Privacy Matters

Brokers clearly understand the need to respect customer privacy. With the passage of the *Digital Privacy Act*, that responsibility continues, but a few new ones have been added. Brokers should have a plan, choose partners wisely and identify potential liabilities.

Brenda Rose
Vice President and Partner, FCA Insurance Brokers and Technology Champion, Insurance Brokers Association of Canada

Life has become more complicated in the insurance business.

Insurance coverage decisions, and corresponding rates, have always been derived from the information available about a given individual or risk.

With the analytics tools now available, however, decisions can be tied even more closely to individual characteristics, rather than to average experience. Very specific data is the prerequisite for such analytics science to be effective, with the result that in order to serve their customers' needs, brokers must collect and share ever-greater amounts of detailed information about diverse aspects of their lives.

Various pieces of Canadian legislation determine how individuals' information may be used. The *Privacy Act* of 1983 set out basic parameters for the federal government's handling of personal data. Then, in 2000, the *Personal Information Protection and Electronics Act* (PIPEDA) enshrined more detailed responsibilities for all organizations.

PIPEDA articulates the following 10 guiding principles, which are intended to protect consumers when they entrust their personal information to others:

- accountability;
- identifying purposes;
- consent;
- limiting collection;
- limiting use, disclosure and retention;
- accuracy;
- safeguarding information;
- policy accessibility;
- information accessibility; and
- addressing complaints.

BROKER VALUE PROPOSITION

The concepts embedded in PIPEDA have always been intrinsic to brokers' basic value proposition; a fundamental respect for an individual's situation and protection of that privacy are prerequisites to effectively serving insurance consumers' needs. "We understand how important it is for brokerages to implement a meaningful and robust approach to privacy protection," comments Patrick Ballantyne, chief executive officer of the Registered Insurance Brokers of Ontario (RIBO).

"From a RIBO perspective, the requirement to maintain confidentiality has long existed in the *Code of Conduct*," Ballantyne says, which states, in part, the following:

> *A member shall hold in strict confidence all information acquired in the course of the professional relationship concerning the business and affairs of the member's client, and the member shall not divulge any such information unless authorized by the client to do so, required*

Illustration by Marc Mones/threeinabox.com

by law to do so or required to do so in conducting negotiations with underwriters or insurers on behalf of the client.

Similar language is echoed by regulators across the country. For example, the Insurance Council of British Columbia has long stated that there is "... no tolerance for intentional unauthorized access to or use of a person's information," and an entire section of the council's published *Code of Conduct* is devoted to client confidentiality guidelines.

Nevertheless, in 2015, the *Digital Privacy Act* was passed by the Parliament of Canada to amend PIPEDA and align it further with privacy statutes elsewhere. Additional responsibilities have been created that impact how brokers and insurers look at how they manage data, and how they communicate with customers about the risks associated with their own information.

NEW ACT, NEW OBLIGATIONS

The legislation applies to all organizations in Canada not otherwise subject to more specific provincial laws. New, additional obligations are included for organizations to track and record any and every breach of security involving personal information.

Further, the new stipulations require organizations suffering a breach to notify affected individuals and the Privacy Commissioner of Canada "as soon as feasible," in any situation where a breach represents "real risk of significant harm."

The concept of consent has been elaborated from its original expression in PIPEDA, so that now consent for collection, use or disclosure of information is deemed to be valid only if the individual understands fully the nature, purpose and potential consequences of sharing their information. The 2015 revisions also make a number of amendments to the exceptions where consent is not necessary for information to be disclosed, situations such as fraud or other criminal investigations, employment relationship management, or due diligence for potential business transactions.

Unlike the United States, there is no detailed breakdown of what constitutes "personal information" within the Canadian legislation. While the U.S. system provides a finite list of the specific types of data subject to special safeguarding, in Canada, "personal information" is simply "information about an identifiable individual."

This scope, therefore, includes any data that could lead to identifying an individual. Current analytics tools can

use virtually any collection of details to identify an individual by their consumption and activity patterns.

