Compliance Checklist

This checklist comprises a set of compliance regimes that all life insurance advisors should have within their practice in order to minimize client complaints and maximize the ability to pass compliance audits administered by provincial insurance regulators and law enforcement entities such as the Financial Transactions and Reports Analysis Centre of Canada ("FINTRAC") and the Office of the Privacy Commissioner of Canada ("OPCC").

✓ Anti-Money Laundering and Anti-Terrorist Financing Compliance Regime ("AML / ATF")

Taken from FINTRAC Guideline 4, Section 2.2, *"If you are a life insurance broker or an independent agent (not an employee of a carrier or brokerage), you are responsible for your own AML compliance regime."* Therefore, independent brokers and independent advisors are required by law to have a documented AML Compliance Regime in order to be in compliance with the Proceeds of Crime (Money Laundering) and Terrorist Financing Act of Canada ("PCMLTFA"). It's the law! Your AML / ATF Compliance Regime must consist of five key documented elements:

1. The appointment of an AML / ATF compliance officer
2. The development and application of written compliance policies and procedures
3. A review of the effectiveness of policies and procedures, training program and risk assessment
4. The assessment of risks for money laundering and terrorist financing and measures to mitigate high risks
5. Implementation and documentation of an ongoing AML training program for you and your staff

✓ Privacy Compliance Regime

According to the Personal Information Protection and Electronic Documents Act of Canada ("PIPEDA"), as a private sector business involved in the collection, use, retention and sharing of personal information for commercial purposes, independent advisors are required by law to have a documented Privacy Compliance Regime which describes policies and procedures used to safely store, transmit and protect personal information ("PI"). Life insurance advisors collect, retain and share a wealth of personal client information such as client identity information, health information and financial information. If you are a skilled fact finder, you even collect information about a client's hopes and dreams. As taken from the amended Digital Privacy Act of 2015 ("DPA"), *"a privacy breach occurs when there is an unauthorized access to, or collection, use or disclosure of personal information including information that is lost, stolen, disclosed in error or as a result of an operational breakdown, that results from a breach of security safeguards or failure to establish those safeguards."* Privacy breaches can occur in a number of ways including but not limited to theft of your computer hardware, online data theft, system hacking or fraud. Even ransom software, where a criminal accesses and freezes your computer system and demands payment to "release" your data back to you, can progress to "doxing" where the criminal releases your personal client data to the open internet. This can result in extortion, coercion, harassment and online shaming for you and/or your clients. You must report privacy breaches to the OPCC and notify affected individuals when *"there is a risk of significant harm to the individual."* If a reportable breach occurs, the OPCC will assess your documented privacy compliance regime. Deficiencies can result in significant fines and penalties, above reparations you may need to make to your client.

Note in British Columbia, we can refer to BC's Personal Information Protection Act ("PIPA") here http://www2.gov.bc.ca/gov/content/employment-business/business/managing-a-business/protect-personal-information

A privacy compliance regime consists of the same structural elements of an AML / ATF compliance regime:

1. The appointment of a Privacy Officer
2. The development and application of written privacy policies and procedures
3. A documented review of the effectiveness of policies and procedures, training program and risk assessment
4. The assessment and documentation of risks of privacy breach in the practice
5. Implementation and documentation of an ongoing privacy training program

General Compliance Regime

A general compliance regime represents your overall compliance policies and procedures and reads like a "best practices" or "code of conduct" compliance manual for your practice. Your general compliance manual should consist of topics such as:

- Conflict of interest management and disclosure
- Maintaining a client complaint log and reporting client complaints to the MGA and applicable insurance carrier
- Complying with Canadian Anti-Spam Legislation (CASL) and CRTC's Unsolicited Telecommunications Rules, including National Do Not Call List "N-DNCL."
- Maintaining active licences, CE credits and required errors and omissions insurance
- Proper holding out and disclosure to clients
- Obeying prohibitions of discretionary authority, fronting, rebating, churning, viatical agreements, twisting and tied selling
- Placing the client's interests first
- Making needs based and risk assessment based recommendations to clients
- Making clear and accurate representations to clients
- Proactively reporting all regulator disciplinary actions and investigations to the MGA and carriers with which you are contracted

The Compliant Client File

Presently, compliance in the life insurance industry is principles-based and driven by code of conduct. Each carrier you sign a producer agreement with has a code of conduct by which you contractually agree to abide by. The central premise is fair treatment of clients and placing client's interests first. Client-facing documents such as - advisor disclosure, fact finding questionnaires, insurance needs analysis, know your client ("KYC") and investment risk tolerance questionnaires - are tools that, when used with and signed by a client, demonstrate the advisor engaged in a communicative process with the client to arrive at a needs based, risk appropriate recommendation which the client clearly understood. The graphic below is a good reminder of the documented process that should be evident in your client files. These are the documents that a provincial insurance regulator will want to see in your client files if you are selected for compliance audit. They are also the documents that a carrier compliance officer, E&O claims adjudicator or defense lawyer will want to see when reviewing a client complaint. These documents represent strong evidence that you took time to assess your client and that you clearly explained the products and strategies that met their needs, wants, budget and risk tolerance, and that you explained the risks of these products and strategies.

Specific documents that should be in your paper and/or electronic client files:

- Advisor Disclosure form, signed & dated by the client
- Privacy Statement, signed & dated by the client
- Needs analysis/financial plan, signed & dated by the client
- Detailed notes and saved emails outlining your discussions and meetings with clients
- Follow up letters that you sent to clients inviting them to call you if they have any questions about a recent purchase
- Illustrations and strategies shown to the client, even strategies and products the client declined to purchase from you
- Communications with the client (e-mails, letters, faxes, texts, etc.)
- Policy Delivery Receipts, signed & dated by the client
- Evidence of the client's instructions to you (including time and date) for transactions where a client signature was not required
- Clear evidence that you explained annual fees to your client for segregated fund purchases
- Clear evidence that exiting fees for segregated funds purchased on a deferred sales charge basis (DSC) were clearly explained and acknowledged (in writing) by the client!