ALFRED W. GROSS
COMMISSIONER OF INSURANCE
STATE CORPORATION COMMISSION
BUREAU OF INSURANCE

COMMONWEALTH OF VIRGINIA

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

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 administrative letter may be found at www.state.va.us/scc/division/boi/.

Any questions regarding this administrative letter may be directed to JoAnne Scott at (804) 371-9600.

Cordially,

Alfred W. Gross
Commissioner of Insurance