Te Poari Kaimātai Hinengaro o Aotearoa
NEW ZEALAND PSYCHOLOGISTS BOARD

BEST PRACTICE GUIDELINES

KEEPING RECORDS OF PSYCHOLOGICAL SERVICES

Introduction

The Board's guidelines on record keeping aim to ensure that practitioners are educated about their legal obligations with regard to the retention of health information and records arising from psychological services. All psychologists are regarded as "health practitioners" by virtue of being eligible for registration under the Health Practitioners Competence Assurance (**HPCA**) Act 2003, and therefore all laws which refer to health information, health records, and health practitioners encompass all psychologists regardless of their areas of specialisation.

These guidelines are not intended to encompass professional supervision notes, although there may be reference within the client records to actions taken arising from a discussion in supervision.

Please note that these guidelines offer the general principles underlying good practice. In all aspects of professional activity each situation needs to be considered on its merits and the practitioner should be open to the possible exception.

Purpose of record keeping:

To ensure there are records for each client including the assessment notes and records of any intervention to aid appropriate ongoing intervention, for the client's personal use, for any legal process, and to provide documented evidence in the event of any subsequent complaint or competence concern.
As an aid to memory for the psychologist.
To provide a record of contact for the client's use for insurance reimbursement and other health-related claims.
To enable the transfer of care to another psychologist should that be desirable.
To assist in the comparison of similar cases and assessing treatment approaches.
To comply with relevant legislation.
To support accounting processes and keeping statistical data.

Legal Requirements

The Code of Ethics for Psychologists working in Aotearoa/ New Zealand 2002 ("**the Code**") is aspirational rather than absolute. However it is used as a guide to professional conduct expectations in legal proceedings, including disciplinary hearings. The Code defines the values to be upheld and the practice implications arising on privacy and confidentiality principles. Section 1.6 of the Code states the ethical requirements for psychologists to obtain informed consent, to only collect information for the purpose consent has been granted, and their obligations to protect confidentiality. Section 1.6.10 determines where there may be exceptions to the non-disclosure ruling, including being compelled by law, where non-disclosure may carry a risk of serious harm, or where a person is deemed unable to give consent to disclosure. In any situation of disclosure the psychologist must provide only that information which they judge to be accurate and relevant to the situation.

The management of all personal information is covered in New Zealand by the Privacy Act 1993. Where health and disability information about identifiable individuals is concerned, the Health Information Privacy Code 1994 (**HIPC**) also applies. The HIPC has the force of law and covers all relevant notes arising from services, including contact details and billing information. The Code does not apply to information about employees in the health sector (but that information is subject to the Privacy Act).

The **HIPC Rules** are designed to ensure that people retain a degree of autonomy when others are dealing with health information about them. In the Code the term 'agency' is used in a generic way to include health service provider and/or organisation.

Rule 1: Information should only be collected for a lawful purpose. The information must be necessary for that purpose. Unsolicited information supplied by a third party is not considered to be collection, nor is asking for clarification of that information considered to be collection. However if further information was sought from that third party, then that is collection. Should the person to whom the information pertains request their records at a later time, the unsolicited information component should be blanked out, to protect the confidentiality of the person who offered that opinion.

Rule 2: Wherever practicable, information should be collected directly from the person concerned. If there is variation from this principle, for example where the individual has given authorised permission to collect information from somebody else, then the source of information should be specified.

Rule 3: When collecting information all reasonable steps should be taken to ensure that the individual is aware that the collection is taking place, who is doing the collection, and the intended purpose of the information. You should also ensure that the individual is given the name and address of the agency collecting the information and that they are informed of their right to access it and/or to correct it. It should be made clear whether the supply of information is voluntary or mandatory, and if so, under what law. The potential consequences of not supplying the information should be stated.

Rule 4: Health information must only be collected by means which are lawful, fair, and in ways which do not intrude unduly on the individual's personal affairs.

Rule 5: Anyone holding health information must take steps to ensure that it is guarded against loss or unauthorised access and use. Records must be kept secure and not available to those who are not entitled to see them. Other than an approved health professional, only those who have been given approval (preferably written) by the client may read or copy them.

