Establishing an Information Security Program

This paper is written by Elsie Reamy for the Professional Insurance Agents Association of Virginia and the District of Columbia, 8751 Park Central Drive, Suite 140, Richmond, Virginia 23227. Where a law or administrative action is quoted, the type is italicized. Be cautious in the use of un-italicized material, as it is a draft. The advice here given is not to serve as a substitute for legal counsel, but we hope it presents a prudent course of action.

Virginia law changed on July 1, 2003, when it added section §38.2-613.2 requiring agents, insurers, and insurance-support organizations to develop technical and physical safeguards to protect the security of customer information and implement a written information security system. A similar law in the District of Columbia was effective on April 3, 2001. Both laws stem from the Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act. The federal acts, known as GLBA and HIPAA, formalize the agent's obligation to protect client information and were passed because the broadened use of technology make it more difficult to protect individual's information. These laws are causing the enactment of laws across the country similar to those of Virginia and the District of Columbia.

Another reason it's extremely important that you have an information security system is because some insurance companies and vendors are requiring agents to sign agreements relative to "private" information. This includes vendors who work with motor vehicle, credit, and comprehensive loss underwriting exchange (CLUE) reports. When you're asked to sign such agreements, it is imperative that you understand the obligations imposed upon you. Often, the type of information will differ from one company to another and from one vendor to another; one reason for this is some who operate in multiple jurisdictions have a procedure that meets the approval of the jurisdiction with the most stringent requirement. If something is unclear, write a letter to your carrier or vendor seeking clarification. It's a good idea to develop a matrix noting the differences in the restrictions contained in these agreements with respect to the definition of protected information and how such information will be protected. This matrix will provide documentation of your effort to determine compliance obligations.

Virginia's law reads:

> *§ 38.2-613.2. Information security program.*
> *A. Each insurance institution, agent, and insurance-support organization shall implement a comprehensive written information security program that includes administrative, technical, and physical safeguards for the protection of policyholder information. The administrative, technical, and physical safeguards included in the information security program shall be appropriate to the size and complexity of the insurance institution, agent, or insurance-support organization and the nature and scope of its activities.*
> *B. The information security program shall be designed to:*
> *1. Ensure the security and confidentiality of policyholder information;*
> *2. Protect against any anticipated threats or hazards to the security or integrity of the information; and*
> *3. Protect against unauthorized access to or use of the information that could result in substantial harm or inconvenience to any policyholder.*

On May 19, 2003, the Virginia Bureau of Insurance issued an administrative letter about this bill.

Virginia's administrative letter reads: *May 19, 2003 - Administrative Letter 2003-4*

> *TO: All Insurers, Health Service Plans, Health Maintenance Organizations, Surplus Lines Brokers, and Other Interested Parties*
> *RE: Senate Bill No. 878 (Privacy Safeguards)*
> *This administrative letter is intended to provide guidelines to insurers, agents (including surplus lines brokers), and insurance-support organizations for the purpose of implementing the provisions of Senate Bill No. 878 (effective July 1, 2003). The following actions and procedures are examples of methods to implement the requirements set forth in § 38.2-613.2 of the Code of Virginia. These examples are non-exclusive illustrations of actions and procedures that insurers, agents (including*

surplus lines brokers), and insurance-support organizations may follow to implement the requirements set forth in § 38.2-613.2.

Examples of Methods of Implementation

A. Identify reasonably foreseeable internal or external threats that could result in unauthorized disclosure, misuse, alteration or destruction of policyholder information or policyholder information systems.

B. Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of policyholder information.

C. Assess the sufficiency of policies, procedures, policyholder information systems and other safeguards in place to control risks.

D. Design the information security program to control the identified risks, commensurate with the sensitivity of the information, as well as the complexity and scope of activities.

E. Train staff, as appropriate, to implement the information security program.

F. Regularly test or otherwise regularly monitor the key controls, systems, and procedures of the information security program, the frequency and nature of such monitoring to be determined by the insurance institution, agent, or insurance-support organization.

G. Exercise appropriate due diligence in selecting service providers.

H. Require service providers to implement appropriate measures designed to meet the objectives set forth in this administrative letter and, where necessary, as determined by the insurance institution, agent, or insurance-support organization, take appropriate steps to confirm that service providers have satisfied these obligations.

I. Monitor, evaluate, and adjust, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of policyholder information, internal or external threats to information, and changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to policyholder information systems.

