APS Australian Psychological Society

APS Position Statement

# Record Keeping in Organisations

December 2020

## Contributors

David Cherry
Director/Principal Psychologist
David Cherry and Associates
Castlemaine Vic 3450

Guy Coffey
Practice Advisor (Legal, Forensic Complex Needs Portfolio)
Foundation House
Brunswick Vic 3056

Geoff Gallas
Director Occupational Psychology
Health Policy Programs & Assurance Branch
Joint Health Command
Department of Defence
Canberra ACT 2000

Jillian Harrington
Director/Principal Psychologist
Southern Cross Psychology
Penrith NSW 2750

Caroline MacLeod
Clinical psychologist
Devonport Tas 7310

Lil Vrklevski,
Principal Psychologist, Director Psychology and Allied Health and Professional Senior Psychology
Mental Health
Sydney Local Health District
Camperdown NSW 2050

Dr David Stokes
Director/Principal Psychologist
David Stokes and Associates
Ballarat Vic 3350

Contact:
Dr Tony McHugh
T.McHugh@psychology.org.au

## Disclaimer and Copyright

This publication was produced by The Australian Psychological Society (APS) to guide best practice in managing psychological records within an organisational setting. This Position Paper (this Paper) aims to provide a framework for making decisions regarding professional record keeping. This Paper is not intended to describe these requirements fully, replace clinical judgement and decision-making or intended as legal advice. Psychologists are professionally obliged to be familiar with the legal and ethical requirements for record keeping in their specific professional contexts organisations and jurisdictions.

While every reasonable effort has been made to ensure the accuracy of the information provided in this Paper, no guarantee can be given that such information is free from error or omission. The APS, their employees and agents shall accept no liability for any act or omission occurring from reliance on the information provided or the consequences of any such act or omission. The APS does not accept any liability for any injury, loss or damage incurred by use of or reliance on this paper. Such damages include, without limitation, direct, indirect, special, incidental or consequential damages. The information provided by the APS does not replace the need for practitioners to obtain independent legal advice specific to the situation, where necessary.

# Table of Contents

## Introduction and purpose

For many years, the APS position on psychological record management supported a two-file system for managing psychology records. This approach no longer aligns with modern psychology practice.

Contemporary psychology practice needs to enable electronic record (e-record) systems and multidisciplinary team (MDT) work. The introduction of legislation that permits access to records by government instrumentalities [e.g., where there is domestic violence, sexual assault of minors or planning or a reasonable suspicion of planning for mass scale anti-social criminal acts (such as terrorism) requires that Services respond to requests for information about such activities]. In the context of these and other developments, there has been a strong move toward keeping single records in the public and non-government sectors. Simultaneously, the keeping of dual records is increasingly becoming a concern for privately practising psychologists.

The use of e-records is now commonplace within organisations that employ psychologists. Such e-records provide great advantages in efficiency for organisations, in that they can, where there is a legitimate need to know:

- be shared appropriately among professional staff and other agencies involved in the client's care
- improve efficacy in standard practice
- be a cost-effective method of storing and maintaining files, and
- provide robust security through use of passwords, logins and audit trails.

The utilisation of e-records can, however, raise concerns around the confidentiality of, and access to, records. As detailed in section four of this paper, a single e-record is professionally and ethically acceptable, where it includes appropriate security features that control and monitor access to information contained on that record.

This position paper articulates a new APS position on psychology record keeping in organisations that is suitable for e-records and aligns with the pertinent privacy and record-keeping legislation and provides high level client confidentiality. It is the result of the deliberations of an APS expert working group, the membership of which comprised private practitioner members with long-standing peer-acknowledged leadership status and senior office holders from the public and non-government sectors, who in some cases possessed dual professional qualifications in psychology and law.

## The nature of the single record

A single record will inevitably contain information that will be available to a range of audiences. This will include summary information.

The sharing of this base-level information enables other professionals in the broader care team to provide services and interventions where they have responsibilities for care of the client and both a right of access to and legitimate need-to-know that information. This type of information is necessarily concise in form (e.g., as might apply in a basic or intake page), but includes sufficient detail to clearly communicate client demographics and the essential elements of the intervention plan developed and services provided for the knowledge of the next practitioner.

