ETHICS, INSURANCE AND INFORMATION

To avoid regulation and legal exposures, insurers can develop their own information-gathering practices and privacy codes.

BY NORMA NIELSON

Who "owns" the information that has been gathered about an individual — the data gatherer or the data subject?

Companies and brokers have a right to gather information about persons who wish to apply for insurance; clearly, this is essential to determining the risk classification of the applicant. The insurer's right to information, however, is not unqualified. It must be balanced against the applicant's right to privacy.

Far from being an arcane issue, the appropriate use of information and respect of personal privacy are issues on the front lines for insurers. One only has to look to the controversies concerning AIDS faced by the life and health insurance industry over the past decade.

Some of these issues may well appear in any future privacy regulations and could include:

- Notification to individuals what information is being collected about them, why this information is needed, and how it is to be used.
- Relevance of information to the purpose for which it is being collected.
- Nondisclosure of information gathered.
- Explanation of why an individual has been denied access to a certain benefit, such as insurance.

The Information Age has led to an across-the-board increase in concerns about the quantity and quality of data maintained by businesses and government. A report released last fall from the newly formed Institute for Applied Ethics in Insurance reviewed the concepts of ethics and U.S. legal issues surrounding information. The report provided industry-specific discussions of standards for information gathering, record maintenance and protection of confidentiality.

Nielson: Front line issues.

Canada at present has no statutes that govern the information practices of insurance companies (there is a voluntary privacy code sponsored by the Insurance Council of Canada: see sidebar). In general, information gleaned by Canadian business that is legally and voluntarily given, such as that obtained in providing insurance, can be used in the private sector.

The use of this information for marketing and other similar purposes is currently legal, though abuses would likely attract regulatory scrutiny. Privacy protection comes primarily from the common law protections derived from torts such as appropriation of personality, trespass, and defamation. Regulators have not intervened beyond telling consumers to be careful. Even if a stable legal standard were available, behaving legally is not necessarily acting ethically.

In today's environment, insurance companies abuse personal information at their own — and the industry's — risk. There are growing consumer activist movements that seek to place shackles on blatant invasions of privacy committed with impunity by some private organizations. There is also some business support for a more uniform body of law to govern the matter to stem inconsistencies across jurisdictions.

Far-sighted insurance companies that seek to avoid government regulation are paying close attention to the demands of consumers for greater respect of their personal privacy. Regardless of legal standards, a corporation can apply broad ethical concepts to guide the planning, development, implementation and usage of information systems today. Standard risk management practices can help professionals organize a wide assortment of material about how to reduce and manage those risks.

Risk identification is, as always, the most important step in the process and the most difficult to generalize. For risk control, a proper balance must be determined. Too little control can risk information privacy, accuracy, access, and intellectual property; too much control can seriously hamper productivity in the form of unnecessary overhead or uncomfortable working conditions. Managing the risk of information requires the attention of management

in three major categories: expectations of management and staff, behavior of management and staff and outside threats

The foundation for a proactive ethical environment is a corporate culture in which the rules and regulations governing data creation, use, maintenance, and disposal have been established and communicated to all users. To be successful, the firm must establish and maintain the desired corporate culture by defining the responsibility of each employee. Two major areas that assist in developing appropriate expectations are a code of ethics and a set of sound information systems policies.

Creating a code of ethics is one way to communicate expectations to the firm's employees. The code should convey management's philosophy on information value, protection of information assets, appropriate use of information, and the responsibility of every employee to "live the philosophy." Although employees are an organization's most important resource, they are also the most likely threat, especially the dissatisfied and disloyal. Therefore, it is extremely important to create a staff that is ethics conscious and motivated to avoid ethical incidents. Because motivation — as well as eagerness to follow established routines — tends to decrease with time, creative measures are needed to keep ethical consciousness high.

To be useful, the code(s) must be specific enough so employees can see clearly the association between the tasks they perform and the code(s) of ethics. An organization may have both a general code of ethics to act as a high-level set of guidelines and a code of ethics directed specifically toward each work group. For example, the technological employees who design, construct, and implement information systems are an extremely important work group in conveying an appropriate philosophy toward information assets.

The second aspect of setting expectations is translating the philosophy generated in the code of ethics into information systems policies that are monitored and evaluated. These policies should be integrated into business processes, procedures, and practices. However, they are more specific and should be measurable with adequate investment of effort to assure that when objectives contradict each other — such as freedom of information and privacy policies — those conflicts are resolved.

