

1. Client Files

Representatives must keep proper records

Adequate records must be kept of all instances where advice, either verbal or written, is given to a client or potential client. Not only is this common sense, it can be valuable in defending any liability that may arise in the future.

Verbal Advice

Where verbal advice is given this is to be confirmed with a Record of Advice and detailed file notes must be kept regarding the circumstances, advice given and commission disclosure. The note should always include the date, time and initials of the person giving the advice.

Written Advice

Records relating to the making of written advice must also be kept.

In addition to a copy of the information collected from the client and a copy of any recommendations made, these records should also include a copy of the research notes relevant to any product recommended.

Naturally, the client's records should also be updated whenever there is a review of the client's portfolio, or any time when advice, either verbal or written is provided or client queries are answered.

Contents

Client files should be a complete record of all information you require to:

- Review your client's details:
- Prepare a comprehensive financial plan:
- Review your client's portfolio:
- Maintain a comprehensive record of what you have recommended:
- Know why you have made your recommendations:
- Know how you have responded to your client's requests and needs.

Each client file should be maintained in such a way that it can be clearly followed by you and anyone else reviewing the file.

Period for Which Records are to be Kept

All records should be kept for at least **7 years** after the preparation of the last review for the client.

Maintaining Client Files

It is essential that you maintain neat, chronological and straightforward client files.

When examining an adviser's conduct ASIC will test the practices adopted by the adviser against their standards. A properly maintained client file will prove that you have followed a disciplined process in preparing advice for your client.

In addition to the legal requirements, well maintained client files ensure your financial plans will be easily accessible and of the highest possible quality. Many financial planning issues are complex and need to be given a great deal of attention. All issues need to be addressed logically and recorded in detail so when preparing a financial plan they can be referred to quickly and easily.

Clear and precise notes are essential to establish and remember issues for later reference. Working papers should be clearly identifiable as working papers and final advice must be clearly identifiable as final advice.

When you need to review your client's affairs, a well organised file will ensure you have all the necessary details to service your client properly and address all the relevant issues.

Consider also the benefit of passing on a well organised and properly maintained file to another person on your retirement or sale of your business. Alternatively, consider yourself taking over another financial planner's clients. A file which allows you to easily review a client's complete history is invaluable.

Retaining Records Electronically

Representatives are encouraged to establish procedures to maintain files electronically. Modern client management systems provide excellent facilities for accurate and efficient management of client data.

The Commonwealth Electronic Transaction Act 1999 allows you to provide information in writing, provide a signature, produce a document, record information and retain a document electronically.

In addition, Corporations Act 2001 and ASICS Regulatory Guide 221 permit the digital delivery of financial services disclosures. Disclosures may be delivered using digital methods (e.g. a digital message with a hyperlink to the disclosure):

- If the client has agreed (orally or in writing)
- if the client has not agreed, the provider can rely on ASIC Corporations (Facilitating Electronic Delivery of Financial Services Disclosure) Instrument 2015/647, which involves making the disclosure available digitally and notifying the client that the disclosure is available (the provider must first give the client the opportunity to opt out of this method); or
- If it is specifically permitted by the Corporations Act (e.g. for annual superannuation information and confirmations of transactions).

The representative must retain a copy of all versions of the disclosure and use technology, where possible, to maintain records of when each version was available. When the disclosure is provided through a hyperlink or a reference to a website address or digital facility, the representative should make it clear to clients that they can request a copy of the disclosure at no cost to the client during this period.

In order to establish an electronic record system advisers are required to implement appropriate data management practices including:

- Regular back ups and off site storage of data.
- Quality control of data input to ensure that records are complete.
- Restrict access to ensure data privacy and integrity.
- Data can be retrieved readily.

- Observing a quality assurance program evidenced by regular evaluations of the electronic recordkeeping system including periodic checks of electronically maintained or retained records.
- Retaining paper copies of records that cannot be clearly, accurately or completely transferred to an electronic recordkeeping system
- Manage and retain electronic records in accessible form for their legal minimum retention period.
- Dispose of them appropriately after the legal retention period.

In maintaining electronic systems representatives must establish clear and effective protocols to ensure the integrity of the system. In particular representatives will need to address:

- There are reasonable controls to ensure the integrity, accuracy, authenticity and reliability of the records kept in electronic form.
- The electronic records are maintained in reasonable order, in a safe and accessible place, and in a manner that they may be readily inspected or examined.
- The electronic records are readily convertible into legible and readable paper copies as may be needed to satisfy reporting and disclosure requirements.
- The electronic recordkeeping system is not subject, in whole or in part, to any agreement or restriction that would directly or indirectly compromise or limit a person's ability to comply with any reporting and disclosure requirement.
- Well understood file structures to ensure records are stored consistently across the business
- File naming protocols, normally including dates, to ensure records can be properly identified
- Protocols to ensure that documents provided to clients can be clearly differentiated from internal file notes and or draft documents
- Offices processes to ensure all documents and file notes are retained on the system.

To ensure the integrity of electronic documents all printed documents provided to clients should be scanned in a permanent format (eg PDF). This will preserve the integrity of the documents so that they cannot be altered (either deliberately or unintentionally eg. through auto-date updates or when accessing the document at some future time). It will also enable demonstration of disclosure of capacity through the use of letterheads and signatures.

https://www.ctg.albany.edu/publications/reports/proper_systems/proper_systems.pdf

Separation of Capacity

Where the adviser has more than one relationship with the client, eg. as the client's accountant, separate files should be maintained.

All items pertaining to the client and the adviser's actions as an authorised representative should be kept in the financial planning file. Documents relating to other functions should be filed separately.