Caution: A client may have knowingly or inadvertently signed a contract for employment or insurance purposes which gives that third party the right to access their health information. If a psychologist receives a request for information in this circumstance, he or she should contact the client first and seek their opinion and consent after talking through any perceived consequences of such a disclosure. If the client is opposed to such a disclosure, then the psychologist should seek legal advice and may choose to wait until there is a Court order to release the information. If the client gives permission but the psychologist is concerned that there is a potential for harm arising from the disclosure, then the psychologist may negotiate with the client to release only to a legal advocate or their GP or an equivalent professional who is acting to protect that person's interests.

Rule 6: Individuals have the right to access or request any health information about them. Access should be given without charge and any request should be responded to promptly (within 20 working days). The health agency should verify the person's identity before handing over the information. If a request is refused then the reason for the refusal should be given and the individual should be informed of their right to complain to the Privacy Commissioner. Possible reasons for refusing a request may include (but are not limited to) circumstances where disclosure may:

- prejudice the maintenance of the law;
- endanger the safety of an individual;
- breach confidentiality with regard to another individual;
- include evaluative material which may breach a promise of confidentiality of the person who supplied the information;
- prejudice the physical or mental health of an individual;
- be contrary to the individual's interests (where under the age of 16); or
- not be possible because the information is not retrievable.

Rule 7: Individuals have the right to request correction of health information about them if they believe it to be wrong. The agency keeping the information may refuse to correct it if they consider it would not be appropriate to do so, but in that situation a note should be kept recording the assertion of error, which should always accompany that portion of the records which pertain to the request. Reasons for declining a request may include considerations such as clinical opinion held at the time which explains the action taken or because the agency is convinced that the records are accurate. If a correction is made to the records, then others to whom the information had been released should also be informed of the correction.

Rule 8: Health information must not be used without taking reasonable steps to ensure that it is up to date, accurate, complete, relevant and not misleading. The degree of rigour required will depend on the proposed use of the information, the age and reliability of the information and the potential for harm to the individual from inaccurate information.

Caution: In a situation where the client has given permission for the release of psychometric data to another psychologist, then both the original assessor and the psychologist recipient of the test information should take care to ensure that the raw data is not (mis)interpreted out of the context of any limiting factors and constraints which would have been taken into account in the interpretation of the first assessment.

Rule 9: Health information should not be kept longer than it is required for those purposes for which it may be lawfully used.

Rule 10: Health information obtained for one purpose cannot be used for any other purpose, unless the new use is directly related to the original purpose for which permission was granted. Exceptions to this rule include where an individual authorises use for another purpose or where information is required for court proceedings.

Rule 11: Limits on disclosure are applicable such that information should only be disclosed if the individual to whom the information pertains has given authorisation. This continues to apply until 20 years after the individual's death.

While there are numerous grounds set out in the HIPC on which this rule can be set aside, psychologists should uphold the confidentiality obligations as stated in the Code of Ethics and be mindful of the limited circumstances (as set out in 1.6.10 of the Code) which may override that obligation:

- When a person is judged to be incapable of giving consent to disclosure due to diminished capacity.
- With regard to a child or young person the level of their emotional maturity and cognitive skills should determine the weight given to their requests and consent to disclose personal information. Caution: Parents do not have an automatic right to be given information about their child unless this is one of the purposes for which the information was obtained.
- In a situation requiring urgent action it may be impracticable or impossible to seek consent to disclose in time to prevent harm or injury to the individual or others.
- Legal requirements may compel a psychologist to disclose information given by a client or a research participant.
- Where there is a risk of harm to the client or another person caused by non-disclosure the psychologist should exercise their professional judgement to decide whether to breach confidentiality or not. Any such decision must be justifiable and should be made only after consulting with a clinical supervisor or senior colleague.

Other circumstances which may allow disclosure include where the psychologist has reason to believe that:

- The disclosure is consistent with the purpose for which the information was collected.
- The source of the information is a publicly available publication.
- The disclosure is to the individual concerned.
- The disclosure has been authorised by the individual concerned.
- Disclosure is required by a judicial or quasi-judicial process.
- The information is to be used in a form in which the individual concerned cannot be identified. Caution: Written permission should be sought from the client to publish or present their case study even where the details have been made anonymous.
- There is a duty to warn due to a serious and imminent threat to public health or public safety or the life or health of the individual concerned or that of another individual and it is believed that disclosure may prevent or lessen this risk.
- A child or young person is, or may be, at risk of abuse or neglect. In accordance with sections 15 and 16 of the Children, Young Persons and Their Families Act 1989 any informant in this situation is protected from any criminal, civil or disciplinary proceeding arising from that report, provided it was made in good faith.
- The Privacy Commissioner has authorised disclosure pursuant to section 54 of the Privacy Act.

