be confused with the almost universal practice followed by institutions of depositing their non-current records en masse in a warehouse, basement or lower-tier server for indefinite storage.

business records of private sector institutions with a connection to the law such as law firms, barristers' chambers, regulators, membership bodies, pressure groups and educational bodies as well as to legal records created and held by businesses, companies, charities etc. "Business records" will include corporate governance records, policy and procedures files, marketing, public relations and accounting records; as such they will be bound by the usual conditions of commercial confidentiality and the Data Protection Act. In this respect the records of a legal institution should not be treated any differently to the records of other private sector organisations when seeking to make them available for research and so there should be no particular confidentiality problems in depositing them in archives. There is, however, one exception to this rule as follows.

Legal professional privilege and client confidentiality

All client information is held by legal institutions under a long-term obligation of confidentiality[2]. Legal service providers are bound by their professional codes of conduct to keep client and complaints information confidential (see **Appendix**). This may be the primary reason both for the reluctance of legal providers to make *any* information about their work available for research despite the fact that many of their records will not be subject to client confidentiality. It may also explain why archive repositories may not wish to collect and store such records where unfeasibly (in archival terms) lengthy closure periods are demanded.

How long does client confidentiality last?

The question is whether this guarantee of confidentiality is in perpetuity or for a limited (in archival terms) period. None of the Codes of Conduct listed in the **Appendix** specify a length of time, so the next question is whether there is a tacit assumption of confidentiality in perpetuity, and whether this has ever been challenged.

'Actionable Breach of Confidence' is a useful base-line for discussion. An action for breach of confidence can only be brought by a deceased person's personal representative – ie executor or administrator. Once that person can be proved or presumed dead (say 82 years after death of the data subject, if we assume that a personal representative must be at least 18 – though 16 might be safer), there is no legal risk in releasing the information. This may be useful in dealing with the confidentiality for individual clients but is more problematic for companies, which do not "die" unless they are wound up or dissolved. It is not an insuperable barrier to eventual release of client information but it may well be an obstacle too far for archive repositories, which as a rule simply cannot afford to sit on material for hundreds of years until they can make it available.

Legal bodies presumably have a responsibility not to transfer client information to a third party unless and until the files are no longer subject to an obligation of confidence (ie the client has died and the time limit for all legal actions has expired or the company has been dissolved/wound up), when they can legally be destroyed or sent to an archive repository.

[2] The 2004 Clementi Report *Review of the regulatory framework for legal services in England and Wales* describes confidentiality thus (p.23): "The codes of conduct of the legal professional bodies generally require lawyers to keep clients' affairs confidential. Communications between a client and his lawyer may be subject to Legal Professional Privilege (i.e. certain communications between a client and legal adviser in the context of obtaining legal advice or assistance are protected from disclosure, even in legal proceedings)."

It appears to be easier to say that this responsibility implies confidentiality in perpetuity than to make decisions as to when client files become redundant and can safely be disposed of. Yet client files cannot be held indefinitely, not least because where individual clients are concerned such retention would be in breach of the Data Protection Act[3]. LRAR suggests, therefore, that legal institutions and practitioners look afresh at the way in which they manage their client files and make carefully considered decisions as to disposal.

Archives and confidentiality

All archival repositories[4] have well developed techniques for dealing with 'sensitive' records, including closure periods and conditions on access and use; they operate under strict confidentiality guidelines and follow The National Archives' advice to close all records for at least 20 years and personal data for 100 years[5].

Deposit agreements: any legal institution or individual depositing records with an archives can also stipulate their own confidentiality requirements (though the archives, equally, can refuse to accept records with an unfeasibly long closure period). Where a private sector organisation deposits records in an archives an agreement is always drawn up specifying the length of time the records should be closed to public access unless the depositor is happy with the archives' own standard access rules.