Where clients are involved in a number of structures or entities, eg. personal investments and self managed superannuation funds, consideration should be given to maintaining separate files and communication for each entity. In this case files should be cross referenced.

Privacy Considerations

IFP Privacy Policy

IFP has a privacy policy. Refer Doc D1.

In the course of our business representatives are required to gather and store potentially sensitive and confidential information about clients. Representatives must therefore address the privacy of this information.

It is a requirement as the Licence is the “legal” owner of the client that representatives adopt the IFP Privacy Policy. To do so:

- Each practice should conduct an information audit to ensure that they are meeting the standards set out in our privacy policy.
- Advisers should also note that client referrals where information is passed on falls under the privacy requirements.

Representatives may also operate their own privacy policy to suit the needs of their business. This may be the case where representatives are involved in other businesses that have their own privacy policy.

The privacy policy is to be available to clients on request and available to clients on the www.iplan.com.au website.

Anti-Money Laundering/Counter Terrorism Financing Act

The obligations imposed under the *Anti-Money Laundering and Counter Terrorism Financing Act 2006* (AML/CTF Act) are no longer simply linked to suspicious cash transactions and cash transactions over \$10,000. Instead an activities based definition is introduced under which anyone who provides a “designated service” is subject to customer due diligence and enhanced reporting requirements.

A designated service is defined as the provision of a financial service in the capacity of holder of an Australian Financial Services licence.

The most common designated service covered under AML/CTF and *Foreign Account Tax Compliance Act* (FACTA) include:

- Arranging for the client to obtain or be issued with new or additional interests/units in a managed investment scheme
- Arranging for the client to open or make a deposit in a cash management trust
- Arranging for the client to buy/sell shares/options in a listed company or trust
- Arranging for the client to pay a premium or be issued with an investment life insurance policy
- Arranging for the client to obtain or be issued with an annuity
- Arranging for the client to obtain or be issued with a pension
- Arranging for the client to obtain an interest in or have the ability to transact through wrap/platforms/IDPS
- Arranging for the client to cash out all or part of a superannuation interest.

Entities who provide “designated services” under the Act are defined as “reporting entities” (RE). The AFSL holder is the RE and the obligations are imposed on the licensee. Although in most cases the obligations are discharged by the representative. The licensee is liable if the obligation imposed on it as RE are not adhered to.

Collection and Verification of Customer Identification Information

Authorised representatives may collect and verify Customer Identification Information.

Under the AML/CTF Act reporting entities offering one or more designated services must identify and verify their clients.

The AML/CTF Act requires reporting entities to check a client's identity before providing a designated service to the client. Only in special circumstances specified in the AML/CTF Rules can a reporting entity delay checking a client's identity until after a designated service has been provided.

The AML/CTF Rules require verification of client information from reliable and independent documentation.

Reporting entities may adopt 'safe harbour' procedures to verify client's information. The safe harbour procedures outline a simplified process for verifying individual clients using documentation where the reporting entity has assessed the level of ML/TF risk as medium or lower:

- Reporting entities adopting the documentation based safe harbour procedures must use a certified copy of a primary photographic, non-photographic or secondary document to verify customer information.

An applicable customer identification procedure should be carried out by IFP representative in accordance with the instruction provided in the ID form applicable to the type of client and for any applicable related parties (such as Corporate Trustees of Unregulated Trust or Beneficial Owners of client). Refer to the website for the ID form.

- Individuals & Sole Traders
- Australian Companies
- Foreign Companies
- Australian Regulated Trusts
- Unregulated Australian Trust & Foreign Trusts
- Partnerships & Partners
- Associations
- Registered co-operatives
- Government bodies
- Verifying Officer

For higher risk clients, representatives should refer to the Licensee.

Irrespective of the actual customer identification procedure conducted, the representative conducting the procedure must be reasonably satisfied that the client is the individual/entity he or she claims to be.

If, after a representative conducts a customer identification procedure, they are not reasonably satisfied that the client is the individual/entity he or she claims to be, and the representative is unable to conduct a further customer identification procedure to address this doubt, then they should not arrange for the provision of the financial service or product.

In addition, where a representative is not reasonably satisfied that the client is the individual/entity he or she claims to be, the representative is required to notify IFP as soon as possible (preferably within 24 hours).

FATCA

Whilst IFP is not defined as a Financial Institution and not required to collect FATCA information on this basis, generally there may be collection information on behalf of Investment Institutions who are required to collect such information, so it makes sense for representatives to collect such information at the point of identification to discharge their obligations to the various Investment Institutions.

Collection of Tax File Numbers

Authorised representatives may collect and store a client's Tax File Number.

When seeking a TFN, the representative needs to ensure that the client understands the legal basis for the collection, and that declining to provide a TFN is not an offence. In addition, the client needs to be informed of the consequences of not providing a TFN.

The client's signed consent should be obtained and retained on the client's file. Refer to Doc. D2 for a "TFN Collection Form" authorising representatives to retain and quote their TFN in certain circumstances.

Accountants are also recognised as lawful TFN recipients and may retain clients' TFN information and use it as necessary to conduct the client's affairs. It is important to ensure that this information is maintained in a separate file to that information obtained and retained whilst acting in the capacity of an authorised representative.

Storage, Security and Disposal requirements

Representatives need to ensure that TFN information is protected, and that safeguards are in place to prevent loss and unauthorised access, use, modification, disclosure and misuse.

Access to records containing TFN information needs to be restricted to those people who have relevant responsibilities pursuant to taxation, assistance agency or superannuation law. When a TFN is no longer required by law or administratively necessary, disposal of TFN information needs to be by a secure means.