Each organization to which this letter has been sent should see that this letter is directed to the proper persons, including appointed representatives. Copies of Senate Bill No. 878 may be found at http://legis.state.va.us/. Copies of this letter may be found at www.state.va.us/scc/division/boi/. Questions regarding this administrative letter may be directed to JoAnne Scott at (804) 371-9600.

Cordially, Alfred W. Gross, Commissioner of Insurance

The District of Columbia's law reads:

§3613 - Each licensee shall implement a comprehensive written information security program that includes administrative, technical and physical safeguards for the protection of customer information. The administrative, technical and physical safeguards included in the information security program shall be appropriate to the size and complexity of the licensee and the nature and scope of its activities.

§3614 - A licensee's information security program shall be designed to: (a) ensure the security and confidentiality of customer information; (b) protect against any anticipated threats or hazards to the security or integrity of the information; and (c) protect against unauthorized access to or use of the information that could result in substantial harm or inconvenience to any customer.

§3615 - Actions and procedures described in §3616 through §3619 of these rules are examples of methods of implementation of the requirements of §3613 and §3614 of this regulation. These examples are non-exclusive illustrations of actions and procedures that licensees may follow to implement §3613 and §3614 of these rules.

§3616 - The licensee shall (a) identify reasonably foreseeable internal or external threats that could result in unauthorized disclosure, misuse, alteration or destruction of customer information or customer information systems; (b) assess the likelihood and potential damage of these threats taking into consideration the sensitivity of customer information; and (c) assess the sufficiency of policies, procedures, customer information systems and other safeguards in place to control risks.

§3617 – The licensee shall (a) design its information security program to control the identified risks, commensurate with the sensitivity of the information, as well as the complexity and scope of the licensee's activities; (b) train staff, as appropriate, to implement the licensee's information security program; and (c) regularly tests or otherwise regularly monitors the key controls, systems and

procedures of the information security program. The frequency and nature of these tests or other monitoring practices are determined by the licensee's risk assessment.

§3618 – The licensee shall (a) exercise appropriate due diligence in selecting its service providers; and (b) require its service providers to implement appropriate measures designed to meet the objectives of this regulation, and, where indicated by the licensee's risk assessment, takes appropriate steps to confirm that its service providers have satisfied these obligations.

§3619 – The licensee shall monitor, evaluate and adjust, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its customer information, internal or external threats to information, and the licensee's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes to customer information systems.

§3620 – Violation of these rules shall constitute an unfair trade practice under §101(9) of the Insurance Trade and Economic Development Amendment Act of 2000, effective April 3, 2001.

§3699 –Definitions:

Customer information means the same as nonpublic personal information, and applies whether in paper, electronic or other form, that is maintained by or on behalf of the licensee.

Customer information systems means the electronic or physical methods used to access, collect, store, use, transmit, protect or dispose of customer information.

Service provider means a person that maintains, processes or otherwise is permitted access to customer information through its provision of services directly to the licensee.

Discussion of Laws

Most people in the insurance industry would agree agents have always had an implied duty to protect client information. This means agents could have been held liable for damages arising from negligence in handling client information. However, as you've read here, the law now specifically says covered parties (including agents) must create and carry out reasonable and prudent measures to execute the responsibility by establishing an information security program. It must be designed to ensure the security and confidentiality of customer information and protect against anticipated threats to the security of the information and unauthorized access to or use of information that could result in harm to the customer. The good news is that the law takes into account that the agent's security program be appropriate to the size, complexity, nature, and scope of the business. . Here are some details on what we think you should do:

Assess risk. You must take a hard look the information your agency gets, how it is handled, and how it is shared. You must identify threats that could result in disclosure or misuse of customer information and assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information.

What kind of threats do you have? Here are just a few: Do you have data (assets, income, beneficiaries, etc.) about people that might be of interest to others, such as a competitor or relative? What facts do employees give others? Do they know they should not share telephone numbers with inquirers? (This could be particularly disturbing to an insured with an unlisted number.) Could someone walk in your agency while the door is unlocked for the after-hours cleaning people and easily look at files or computer data? Do you or some your employees leave computers or desks unattended with information visible or easily accessible to a casual visitor? Do you keep information about former customers as secure as for your current ones? Could a "hacker" access your database? Are you thinking of joining with a cluster of agencies or selling or merging your agency with others? Be careful what you share.

What information does your agency need to shop quotes and place business? Since this will differ based on the line of insurance involved, you must look over every line for which your agency solicits or binds coverage. Make sure your agency procedures manual says you will request only minimal information necessary to place the requested insurance; it's best not to have information that you don't need. Often, asking for more information than needed doesn't bode well with the client anyway, but now that it's more important that you not be accused of causing damages because of sharing personal information,

Assess your system. Take a look at the procedures used with customer information at your agency. Ask employees to help you think of things in your files that should not be disclosed. Ask your companies and automation vendors what they are doing and what they suggest that you do. They must also comply with this law, and many of their procedures can be used at your agency.