Although there will be inevitable organisation-by-organisation variations in the composition of this summary level of information, it will typically include brief versions of the following:

- the date and time the psychology service took place
- who was involved
- the purpose of the psychological service
- the type of psychological service delivered
- how the psychological service was provided (e.g., face-to-face, Skype or telephone)
- the setting in which the psychology service took place (e.g., community clinic, outpatient service or inpatient ward)

- a summary mental state examination (MSE), if appropriate
- diagnoses and cases, as appropriate
- a summary risk assessment and plan for intervention, if appropriate
- appropriate alerts, and
- the date of any next appointment.

A single record will also inevitably contain information in which the psychologist substantively records the nature and content of the service provided to the client. This is likely to include sensitive information.

Information recorded in the summary information area of the record is not typically duplicated in this sensitive information area. Conversely, sensitive information need only be documented in the summary area of the file if it is required to mitigate risk, facilitate future sessions or otherwise guide interventions and decision making.

Such information is typically stored apart from summary information. What is included at this sensitive information level will differ by organisation type and work environment. As a general guide, however, access to such information will be restricted to professional and clinical staff directly involved in the provision of care to the client. It is important that this information is flagged in a manner that is transparent and easily understandable for all staff of the employing organisation who may have a right and need to know about it. Access to this information is best constrained to those items of information that are only accessible or useable by an appropriate professional.

Identifying what information is included and who may access it will best be achieved by structuring the client record in such a way that it leads with a clearly marked summary section, which can then be followed by more detailed notes arising from the assessment and/or intervention, all of which would be part of the same over-arching record. Alternatively, the additional, more detailed sensitive notes might be attached to the over-arching record as a separate document, rather than simply entered into the primary record alongside the shared file component. This would effectively maintain a single-file system, while at the same time adding a conceptual gap or separation between the shared part of the file and the attached confidential part.

Sensitive information may consist of materials (e.g., psychometric test scores, test profiles, interpretations, and the like) that require advanced levels of psychological training to understand and use them effectively. Those with access may include psychologists or a wider MDT, depending on the organisational setting. For instance, in health organisations that operate according to a community case management framework, this typically includes mental health clinicians such as psychiatrists, psychiatric nurses, occupational therapists, speech pathologists, social workers, chaplains and peer support workers. Access to the client record by a range of professionals may also be permitted by law specific to that sector; for example, in domains like Corrections, Juvenile Justice, Justice Health and Child Protection, where information sharing is seen as critical and relevant to the wellbeing, risk-management and best interests of the client.

Regardless of setting, it is important to, where possible and practicable, restrict the following information to this sensitive part of the file:

- detailed descriptions of assessments and interventions applied
- detailed description of client MSE, vulnerabilities and, appropriately de-identified, protective factors
- diagnoses and case formulations
- verbatim client and relevant-other comments, statements and observations
- objective data and subjective professional observations
- analyses of behaviour change
- reference to expert opinions and judgements, as appropriate
- a summary of the clinical impression/working hypothesis, if appropriate
- details of reports, information prepared for internal/external parties
- consent form(s)

- psychological tests, and
- any other supporting data.

## Obligations of organisations and practitioners

Best practice in record keeping dictates that organisations have clear policies and procedures governing who, within and outside the record-originating organisation, has access to client information, under what circumstances and to what extent. These policies and procedures must be articulated in plain language policy statements. Such statements must inform clients about the nature of the record system and its safeguards and protections, enable psychologists to assist clients to fully understand such matters and provide for a written acknowledgment by clients that they have so been informed about, and understand, the protocols surrounding the recording of information about them.

Privacy legislation makes clear that psychologists can only access information about clients for whom they are directly providing an intervention. They cannot access their own record, those of family members, friends, associates or similar others or other clients for whom they do not have a direct professional relationship.

Where organisations have policies and procedures regarding recording and retaining clinical notes, psychologists are obliged to adhere to them as part of their employment contract. For example, if required by the organisation to use a single e-record, a psychologist must not keep a separate set of detailed notes for their own use.