Standard closure periods based on confidentiality applied by archival repositories, after which records may be made available for research, are as follows:

- Records in general: all records held by an archives are closed for 20-30 years other than material already in the public domain or for which permission for earlier access has been given by the depositing organisation/individual.
- Commercial confidentiality: usually assumed to expire after 20-30 years, unless a specific stipulation is made by the depositing body that it should be closed for a longer period.
- Personal data: the Data Protection Act specifies that the term "personal data" only applies to the data of living individuals, so archives close such data for 75-100 years as recommended by The National Archives. Once the data subject is deceased or presumed deceased the Act no longer applies. In certain circumstances personal data may also be examined for bona fide research purposes provide a legally binding guarantee of anonymisation is signed, or research bodies may redact personal data to make it available[6]. In other words, client confidentiality is not an insuperable barrier to making client data available for research.

There is, therefore, no reason for any legal institution to be concerned that an archive repository will not professionally manage access to deposited records.

---

[3] See Schedule 1 and the 8 Data Principles, in particular Principle 5: "Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes."

[4] The term "Archival repositories" in this guideline refers to places where archival records (ie collections of records selected for long-term preservation as evidence of the activities of organisations or individuals) are stored, preserved and made accessible. The term does not refer to the mass storage of information in 3rd party records stores, basements or lower tier servers pending disposal.

[5] TNA Code of practice for archivists and records managers under Section 51(4) of the Data Protection Act

[6] Section 33 of the Data Protection Act 1998 refers

Appendix: Confidentiality Codes of Conduct and Practice Guidelines

The Bar: the Bar Standards Board Handbook states in S12: "The regulatory objectives of the Bar Standards Board derive from the Legal Services Act 2007 and can be summarised as follows…that the affairs of clients are kept confidential." and rC106 "All communications and documents relating to complaints must be kept confidential".

Solicitors: the SRA Code of Conduct 2011 states in Ch 4 Client confidentiality: "firms are required to have effective systems and controls in place to identify risks to client confidentiality and to mitigate those risks…... Protection of confidential information is a fundamental feature of your relationship with clients. It exists as a concept both as a matter of law and as a matter of conduct. This duty continues despite the end of the retainer and even after the death of the client."

Arbitrators: institutions have their own rules eg Article 30(1) of the Rules of the London Court of International Arbitration states: "Unless the parties expressly agree in writing to the contrary, the parties undertake as a general principle to keep confidential all awards in their arbitration, together with all materials in the proceedings created for the purpose of the arbitration and all other documents produced by another party in the proceedings not otherwise in the public domain - save and to the extent that disclosure may be required of a party by legal duty, to protect or pursue a legal right or to enforce or challenge an award in bona fide legal proceedings before a state court or other judicial authority."

Mediators: the Chartered Institute of Arbitrators' Practice Guideline 1: Confidentiality in Mediation states "Save as required or permitted by law… the Institute, the parties, their representatives, their advisors and the mediator(s) shall keep confidential all information (whether given orally, in writing or otherwise) produced for, or arising out of or in connection with, the mediation passing between any of the participants and between any of them and the mediator made for the purposes of the mediation, including the fact that the mediation is taking place or has taken place…The mediator's duty to protect the confidentiality of the mediation proceedings commences with the first communication to the mediator, is continuous in nature, and does not expire upon the termination, for whatever reason, of the mediation under Rule 11. The mediator's duty extends to all information relating to the mediation proceedings, even indirectly, such as previous invitations and/or negotiations leading to mediation, terms of the agreement to mediate, appointment of mediators and performance, or non performance, of the settlement agreement. All records, reports, or other documents received by a mediator, as well as all notes taken by the mediator during, with reference to, or for the purposes of, the mediation should be returned to the parties or kept secure until no longer needed for any purpose relating to the mediation and then destroyed."

Conveyancers: Outcome 3.6 of the Council for Licensed Conveyancers' Code of Conduct requires that: "Clients' affairs are treated confidentially (except as required or permitted by law or with the Client's consent)"

Notaries: Ch. 17 Recordkeeping and file storage of the Master of Faculties Code of Practice states: **"**A notary's records are as a general principle confidential [Practice Rule 23.6]".

Patent and Trade Mark Attorneys: the Chartered Institutes of Patent Attorneys and Trade Mark Attorneys have produced joint Business practice guidance containing many references to the need to safeguard clients' confidential information, including information of clients for whom the attorney no longer acts.

Will writers: the Institute of Professional Willwriters' Code of Practice states: **"**Members shall act with independence and integrity, maintain proper standards of work and keep the affairs of the Client confidential."[S.5.1]