COMMONWEALTH OF VIRGINIA

ALFRED W. GROSS
COMMISSIONER OF INSURANCE

P.O. BOX 1157
RICHMOND, VIRGINIA 23218
TELEPHONE: (804) 371-9741
TDD/VOICE: (804) 371-9206
http://www.scc.virginia.gov

STATE CORPORATION COMMISSION
BUREAU OF INSURANCE

September 1, 2009

To: All Insurers, Health Service Plans, Health Maintenance Organizations, Surplus Lines Brokers, and Other Interested Parties

Re: Guidance for Agents Developing Privacy Safeguards

On May 19, 2003, the Bureau of Insurance issued Administrative Letter 2003-4, which provided guidance on implementing an information security program in compliance with the newly enacted § 38.2-613.2. This law requires every insurer, agent/agency, and insurance support organization to design and implement a **written** program to ensure the security and confidentiality of policyholder information. This program must address anticipated threats or hazards to the information and must provide for the prevention of unauthorized access to or use of the protected information that may result in substantial harm or inconvenience to any policyholder.

The purpose of this informational letter is to assist insurance agents/agencies in complying with the provisions of § 38.2-613.2. The Bureau of Insurance is providing additional guidance to help ensure that agencies have in place a comprehensive written information security program appropriate to the size and complexity of the agent/agency.

Agents and agencies should consider the following information when developing their own individualized security program:

Physical Security of Policyholder Information

The law requires physical safeguards for the protection of policyholder information. Questions to consider when evaluating the physical security of information include:

When you leave in the evening, how secure is your physical office? Is it in a stand-alone building or is it in a shared space? Is there a security service at night?

Do you have key-controlled access to individual offices or are all employees in an open office setting?

Do you have a cleaning crew? Do you know your cleaning crew? Do you dispose of potentially sensitive information in the daily trash?

Do you have a paper shredder? Do you have a policy regarding shredder usage?

Are files stored in a locked or access controlled strong room? Are files kept in desks or credenzas? Are files left in the open on desktops? Do you allow files to be removed from the office?

During the day, are visitors allowed in the non-public areas of the office? If yes, are they always escorted?

Do you have desktop computers? Do you have laptop computers? Do you use personal data assistants (PDAs)? Are these items secured when not in use or transported?

Is access to files restricted to only those employees who have a "demonstrated need"?

Do you have a document retention schedule? Do you follow it?

Virtual Security

Agents must also address the security of policyholder information in a virtual environment. Do you have desktop computers, laptop computers, PDAs, internet access, internal networks, external networks, wireless networks, remote servers, and/or offsite backups? If any of these or similar electronic devices are used, every written program should consider the following:

Do you have a password protected screensaver on your computer desktop? Do you log off your computer when you leave the office for lunch, meetings, or at the end of the workday?

Do you keep your passwords in a protected area or do you write down your passwords on paper or sticky notes and keep them near your computer?

If you have a server, is it in a secured computer room with limited access? Do you have a dedicated network administrator?

Do you use removable storage media such as zip drives, USB memory sticks or thumb drives, CDs, floppy disks, or external hard drives?

Do you use email? Do you have an internal email server or do you use external email services such as AOL, Yahoo, or Hotmail?

Do you encrypt policyholder data? Do you encrypt backup data? Do you encrypt emails? Do you encrypt removable media?

Do you run virus software protection? Do you run a personal firewall? Do you run network firewalls? Do you run spyware or malware protection or services?

Can employees access customer and policy data remotely from the agency computers using a remote PC, home computer, laptop, or public computer?

These are all important questions that any information security program should address. Many of the best security practices are very simple. For example, agents should take care not to send personal information via unsecured email. Files should be kept in lockable storage areas. All computer backups should be encrypted. Passwords should be closely guarded. All electronic devices should be protected from loss or theft. No non-public customer and policy information should be stored on unprotected PCs, PDAs, laptops, and portable media. Employee training with the security program is vital.

No guidance document can reliably enumerate all items necessary to guarantee protection of policyholder information. Therefore, each agent/agency must carefully evaluate their individual operation and circumstances to develop a comprehensive written information security program tailored to protect policyholder information.

There is a wealth of information available from numerous sources that can assist you in evaluating and addressing protection issues for you and your agency. The following websites provide specific guidance to agents on how to protect policyholder information:

The Independent Insurance Agents & Brokers of America (IIABA) at http://na.iiaa.org/ACTDownloads/ACT1031505.doc

The Independent Insurance Agents of Virginia at www.iiav.com

The National Association of Professional Insurance Agents (for member agents/agencies) at http://www.pianet.com/IssuesOfFocus/OngoingIssues/privacy/

This letter is intended to be used as an informational guide only. The Bureau does not make specific recommendations concerning the design and implementation

of a particular agency's information security program. We encourage all agents and agencies to seek specific legal or other expert advice if needed to assist in developing a written information security program.

Each organization to whom this letter has been sent should make sure that it is directed to the proper persons, including appointed representatives. Copies of this letter may be found at www.scc.virginia.gov/division/boi/. Any questions regarding this letter may be directed to:

For P&C related questions:

Michael T. Beavers, CPCU, CIC, CIE
Supervisor, P&C Agent Investigations
Virginia Bureau of Insurance
Agent Regulation and Administration Division
P.O. Box 1157
Richmond, Virginia 23218
(804) 371-9465

For L&H related questions:

Ray Anderson
Supervisor, L&H Agent Investigations
Virginia Bureau of Insurance
Agent Regulation and Administration Division
P.O. Box 1157
Richmond, Virginia 23218
(804) 371-9970

Cordially,

Brian P. Gaudiose
Deputy Commissioner
Agent Regulation and Administration Division

BPG/MTB/ifg