Psychologists must also consider the potential readership of their notes. They need to be mindful that what they enter into a client record may, at some stage, be read by the client and other parties, including professionals and others within and external to the organisation. No information should be recorded which is not relevant and would, hence, constitute a breach of the individual's right to privacy. The APS Code of Ethics is consistent with this and requires that psychologists are aware of and understand the ethical and legal standards related to managing confidential client information in a given setting.

Psychologists must exercise their professional judgement in determining what relevant sensitive personal information to record in the file. For example, certain details revealed by the client or observed by the psychologist in providing psychology services, may be relevant as evidence supporting (or otherwise) claims of behaviour change, differential diagnosis or other response(s) to intervention. This will vary according to client presentation, the organisational environment involved, the purposes of that consultation, the role of the psychologist and their professional training. Where the psychologist is unclear about the potential risks involved to the client in others reviewing information or has other concerns regarding the nature of requests to access a client's records, they must refer to their organisational policy and/or delegated officer for advice.

There is a professional responsibility to ensure sufficient information is recorded to enable another psychologist or professional to continue to provide interventions and services to the client if required. In making summary level information entries, psychologists need to be aware that other members of staff within the employing organisation, including any MDT members involved in the provision of client intervention(s), may need to access that record. It is, accordingly, important that the information included allows for the best description of the client's presentation and intervention planning, using terms that would be understood by the broader team. This also requires a balance between the need for brevity and thoroughness. Hence, the practitioner must consider whether decisions and recommendations about interventions and client presentation are adequately detailed to justify the actions undertaken to a future reader.

Risk to the client, together with an obligation to act in the client's best interests and accountability for one's professional decisions, need to be balanced with accurate, full and factual recording of sessions in the client record. Accordingly, while the issues of who might subsequently access those records and how they might be used are important, the most important factor is to ensure that the taking of notes and maintenance of records is done in accordance with best professional practice. To ensure the appropriateness of records, psychologists in organisations

must be clear about who the client is. To illustrate, the client can be a third party referring an individual for an assessment, a customer of the service involved or an employee of the organisation. How records are kept needs to reflect this. There is also a need to highlight what should be done with information gathered or reported about a client. This should be contained in a Memorandum of Understanding with other organisations, agencies or parties; for example, by restricting to whom information can or cannot not be further disseminated or included in correspondence.

There may also be occasions where clients discuss matters with their psychologist which they do not wish to be recorded on their record. Under some circumstances, psychologists and their clients may reach agreement to keep certain client information confidential and not record them in the file.

Decisions as to whether to record or keep information confidential are, however, not matters of individual judgement and are informed by legislation, organisational policy and the APS Code of Ethics (standard A.3). Such decisions should be exercised with caution by psychologists for two reasons. First, an issue that does not seem relevant at the time *may become* relevant later or when seen in a different context. Second, that issue might be highly relevant to a third party (including an employer); such as, in the context of court proceedings or a Freedom of Information (*FOI*) request. This exercise of judgement would necessarily include an assessment of the potential risk (i.e., the risk associated with both including and not including the information) to the client or a third party should that information become known.

## Critical principles for safeguarding client information in e-records

Best practice dictates that organisations act to ensure sufficient safeguards exist to protect client confidentiality and the client-practitioner relationship and meet the underpinning legislative framework. Where organisations centralise records in a single e-record system, the use of privacy caveats like “psychology-in-confidence” or distribution limiting markers such as “Personal: Psychology/Health Information” alert potential readers to the sensitive personal nature of the information contained in the client file are a useful starting point. As previously observed, this needs to be in accordance with the “need-to-know” principle (noting that different providers within an MDT might have different levels of need-to-know associated with their role within the treatment team and/or their wider organisational role).

Protocols relating to confidentiality, note taking, storage, disposal and security must be made known to staff and clients. Such procedural documentation should indicate:

- what, how, when, and under what conditions, records are created, maintained, protected and stored
- the situations in which access by others to the client record might be permissible
- the means by which clients will be informed about organisational record storage policies and protocols and given the opportunity to acknowledge being advised about those requirements
- processes for dealing with consent where clients are temporarily or permanently incapable of giving consent and
- how any requests for anonymity will be managed.