Caution: Psychologists should guard against inadvertent disclosure through the sending of a FAX or email which risks the information being read by an unauthorised recipient.

Section 42 of the HPCA Act authorises a practitioner to release health records for the limited purpose of a competence review or programme, and s 77 of that Act gives a Professional Conduct Committee set up to investigate a complaint the right to request any records for that purpose. Legal privilege and the implications for disclosure are discussed in a later section of these guidelines.

Circumstances which create constraints on confidentiality should normally be discussed at the beginning of information collection and in the process of gaining informed consent. These circumstances may include working within a multi-disciplinary team context, contractual obligations to make information available to a third party, and the sharing of information in supervision.

Rule 12: Unique identifiers can be used where these are assigned by the agency and are necessary for the agency's own purpose. You can only use another agency's unique identifier when your use is part of the purpose for which it was assigned.

The retention of health records is covered by the Health (Retention of Health Information) Regulations 1996 (see below).

In accordance with s 22F of the Health Act 1956, transfer of patient records cannot be refused because of money owing or conflicting commercial interests.

Caution: It should be noted that there are some areas of psychologists' work to which the Privacy Act does not apply. For example, psychologists' assessments carried out on referral from the Family Court under the Care of Children Act 2004 or The Children Young Persons and Their Families Act 1989 are exempt from the Privacy Act. An implication of this is that where a party who is subject to the assessment seeks from the psychologist access to information in the notes that concern them, the psychologist should not comply with that request and should instead refer the person to the Family Court.

Retention of Records

According to the Health (Retention of Health Information) Regulations 1996, all health agencies and practitioners must retain records of health services for a minimum of 10 years, starting from the day after the most recent treatment. If the records are transferred to another provider or organisation, the obligation transfers with the records.

The Regulations do not determine the form in which those records must be retained. If the medium in which they are held is likely to deteriorate to an extent that it places in doubt that the records will be able to be read or retrieved over the time period, it is sufficient to keep an accurate summary or interpretation of the original records.

A psychologist in private practice ordinarily owns the records created in that practice and is therefore also responsible for the safe storage of those records.

The records arising from the practice of an employee or contractor to an organisation would normally be the property and the responsibility of that organisation. This may impose constraints on the control and confidentiality of that information, or cause a client to perceive that confidentiality may be compromised. The psychologist should clarify these issues as much as possible so that they are in a position to adequately advise their client.

Records Held Electronically[1]

The Health Information Security Framework[2] is designed to support health and disability sector organisations and practitioners holding personally identifiable health information to improve and manage the security of that information. Because the HPCA Act defines all registered psychologists as health practitioners, this framework and the standards that it sets, apply to all psychologist practitioners, regardless of their practice settings. The HISF sets standards for the health sector to maintain the information's confidentiality, integrity and availability, defined as:

Confidentiality: Access to health and disability information is limited to the authorised users for approved purposes.
Integrity: Data and information is accurate, consistent, authentic and complete. It has been properly created and has not been tampered with, damaged or subject to accidental or unauthorised changes. Information integrity applies to all information, including paper as well as electronic documents.
Availability: Authorised users ability to access defined information for authorised purposes at the time they need to do so.

The relationship of trust between a client and a practitioner is vital for good health care and therefore a health care practitioner must manage health information with respect. This means that risk management must be done proactively, by considering the probability of a risk event occurring, the impact if such an event occurs, and the appropriate use of available risk mitigation strategies.

[1] Note: This section added August 2017.
[2] Ministry of Health. 2015. HISO 10029:2015 Health Information Security Framework. Wellington: Ministry of Health.

According to the HISF, threats to confidentiality, integrity and availability must be identified, assessed, recorded, prioritised and managed proactively.
Computing "hygiene" requires practitioners to use electronic storage and transfer systems that reduce the risks to data confidentiality, integrity and availability wherever possible.