Automation vendors should be aware of security problems that have affected their specific software systems and should have or be able to direct you to where you can secure patches to fix them. If they can't help you, perhaps you should consider changing service providers. Be sure vendors are aware of the variables in their information technology configuration so they can take them into account when recommending security precautions, updates, and fixes. Be sure they provide new patches and security alerts as they are developed for your present software. When obtaining new software, be sure all known bugs have been fixed. If this is not possible, as with many off-the-shelf products, go to the manufacturers' web site and download appropriate patches. For both old and new software, if possible, have manufacturers alert you as patches are developed. Document that your service provider is designing measures intended to prevent the identified risks and confirm that the service provider has implemented those measures. Be sure you utilize all of the tools, such as software patches, provided by your vendor.

Ask the vendors from whom you get motor vehicle reports, CLUE reports, and insurance scores about their procedures. Tell them they should ask for only minimum information needed for the particular transaction. Place these parties on notice of (1) the agent's privacy obligations – that you must keep clients' information according to law; (2) the limited use (only for the immediate purpose) for which they may use non-public personal information; and (3) your ownership of expirations which they may not usurp by using expiration information for any purpose beyond completing immediate transactions. A letter is at the end of this document to help you write them; it will probably not be considered legally binding but may help. A non-disclosure agreement would be better, but we cannot issue a model one because agents have signed varying agreements. Perhaps some of the vendors will have such agreements available.

Most agencies employ virus protection measures; if you don't, you should. Advancements in computer technology and the ability of hackers make the agent's job more challenging than it used to be. Firewalls monitor what goes in and out of a computer system and block many intruders and viruses; ask your vendor about your firewalls and how safe you are from a "hacker" or virus. Although firewalls are usually software programs, there is firewall hardware that provides another level of security. In addition, agents may consider an intrusion detection system (IDS). Should something make it past the firewall, IDS can determine who and what is involved so the situation can be remedied before much damage is done. Be sure all of this hardware and software – whether it's a firewall, IDS, anti-virus, or something else – doesn't conflict or interfere with your agency vendor applications. Often, it does.

Do you have procedures in place to educate employees on privacy issues? Is the treatment of information included in employee training? All of your procedures and systems must be carefully and clearly written into the employee manual's code of conduct. Staff must be trained in what is expected of them and in how to perform these tasks. Should employees' passwords change more often? Find out if employees have shared their codes with others. Do you change identification codes of employees who leave you? You should. You should not re-assign these same codes to new employees.

List the ways you get information from insureds and prospects – in person? email? regular mail? fax? When insureds fax information to you, does the fax stay in an open area until it's delivered to you? Require faxed and mailed information be immediately delivered to you. If it is emailed, be sure you have a secure provider. It's extremely important that your procedures manual document how you handle this so if your security procedure is questioned, you can show your agency's tangible proof of the due care.

Do employees understand the kind of information they can disclose and to whom they can disclose it, especially that relating to people's credit, finances, character, health, or reputation? Look at your employee manual; do you have strong wording about keeping what goes on in your agency confidential? Do you enforce the rules you have in the manual?

Design and write your security program. In your information security program, say where you get data, how you treat what you receive while it is in the office, and with whom it is shared. State why you must share it with various entities and state exactly what is shared with whom. Include the means you use to create, retain and retrieve archived files with full details on your automation system and how it is protected from hackers, viruses, and the like.

If you must get motor vehicle reports, credit reports, CLUE reports, etc., say so. If the information is seen at your agency, say so. If all you see is a "score," say that. If the procedures differ according to the company with whom you work, say that. If what you see is shared only with insurance companies with whom you have a contract, say that. If it may be shared later with other insurance companies who may offer better coverages or rates, say that. If you send out privacy notices to your insureds, say so; if you depend on your companies to do it in your behalf, put that in the written program. If you send forms that allow your insureds to tell you if you may or may not share information, describe your procedure.

All of this is even more important if you have health or medical information; the privacy requirements are more stringent here. Remember when one of your insured businesses adds an employee to a health/ medical insurance program, you must advise the employee that if his employer wants to shop for coverage through another insurance company, you may have to share health/medical information with the prospective insurer. Ask the employees to sign that they have read, understand, and agree you may have to do this. Many times when group disability programs are written for employers, insurance companies will require information, such as each insured's salary for underwriting purposes. However, if you know data about employees' health, salary, or finances will be given to a prospective insurer on only an aggregate basis and you don't have to give individually identifiable information; say that too.