Such policy and protocols should also be subjected to periodic review to ensure they remain consistent with developments in the law.

The APS views the use of a single e-record as appropriate from a privacy and confidentiality perspective, provided it operates with specific safety features. To assure this, as a minimum, it is recommended that organisations adopt the following security features in their policies and protocols.

i. **The system permits access to authorised users, based on legislation, organisational policy and role descriptions.**

The record system software must meet the pertinent legislative standards for e-records. It must also comply with privacy legislation; that is, the Commonwealth Privacy Act (1998) and any applicable state-based privacy legislation.

ii. **The system restricts access to authorised users on a need-to-know basis.**

Examples of the need to know include situations of risk to the health or safety of clients, other individuals or the public (see Australian Privacy Principles: APP's chapter 6 - Use or disclosure of personal information), case management, multidisciplinary team work and where there is a requirement for information to be shared between government instrumentalities and agencies (e.g., child protection and family violence).

iii. **All information entered is classified with reference to its level of accessibility.**

Records are restrictable according to the need to know and the levels of access within the record system are constructed and organised to constrain user access in line with legislation and policy that is reflective of that legislation.

iv. **Users are allocated personal identifiers and use them to gain access to records.**

Personal identifiers are allocated to staff by the organisation's records administrator and are securely maintained in a register. Staff cannot access client information unless they use their allocated identifier and a personal password that meets the organisation's security requirements.

v. **Users are classified in respect of the levels of information they can access.**

Authorised users are accredited to appropriate security classifications and distribution limiting markers. All information within the records system in place is managed and handled in accordance with these requirements.

vi. **Users may only access information they have clearance to access.**

Authorised users are only permitted to access the information needed to perform their employed role (as per their identified and agreed scope of practice). They must have the legal right to access the information concerned and a genuine need for that information. This access right may operate temporarily (for specific reasons) or on an ongoing basis.

vii. **There are clearly stated rules that govern access to the system.**

Authorised users (including administrative and professional staff) are informed, via induction and training, of the privacy and confidentiality rules applying to the creation, maintenance and accessing of client records and are required to undertake to adhere to them. An organisation-wide independent audit or regulatory system for the e-record system must be in place. Organisations must monitor compliance with the stated rules via periodic, ad hoc and as necessary audits. Unauthorised attempts at access must be immediately and automatically reported to the organisation privacy regulator, who must investigate such occurrences.

viii. **The applicable rules and processes and penalties involved where violation of those rules occurs are well described.**

Authorised users of the e-record must be advised as to what potential outcomes might ensue and the possible organisational and legal implications of their actions, should they access personal client information when not authorised to do so.

ix. **Storage and destruction.**

Records are maintained in line with legislative requirements for the duration specified by that legislation. Destruction of records is timetabled and completed by authorised persons - for example, the appointed agency records administrator - and a summarising schedule verifying destruction is maintained. If there is no law requiring retention, records should be destroyed in line with the historic schedules applicable to record disposal.

x. **Clients are informed of the security and access features of the system on which their records will be stored.**

They are provided with a plain language summary statement appropriate to their cultural background that describes how their records will be maintained and secured and under what circumstances others may be granted access to them. In addition, they are requested to sign a standardised acknowledgment as evidence of having received a description of the conditions under which records are established, maintained and disposed of.

## References

Australian Psychological Society. (2007). *Code of Ethics*. Melbourne, Vic: Author. https://psychology.org.au/About-Us/What-we-do/ethics-and-practice-standards/APS-Ethical-Guidelines

The Commonwealth Privacy Act (1998). Commonwealth Parliament of Australia. Canberra. https://www.oaic.gov.au/privacy/the-privacy-act/

Australian Government Office of the Australian Information Commissioner (OAIC, 2013). Australian Privacy Principles. https://www.oaic.gov.au/privacy/australian-privacy-principles/