Storage of Records on the "Cloud"

Cloud computing refers to the transmission, storage and processing of information at a location not owned or managed by the information's owner. It includes products, services, and solutions provided by IT companies and individuals delivered from an off-site server which the user accesses in real time by an internet connection. Examples of cloud services are the storage of records electronically to an off-site server or the accessing of software to use when required through a cloud platform. One example of such software of particular relevance to psychologists is the delivery of psychometric tools delivered via an electronic platform. This topic is covered in more depth in the following section.

The NZ Institute of IT Professionals defines cloud computing as "On demand scalable resources such as networks, servers and applications which are provided as a service, are accessible by the end user and can be rapidly provisioned and released with minimal effort or service provider interaction".[3] They identify five essential characteristics:

- on-demand self-service without requiring interaction with the service provider;
- broad access through a wide range of devices accessing the web;
- resource pooling so that multiple customers are served using a "multi-tenant" model;
- "rapid elasticity" to accommodate demand for expanded capability; and
- a measured service which allows reporting resource use and any agreed charging system.

Cloud services may offer advantages such as: remote access; elimination of the need for purchasing, installing, and maintaining an in-house server; the convenience of the cost of the service being rolled into the one service contract rather than paying for numerous components; and a reliable recovery option in the case of a disaster to the home equipment. However using cloud services also raises issues with regard to security, the control over stored data, and the geographic location of the computer storage facility. Because the use of off-site storage facilities involves handing over information to a third party, this raises risks which must be anticipated and managed proactively to avoid unwanted privacy breaches and loss of control over health information.

With regard to psychological records, and in accordance with the Privacy Act and the Health Information Privacy Code, the owner of the records retains sole responsibility to ensure the on-going security and safety of those records. There is a legal obligation to protect data which has been entrusted to the psychologist by the client, whether arising out of a counselling relationship or within an organisation, from the potential harm from being lost, stolen, accessed without consent, or otherwise misused. Security while the data is in transit and while it is on the server is therefore crucial. Encrypting data combined with using password protection are options to assist in reducing risk. Some providers automatically encrypt data when it is being transferred between the organisation and the off-site server.

Psychological records need to be readily accessible and in some circumstances, may need to be changed if, for example, a client requests a correction. Data that has been converted to a 'pdf' form to enable password protection may restrict the ways that the correction is made.

- If considering using a cloud storage system, relevant considerations are:
- the reliability and security record of the provider,
- the terms of the contract with regard to the control of the data should the provider cease trading, and
- whether the customer is informed in the event of a breach of security or in the event the information is passed to somebody else.
- Does anybody have access to the data and will it be used in any form, such as the collecting of statistics?
- How would a search warrant be responded to?
- Access to the data should be unimpeded if the psychologist (customer) chooses to withdraw their data to switch to another provider, but there would need to be an assurance that the data previously stored has been permanently deleted, including from any back-up storage system.

New Zealand cloud service providers may be signatories to the Institute of IT Professionals (ITP) Cloud Code. This Code requires providers to declare their professional practice against a checklist of ethical and professional standards. Although helpful to have this transparent information, this is a self-regulatory system within that industry and there may be no independent audits of these standards or over-arching authority to receive a complaint, should an unsatisfactory event occur.

[3] Based on the US National Institute of Science and Technology definition, broadly accepted as the worldwide authority. See http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

The use of an off-site electronic storage facility is not necessarily more risky than other storage options but should be approached with an awareness of the potential risks and careful consideration of the ways to manage those risks.

The Use of Off-Shore Storage Facilities

The geographical location of the storage facility is another relevant consideration as the off-site server will be subject to the privacy laws of the host country. For example, if the storage facility is located in USA, the US Government can access information without a search warrant, but the psychologist owner of the data would be in breach of the NZ Privacy Act. Some New Zealand laws require data to be stored in New Zealand.[4]

The Ministry of Health approach to the use of offshore cloud storage is evolving. Initially there was a blanket ban (unless a specific exemption was obtained) on the use of offshore cloud storage facilities for personal identifiable health information. This applied to all off-shore cloud storage facilities, whether it was in regard to the storage of health data or the use of software that "inadvertently" gathers health data (as is the case for psychometrics delivered electronically). Until April 2017, the Ministry required health providers and public cloud services to undertake a thorough risk assessment to the Ministry before the Ministry would grant an exemption for that specific service. As of 12 April 2017, this previous policy was discontinued and the Ministry devolved the risk assessment back to the health providers and the senior managers within their health organisations. However the requirement to undertake a formal risk assessment for each cloud storage facility service remains in place. The change in policy means that the decision to proceed resides with the health provider organisation. However, each service must be approved by the health provider agencies' Chief Executive or a delegate from the upper levels of management. In the case of DHBs, a copy of the completed risk assessment is to be forwarded to the Government Chief Information Officer (GCIO). Other health provider organisations are encouraged to also inform the GCIO of their completed formal risk assessments and the approved services.