You should understand – and see that your employees understand – the difference in the requirements for "opt in" and "opt out." In most instances, insurance companies send the required notices to insureds and you can share limited information (such as required financial data) unless they tell you that you can't – that's "opt out." An exception to this is that the agency must have sent its own notice to insureds within the past twelve months before giving information to another insurance company. Another exception is, in most instances, sharing health or medical information requires the insured to tell you that you can do so – that's "opt in." (PIA previously sent you information and a suggested letter that you may send your clients relative to this; if you want another copy, just ask us for it.)

If you share any of your insureds' information with another department or branch and they use it for marketing your insureds for other products, by all means say that. If you don't share it with a marketing group, it would be a good idea to include that in your security manual.

In most of the PIA-member agencies, every employee will have access to all files; but if you have staff assigned by line of insurance, that should not be the case, so include who has unlimited access and which files have limited access and by whom. If you require that computer screens are blackened and files put away when employees leave their workstations, say so. Include how you assign employees' computer identification codes and who has access to them. State that you change the codes when you have staff turnover and you do it more quickly when there's a termination.

Enforce Your System: Write down how you will control the identified risks and how you train your staff to implement them. Document that you include the matters in staff training. On a regular basis, see if what you've written is in operation. State in your manual that while an error can and will occasionally occur, a pattern of errors is not permitted or tolerated. Make enforcement clear; say the consequences, such as retraining, termination, reports to authorities, and legal proceedings.

Be Willing to Change: Be willing to make adjustments as needed. Over time, there will be changes in technology, different clients, and changing business arrangements. Be certain your systems have kept reasonable pace with technology development. It would be good to list your technology goal, especially

virus protections, in your procedures manual. Agencies should budget for technology and secured systems in their annual expenditure budgets.

What Else? The question comes to mind: do you need an attorney or consultant to assist you? The answer is maybe. We can't speak for all of our members as we have some who have no employees, some who have few, and some who have dozens or 100+. We recommend that you ask your software vendor and your carriers what they think, including if they think you need an attorney or consultant. If they think you do, perhaps they can recommend someone to you.

Here is the sample letter we said in the "Assess your System" section on page 3 that we would give you.

SAMPLE AGENT LETTER TO VENDORS

Dear _____:

In the interest of clarity, we are writing to notify XXX (insert the name of vendor firm in blank) regarding several very important ownership and privacy issues that will no doubt come into play throughout the course of our vendor-vendee business relationship. It is very important that there be no doubt as to where our agency stands on these issues.

In the course of this business relationship, you will be provided with or have limited access to certain nonpublic customer or consumer information regarding our insured clients. Significantly, both federal and state privacy statutes and our own agency agreements with different carriers place very strict limitations on our and your ability to use or disclose this information. In addition to the restrictions placed on non-public personal information by the various statutes and agreements, common law has long recognized the independent insurance agent as the owner of client expiration information. The courts have extended the term "expirations" to include not only the physical records of the insurance agency, but also the exclusive right to use such records to solicit renewals and service the client's insurance needs.

As a result of the various statutory restrictions on non-public personal information and the independent agent's ownership rights over certain pieces of client information, we are compelled to notify the vendors to whom we may be required to provide such client information in the normal course of business, that our agency will give XXX (insert the name of vendor) only the minimal amount of nonpublic personal information which is necessary to complete the transaction and perform the services which XXX (insert the name of the vendor's firm) has agreed to provide to our agency. Any personal information or the occasion of receiving this information from our agency can be used by your firm for only the purposes of completing the services XXX (Insert name of vendor firm) agreed to provide to our agency.

This letter is intended to confirm with you, our vendor, that client information we share with you constitutes neither a waiver nor a relinquishment of any ownership interest or right we have to such clients information. Our providing you with such client information is not a license for you to use the information in any manner inconsistent with the very limited service you provide to us. We strongly recommend that you become familiar with the specific limitations of the federal and state privacy statutes that apply to your business operations and that you discuss the same with legal counsel familiar with these issues.

We look forward to continuing to work with your firm in the future.

Sincerely,

Your Signature

This article was written with the assistance of information from the Virginia Bureau of Insurance, the District of Columbia Insurance and Security Regulation, the National Association of Professional Insurance Agents, and the Professional Insurance Agents Association of New York. It is not intended to be a legal document, but could be beneficial to PIAVA/DC members.