



Protect Your Data

With the importance placed on cyber security and data breaches today, state laws place a legal duty on businesses with access to personal client information to have data security plans in place. Agents collect and store personal information on customers on a daily basis. Interestingly, the information that an agency has about its clients and their coverages constitutes a major asset for an agency. Just like insureds who may collect and store personal information, the agency has a duty to keep the personal information of their clients private.

Beyond legal duties, it only makes sense that an agency would want to keep its major asset protected and confidential for business reasons. It is important to keep in mind that protecting personal information of customers is not a large agency or small agency issue; it's an every agency issue. A large agency cannot simply sit back and assume that its IT department has handled its obligation without a thorough review. And a small agency cannot assume that it does not have the same obligation to keep their data secure just because their resources may be more limited. The IT challenges and the complication of understanding legal duties make protecting information a complex issue, but it is a responsibility nonetheless.

When establishing a plan to keep an agency's data secure, consider the following questions:

What is personal information? Generally, it's a client's name and other private identifying information, such as a social security, driver's license and credit, debit or other account numbers. Information that can be obtained lawfully from public records is not generally considered personal information.


Where is the data being stored, and is it protected? If in paper form, are the documents being stored in files? If so, where? Are they left unattended on desks? If stored in file cabinets, are they locked? Are there locks on the doors and windows of the building and room where the documents are stored? Is there a burglar alarm or security camera? What is the agency's policy for throwing out paper? Is the paper shredded? Is it disposed of in accordance with state laws?

For electronic data, make sure that there are strong passwords to access servers, desktop PCs, laptops and other portable devices, and that these passwords are changed on a regular basis. Make sure that the passwords are not shared. Unattended PCs should be locked. Consider strong anti-virus and malware protections.

Is the electronic data on laptops or other portable devices? If so, the data may need to be encrypted. Any emails sent out that have personal information should also be encrypted.

Who has access? Access should be limited to authorized persons only. One or more employees should be designated to maintain the data security plan. There should be ongoing employee training regarding the agency's security policies and the steps necessary to keep data secure. There should be disciplinary measures in place for violations of data security plan rules. Terminated employees should immediately lose access to all data. If your agency contracts with third party vendors that might have access to any personal information, a written agreement can ensure they have their own data security plan in place.

What if the data gets compromised? Comply with the data breach disclosure laws in your state which outline the requirements for notifying clients of any breach of the system data. Consult with an IT expert and counsel if data, a laptop or other portable device containing personal information is stolen. Because a breach of data privacy could be very costly to an agency, consider adding personal data protections coverage. Such coverage may be available under an existing E&O policy, but if not, consider a stand-alone policy.

Laws on this issue vary greatly by state and are evolving rapidly. Still, remember guidelines that an agency needs to consider in regards to keeping data secure. A breach of the obligation to keep a client's personal information private could not only result in costly remediation measures and loss of agency productivity, but also irreparable damage to an agency's reputation. 

Caryn Mahoney is an assistant vice president, claims and liability management, with Swiss Re. She handles claims against insurance professionals out of Swiss Re's Overland Park, Kan., office.

Data Security and Privacy Tools

IIABA's Agents Council for Technology (ACT) has information and tools to help agencies understand the issues and requirements associated with protecting customer information. ACT has even created a prototype agency security plan available to members. Visit the Security and Privacy section of ACT's website at www.iiaba.net/act.

The potential first- and third-party liability of a data breach affects not only insurance agents but their customers as well. To help agents protect both themselves and offer coverage to their customers, IIABA is offering members access to stand-alone Cyber Liability markets on Big "I" Markets. Visit www.bigmarkets.com to learn more.

Remember, offering cyber liability to your customers can reduce E&O exposures to uncovered claims while increasing agency revenue.

—C.M.