Cloud Service Risk Assessment

The Department of Internal Affairs and the GCIO have issued a formal risk assessment tool that must be undertaken before the cloud service is adopted. This tool consists of a set of questions to be worked through conjointly between the health service provider, e.g. psychologist or health organisation, and the vendor of the service, e.g. the cloud service provider (which may be a psychometric test distributor). The questions cover the following domains of information:

1. The sensitivity of the information
   Including but not limited to such questions as:
   - Who does the information belong to?
   - What are the laws applicable? (e.g. the Health Information Privacy Code)
   - How serious would it be if there was a breach of this information?

2. The sovereignty of the data
   Including but not limited to:
   - Where is the head office of the service provider?
   - What countries are the cloud services delivered from?
   - What is the legal jurisdiction that the data is stored under?
   - Do you as the customer have the right to choose where it is stored?
   - Are there any third parties involved that introduce additional risks?
   - How do the laws of the country impact on the security of the information?

3. Privacy
   Including but not limited to:
   - What are the privacy risks?
   - If there is a disclosure to an unauthorised third party, would the service provider notify you as the customer?

[4] The following NZ Acts require data to be located in New Zealand:
- Companies Act 1993
- Electronic Transactions Act 2002
- Financial Reporting Act 1993
- Financial Transactions Reporting Act 1996
- Goods and Services Tax Act 1985
- Income Tax Act 2007
- Public Audit Act 2001
- Public Finance Act 1989
- Reserve Bank Act 1989
- Securities Act 1978
- Tax Administration Act 1994

- Who would you complain to if you became unhappy with the service?

4. Governance
   Including but not limited to:
   - Are there standard terms for a contract or does the service provider allow you to negotiate contracts with their customers?
   - Do the terms of the service define how the confidentiality, integrity and availability of information entrusted to them, and the privacy of the personally identifiable information, will be managed?
   - Will the data be used for any other purpose?
   - Does the service provider allow independent audits?
   - Does the service provider undertake regular checks against internationally recognised information security standards by an independent third party?
   - Can the health service provider (customer) do reference checks and review recent audits?

5. Confidentiality
   Including but not limited to:
   - Does the health service provider have an identity management strategy?
   - Have the requirements for encryption of the information placed on the cloud service been determined?
   - Is there an effective patch and vulnerability management process in place?
   - Are there appropriate checks on employees to address potential insider-threats?
   - If there is any incidence, would that be reported to affected customers?

6. Data integrity
   Including but not limited to:
   - Does the service provide data back-up or archiving services to protect against data loss or corruption?
   - Does the service provider check that data can be restored?
   - Would the health service provider need to provide their own data back-up service?

7. Availability
   Including but not limited:
   - What is the expected and minimum availability performance percentage over a clearly defined period?
   - Does the cloud storage provider have continuity and disaster recovery plans?

8. Incidence response management
   Including but not limited to:
   - Do they have a formal incident response and management process that clearly defines how they detect and respond to information security incidents?
   - Would they notify customers if such an incident occurred?

There are advisory services available at the Ministry of Health to assist a health service provider work through this risk assessment worksheet, and to discuss the implications that may become evident in the process (email: cloudcomputing@moh.govt.nz).

Where the risk assessment identifies areas of significant concern, the health provider may wish to discuss these matters with the Ministry before making a decision.

Electronically Administered Psychometrics

Psychometric tools administered on an electronic platform means that the records of that assessment are recorded on that test distributor's storage facility. This applies regardless of whether the psychometric test data is printed off and "deleted", or whether the identity of the person is disguised by use of an alternative identifier system. Most psychometric test developers and distributors are located off-shore. Therefore using an electronically administered psychometric tool invariably triggers that threshold of engaging an off-shore cloud storage facility.