Once policies have been written, appropriate security measures for the identified ethical vulnerabilities and risks must be selected. Measures usually correspond to (1) loss prevention, (2) loss reduction, and (3) loss recovery familiar to the risk management discipline. Each measure usually will have three media formats: physical, logical, and administrative. For example, loss prevention measures can be implemented that include physical placement of servers and work stations or terminals in building, levels of humidity, type of fire extinguishing devices, and power supply. Logical measures include limiting the life of passwords, station restrictions, time restrictions, and composition of password. Administrative measures include procedures for data disposal, disaster planning, back-ups, and building systems.

Information security is a "people problem." While technology can help minimize breaches, it cannot eliminate them. Most organizations will pay more attention to the outside "snooper" and willingly spend more time, effort and money to prevent these types of intrusions when ethical misuse of information from inside the organization is much more prevalent. A comprehensive program is necessary to create the desired usage and security environment for an organization. As the environment, industry, competition, clients, employees, and technology change, the comprehensive program for information security must include an evaluation process.

In addition to managing the information security issues generated inside the organization, you also need to manage information security threats that may come from the outside. Two major areas of concern here are Internet access (or other unsecured networks) and remote access.

There are important areas of information-gathering activity that insurers should regard as relevant to their operations. Specifically, they should recognize that:

- privacy concerns of their customers are legitimate and appropriate steps must be taken to secure data;
- careful data handling can be a competitive advantage;
- almost every public policy activity of insurers, agents, and trade organizations can have secondary effects that deal with data and privacy;
- rules governing the privacy of data will evolve from social values and eventually produce a body of common law;

continued on page 66

IBC HOPES FOR PRIVACY CODE PUSH THIS FALL

Although the property and casualty insurance industry has had a formal privacy code in place since 1996, only a half dozen insurers have officially adopted it for their operations.

Insurance Bureau of Canada (IBC) legal counsel Steven Lingard says that the delays have involved getting the code on the agenda of a company's board of directors and having it approved, especially for branches of foreign insurers operating in Canada. "The issue has been more one with process, rather than any philosophical disagreement per se with the privacy code," says Lingard.

He expects a majority of IBC members, "as measured by market share," to adopt the code this fall. The IBC has asked companies to appoint a privacy liaison representative to monitor privacy issues at the company level and deal with the IBC on matters of client confidentiality.

The privacy code was approved by the IBC board of directors in June, 1996 and received accreditation for meeting the standards of the Canadian Standards Association in February, 1997. The Office of the Superintendent of Financial Institutions (OSFI) has made public comments about potential regulations on client confidentiality and a federal privacy law for the private sector, but Lingard indicated that ongoing OSFI reorganizations have "put the issue on the back burner."

— Craig Harris

ETHICS . . .

continued from page 50

• society harbors an inherent distrust of large organizations, including insurers.

This distrust, in turn, implies that regulation of the insurance industry's data practices is a real possibility. One strategy to avoid unacceptable regulations in this area is to work proactively to develop the system that will provide the regulation.

Insurers should make an active decision about where to go next. With the convergence of sophisticated technology for gathering customer data and increased public concerns about privacy, now is the time to actively join forces as an industry to help define the future of information handling. If they choose this proactive path, the insurance industry can have a profound impact as society enters the Information Age.

The law, because it evolves through a series of court cases, lags behind new developments in society. If the industry chooses to remain on the sidelines and merely react to decisions, they will forfeit their right to complain about the results. The insurance industry is today challenged to step forward and accept the substantial opportunity that is available to provide leadership in this area — and to potentially avoid unwanted regulation.

Failure to do so could see test cases holding the property/casualty insurance industry responsible to pay court-ordered financial damages for such tort claims as defamation of character under a wide range of property-casualty contracts. ❐

Dr. Norma L. Nielson is chairholder in Insurance and Risk Management in the Faculty of Management at the University of Calgary, where she teaches courses and conducts research in a wide range of insurance and risk management subjects. *She would like to acknowledge the contributions of Daniel J. Brown, Linda Gammill, and Mary Alice Seville, and the assistance of Peter Bowal with respect to some specifics of Canadian law.*

LETTERS

NUMBER CRUNCHING

Regarding your editorial, Privatization Potential *(CI, August, 1998)*, the 1995 statistics you quoted for Manitoba Public Insurance are for a 16 month time period as a result of the corporation changing its year-end to February 28 from October 31.

MPI's combined ratio for 1996 and 1997 fiscal years is 108.3 per cent and 110.6 per cent respectively. Overall, in the 26 year history of the corporation, the combined ratio has been 115.5 per cent. Accumulated retained earnings are $102.1 million, with annual premium volume of approximately $483 million per year.

Also over its 26 year history, MPI has returned almost 90 cents of every dollar in insurance premium earned back to policyholders in the form of claims payments.

B.W. Galenzoski, vice president, finance
Manitoba Public Insurance