Developing a plan

For brokers, the consequences of the legislative updates are manifold. A brokerage's privacy strategy impacts every aspect of an operation, as customer information lies at the heart of every relationship and exchange. The new, added responsibilities and refinements can, consequently, lead to a wholesale review of all established processes within a firm.

In order to track all breaches as required by the *Digital Privacy Act*, security measures in place for a brokerage's internal and external network connections need to include the ability to both monitor and report on all access. Regular routines for reviewing the reports are also needed, so that unusual activity and warning signs are identified promptly.

Every operation is unique and the information collected varies, so the legislation does not mandate the specifics of monitoring, but instead is concerned with the capability of a business to be accountable. In addition, for situations where a breach is identified, brokerages need to have established procedures for informing affected parties, as well as the privacy commissioner.

Again, no specifics are mandated for the notification itself, other than the stipulation to accomplish it quickly.

With urgency as the prime directive, there is little time to be devising a response plan once security has already been compromised. The notification process may be complex, incur significant expense and the follow-through can linger over many months. Brokerages' current disaster plans need to incorporate strategy for immediate responses to breaches, including details of how the activity would be managed and funded.

Choosing partners wisely

Given the new mandate for customers' full comprehension of the implications of data collection or use when providing valid consent, particular care is in order when information is collected by third parties and may be used in determining what is offered to a customer.

Insurers commonly supplement the data directly supplied by clients and their representatives from additional sources, such as public databases or reports, claims archives or information culled from an individual's public activity online. Even without knowledge of an insurer's specific proprietary algorithms, brokers can still help consumers understand what information may be used and how it might affect their insurance options.

Brokers also need to be vigilant about how other business partners — vendors as well as insurers — may use or share information that the broker has collected and relayed, and challenge any potential inappropriate uses.

With the proliferation of "online" and "hosted" applications, some careful questions and a clear understanding of proposed contracts are necessary, so that a broker can keep customers informed about where their information goes and how it may be used.

Identifying potential liabilities

While safeguarding customer's interests, brokers should also recognize the impact on their own potential liabilities.

Internal procedures that reflect the new guidelines will be needed. Updates may include reviewing how client discussions are conducted, and revisiting published privacy policies and the disclosure templates used to document that clients fully understand the implications of providing consent.

To assist brokers with these internal reviews, an updated toolkit has been developed by the Insurance Brokers Association of Canada. The revised documents have been shared with the provincial and regional brokers' associations across the country, with the recommendation that input from provincial regulators be solicited, before the updated tools are, in turn, provided to broker principals.

Additional support can be found through the legal commentary offered in papers and interpretations published over the last few months, including from legal firms, the privacy offices of the various provinces and, above all, the Privacy Commissioner of Canada.

Included in the posted documentation are advisories on the creation of business privacy plans and conduct of privacy impact assessments of planned activities.

BEYOND COMPLIANCE

It is evident that the standard of care expected of any organization holding personal information continues to rise. Beyond simply complying with specific rules, such as the appointment of a privacy officer or notification of individuals following a breach, organizations are to emphasize the context in which these measures are executed.

The Office of the Privacy Commissioner of Canada looks for evidence that key components — from fundamental "building blocks" through ongoing controls and routines for regular updates — are embedded throughout the entire organization and its governance structure to foster a privacy culture.

Brokers are, of course, intimately familiar with what are essentially risk management processes; now, however, they have the added responsibility of conducting these reviews for their own operations, focusing explicitly on privacy.

Though the regulations to define the rules for breach notifications, and the attendant set of penalties for failure to do so, have not yet been published, the *Digital Privacy Act* is otherwise already in force.

In concert with the earlier PIPEDA principles, it is already providing a frame of reference for businesses, even as the options for distributing and deploying information continue to evolve.

There is much for brokers to do to help consumers understand how they are affected both by increasing risks and by the protection their advisors offer.