The Health Information Security Framework applies to all health practitioners. As psychologists are defined as health practitioners by the HPCA Act, the edicts that arise as a consequence of this set of standards apply to all cloud services to store health data used by psychologists, regardless of their practice setting. Therefore prior to the electronically administered psychometric tool being used, the health practitioner must check that a formal risk assessment has been undertaken.

In practice, it means that the psychometric test distributor or vendor needs to be assessed. Once clearance is gained, that would apply to all of the tests in that vendor's portfolio (presuming the same platform and storage facility applies to all of the tests promoted by that distributor). This emphasises that it is not the test that is being assessed but rather the facility that the cloud service agency is to provide and through which a number of tests may be provided. At the time of the preparation of these guidelines it is anticipated that a list of cleared psychometric distributors may be held by key agencies, such as the NZ Psychological Society, the NZ College of Clinical Psychologists, the network of DHB Leaders for Psychology and NZCER.

What is Included in Records?

The records should include a complete record of the contact with the client. Records should be full enough to accurately track the initial assessment, formulation, planning and the progress of intervention. Risk assessment issues should be noted as well as any "out of the ordinary" communications. There should be sufficient detail to show professional judgement and the basis of decision making.

The term "records" refers to both written and electronically stored information.

Records of psychometric testing should include the raw scores and any recording forms, as well as the summary and interpretations.

Records should be legible, accurate, and kept up to date. All entries should be dated and initialled. Any changes should also be initialled and dated, and done in a manner that allows the original notes to be visible. Any electronic additions should be done in a manner that records the date of entry and the author of that addition.

The record should contain sufficient detail for another psychologist to follow. Every face-to-face consultation or other significant contact (including office and online contact) between the client and psychologist should be recorded with the identity of the recorder, the date on which contact occurred, and the date on which the notes were recorded (if different) all evident.

Text messages and phone calls should be recorded as file notes if considered of sufficient significance to record.

Once notes are recorded they should not be deleted unless as part of an archives clean-up after the mandated retention period has passed. Any destruction or wiping should be done in a manner to preserve confidentiality.

The records should not contain any terms that could be perceived as derogatory or judgemental. If abbreviations are used, then a glossary may be necessary to preserve clarity of meaning.

Confidentiality of Records

The general principles that apply to the confidentiality of the records include that records should be preserved by being kept in a secure location and that psychologists should not disclose to any third party the fact that there has been professional contact nor any content of the professional interaction without the permission of the client.

This confidentiality extends to family relationships. Psychologists should not disclose the psychological condition of one member of a family to another family member without the consent of the first person. Exceptions to this may apply, such as where a child or young person is being assessed or where there is deemed to be risk to the safety of the person concerned or a third party.

The practitioner must ensure information is protected against:

- Loss;
- Access, use, modification, or disclosure except with the authority of the client; and
- Other misuse.

Where a document containing health information is to be disposed of, it should be done in a manner that preserves the privacy of the individual, such as shredding or careful incineration.

A psychologist who works as an employee of an agency or service should give any client of that agency or service an explanation of the constraints to confidentiality that may apply (for example, the implications of working as part of a multidisciplinary team) and who may have access to their records.

Caution: An exception to these principles is where a psychologist is contracted by a third party to assess and report on a person or persons (such as a family). In this situation the information and the report arising is the property of the third party contractor, and must not be released to the person concerned without that contractor's permission. Furthermore, in third party referrals there may be a number of people in addition to the contractor that have access to the client's

information relating to the purpose of the referral. In such circumstances the psychologist must explain the purpose for which the information is being gathered, the real and potential consequences for confidentiality, and the particular conditions attached to the storage of and access to records.

Release of Records or Information

The general principle that applies to records is that records should only be released with the permission of the client who is the subject of the records. Ideally this should be in writing. However any decisions pertaining to the management and release of health information must be filtered by the HIPC Code principles.

If the client who is the subject of the records requests in writing that the records should be released to another professional, then that should be acted upon promptly, or at least a summary provided. However the psychologist should keep a copy of the notes in case of a subsequent complaint or competence concern.

If the records are released to another professional (with the client's permission) then an assurance should be sought from the recipient that the records will only be used for the purpose for which permission was granted.

If transfer occurs to a professional recipient, the legal obligation to retain records for ten years transfers with the records.

Extra care should be taken to gain informed consent where the release of information pertains to more than one person, such as in a consultation with a couple. A request for release of the records of consultation should be signed by all identifiable parties. Where one party objects to the other party receiving a copy of their joint records, a compromise may need to be reached such as blanking out reference to the party that withholds permission and any information provided by that party outside of joint discussion.

An individual may request access to any information pertaining to them.

Psychometric assessments or other information that requires professional training for interpretation or analysis should not be released to persons who lack that training. Any release of interpreted or analysed information should include the constraints or limits to the applicability and meaningfulness of that data.

Records pertaining to a client who has since deceased should not be released to a next of kin due to the sensitivity of some records.

Confidentiality Within Legal Processes

In accordance with section 59 of the Evidence Act 2006, clients who consult a clinical psychologist for the purpose of assessment or treatment of drug dependency issues or "any other condition or behaviour that manifests itself in criminal conduct" have legal privilege. This means that the treating clinician is not required to disclose information in a court or quasi-judicial proceeding, unless assessment or therapy is mandated by the court (e.g., an assessment to determine fitness to plead or their current psychological state).

Under section 69 of the Evidence Act 2006, any confidential information or information that would reveal a confidential source of information is deemed privileged unless a Judge orders otherwise, after weighing up the public good arising from disclosure versus the potential harm from breaching confidentiality. In making a direction to disclose the Judge may consider the likely extent of harm from disclosure; the nature of the communication or information and its importance to court proceedings; the nature of the proceedings; the availability of other means of obtaining the information; to what extent the public disclosure can be controlled or restricted if the evidence is given; the sensitivity of that information (including the length of time that has elapsed and the extent to which the information has already been disclosed); and society's interest in protecting the privacy of victims of offences.

Privilege gives the right to refuse to answer questions in any judicial or quasi-judicial enquiry. Privilege belongs to the client rather than the psychologist. The client also has the right to waive their right to legal privilege. If clients waive their rights with regard to their private information, they should be advised that once the information is in the legal arena, they may have little control of how that information is used.

If a psychologist receives a subpoena with regard to a particular client, the psychologist must contact the client to determine their wishes. If the client wishes their information to be forwarded to the legal process, then they should be fully informed about the likely extent of the disclosure. A signed consent form should be obtained from the client before the psychologist releases any information.

A judge may issue a court order requiring a psychologist to provide requested information where he or she considers the information is essential for the court proceedings and where it is considered that legal privilege does not apply. In that circumstance the psychologist may make submission to the Judge requesting the matter is reconsidered if they believe that disclosing information in that situation violates the client's legal privilege. The psychologist would need to make a case that disclosing information may do more harm than good. Otherwise failure to respond to a court order puts the psychologist in contempt of the court.

Psychologists should consult a lawyer if in doubt about the applicability of legal privilege.

Caution: A psychologist may receive a request to release client records or information from records to the Ministry of Social Development (MSD) under section 11 of the Social Security Act 1964 where that Ministry is investigating a client for alleged benefit fraud. While this legislation gives the MSD wide powers, it is not absolute and is moderated by the Code of Conduct associated with this legislation. The Code specifically excludes demands on clinical psychologists to provide information concerning confidential communication for the purpose of diagnosis or treatment and the Appendix to the Code notes that this exemption may also extend to the special relationships of confidence between any psychologist and patient. Any legally privileged information is also exempt. If a psychologist receives such a request, they should seek a legal opinion, discuss the request with the person or persons it pertains to, and consider declining the request unless ordered to do so by a court. The MSD or other organisation with an interest in the information can ask the court to rule on a request, which would then prompt a judge to determine whether or not information should be disclosed, having weighed up the public interests served by disclosure versus the public interest in preserving the confidential relationship and other benefits that may arise from non-disclosure.

In any situation where there is a request to disclose for a legal or quasi-legal purpose, the psychologist is advised to seek independent legal advice and if necessary refuse to disclose. The requesting party can then apply for a court ruling on the matter.

Planning Ahead for Possible Interruptions to Practice

The practitioner should have contingency plans in place to cover an interruption in practice caused by sickness, retirement or death.

Psychologists who work in an employment setting can assume the responsibility for retention of records falls on the organisation concerned. Psychologists who work privately must make provision prior to retirement to ensure the safe storage of records.

All psychologists are urged to make clear provision in their will or in their retirement plans to ensure the safe and secure storage of their clinical records.

Please note: The Board is considering making it mandatory for practitioners to declare when renewing their APC that such arrangements are in place.

This is of particular importance in the case of a sole practitioner in private practice. This may involve retaining control of the records until they can be safely destroyed; transfer to another practitioner; obtaining written agreement from a group practice that the records will be retained and safely stored; or in the event of the death of the practitioner, transfer to a person who is the Executor or who has Power of Attorney.

The Sudden Death of a Practitioner

The sudden death of a practitioner can cause immediate issues with regard to the ongoing care of patient records.

If the psychologist has been an employee or attached to a larger practice, the client is likely to use that organisation as a focus to seek ongoing help. An organisation or group practice is likely to assume responsibility for the safe storage and transfer of records to another provider.

Relatives of the deceased psychologist may seek advice to maintain responsible care for the records. The legacy of electronic storage devices such as laptops and computers poses the issue of how these devices can be safely cleansed of client records without breaking confidentiality. The involvement and mediation of the clinical supervisor or a practice associate may assist.

The executor of the will of a deceased private practitioner psychologist (such as a legal representative or a family member) or delegated professional representative (such as a clinical supervisor) should contact clients and seek guidance on what they would like done with their records. In the event that previous clients are unknown or not

traced, details of how to contact the guardian of the records should be posted in advertisements or at the physical location of the previous practice.

In the event of the death of a practitioner who has been a sole practitioner and who has not made provision in their will for the storage of their records, possible solutions to the ongoing care of the records include transfer to a known colleague of the psychologist and/or public notification of the death of the psychologist to inform clients so that they may choose to contact the Executor of the will to uplift their file. Any records not uplifted within a certain time frame could be destroyed. Clause 8(1) of the Health Retention of Records regulations states the obligation to keep records for ten years does not apply to a practitioner's next of kin or Executor after his/her death.

Is It Legal to Hold Records for Longer Than 10 Years?

According to Rule 9 of the Health Information Privacy Code, a health agency holding health information must not keep information longer than is required for the purpose for which the information may be lawfully used. This does not prohibit the health agency retaining information where it is desirable to do so for purposes of providing health services. Mental health services, obstetrics, and services to children are often included in lists of services where it is optimal to keep records for longer than the minimum requisite years, all of which may include psychological services. Where there is good reason for extending the period of retention, records should be retained for longer periods.

References

Code of Ethics for Psychologists Working in Aotearoa/New Zealand, 2002. Prepared and adopted by the NZ Psychologists Board, the NZ Psychological Society, and the NZ College of Clinical Psychologists.

Health Information Privacy Code 1994, Revised Edition 2008. See http://privacy.org.nz/health-information-privacy-code/

Infoage newsletter (August, 2013) www.infoage.co.nz

Institute of IT Professionals (2013) New Zealand Cloud Code: Cloud computing code of practice version 2.0. www.iitp.org.nz

Jefferson, S. (In press). Privacy and privilege. In F. Seymour, S. Blackwell, & J. Thorburn (Eds). The handbook of psychology and law. Wellington: New Zealand Psychological Society.

Medical Council of New Zealand (2005) Maintenance and retention of patient records. Accessed online at: www.mcnz.org.nz

Mell, P. and Grance, T. (2011) The NIST definition of cloud computing: Recommendations of the National Institute of standards and technology. NIST, US Department of Commerce Special Publication 800-145.

Ministry of Health (2015) HISO 10029 Health Information Security Framework. Wellington: Ministry of Health.

Privacy Commissioner Te Mana Maapono Matatapu (2013) Cloud computing: A guide to making the right choices. Published by the Office of the Privacy Commissioner, Wellington.

Stevens, Robert. The Medical Record, in Medical Practice in NZ. Coles (2011 edition) Medical Practice in New Zealand, published by Medical Council of New Zealand online at: www.mcnz.org.nz

Taylor, Joanne and Dickson, Jan (2007) Confidentiality and Privacy. In "Professional Practice of Psychology in Aotearoa New Zealand" published by New Zealand Psychological Society, Wellington.

Guidelines from a range of North American and Australian regulatory and professional associations were read but were not directly used to inform the guidelines development.