

**NEW YORK STATE  
INSURANCE DEPARTMENT  
REGULATION NO. 173  
(11 NYCRR 421)**

**STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION**

I, GREGORY V. SERIO, Superintendent of Insurance of the State of New York, pursuant to the authority granted by Sections 201 and 301 and Article 24 of the Insurance Law, and in accordance with the provisions of 15 U.S.C. 6801, 6805(a)(6), 6805(b), 6805(c) and 6807 and 15 U.S.C. Chapter 94, do hereby promulgate a new Part 421 of Title 11 of the Official Compilation of Codes, Rules and Regulations of the State of New York (Regulation No. 173), to take effect upon publication in the State Register. Part 421 shall read as follows:

(ALL MATERIAL IS NEW)

**TABLE OF CONTENTS**

**GENERAL PROVISIONS**

- Section 421.0 Preamble.
- Section 421.1 Definitions.
- Section 421.2 Information security program.
- Section 421.3 Objectives of information security program.

**DEVELOPMENT AND IMPLEMENTATION OF INFORMATION SECURITY PROGRAM**

- Section 421.4 Examples of methods of development and implementation.
- Section 421.5 Assess risk.
- Section 421.6 Manage and control risk.
- Section 421.7 Oversee service provider arrangements.
- Section 421.8 Adjust the program.

**ADDITIONAL PROVISIONS**

- Section 421.9 Determined violation.
- Section 421.10 Compliance date.

**GENERAL PROVISIONS**

**Section 421.0 Preamble.**

(a) This Part establishes standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of

customer information, pursuant to sections 501, 505(b), and 507, codified at 15 U.S.C. 6801, 6805(b) and 6807, of the Gramm-Leach-Bliley Act.

(b) Section 501(a) provides that it is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information. Section 501(b) requires the state insurance regulatory authorities to establish appropriate standards relating to administrative, technical, and physical safeguards: (1) to insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

(c) Section 505(b)(2) calls upon the state insurance regulatory authorities to implement the standards prescribed under Section 501(b) by rule with respect to persons engaged in providing insurance.

(d) Section 507 provides that a state regulation may afford persons greater privacy protections than those provided by subtitle A of Title V of the Gramm-Leach-Bliley Act. This Part requires that the safeguards established pursuant to this Part shall apply to nonpublic personal information, including health information, as health information is covered by the privacy protections set forth in Part 420 of this Title (Regulation 169).

### **Section 421.1 Definition.**

For purposes of this Part, the following definitions apply:

(a) "Customer" means any customer of the licensee as the term customer is defined in Section 420.3(h) of this Title (Regulation 169).

(b) "Customer information" means nonpublic personal information as defined in Section 420.3(r) of this Title, about a customer, whether in paper, electronic, or other form, that is maintained by or on behalf of the licensee.

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

(d) "Licensee" means a licensee as that term is defined in Section 420.3(p)(1) of this Title, except that "licensee" shall not include: a purchasing group; or an unauthorized insurer in regard to the excess line business conducted pursuant to Section 2118 of the Insurance Law and Part 27 of this Title (Regulation 41).

(e) "Service provider" means any person or entity that maintains, processes, or otherwise is permitted access to customer information through its provision of services for the licensee.

### **Section 421.2 Information security program.**

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.

### **Section 421.3 Objectives of information security program.**

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 such information; and
- (c) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

## **DEVELOPMENT AND IMPLEMENTATION OF INFORMATION SECURITY PROGRAM**

### **Section 421.4 Examples of methods of development and implementation.**

The actions and procedures described in Sections 421.5 through 421.8 of this Part are examples of methods of implementation of the requirements of Sections 421.2 and 421.3 of this Part. Such examples are non-exclusive illustrations of actions and procedures that licensees may follow to implement Sections 421.2 and 421.3 of this Part.

### **Section 421.5 Assess risk.**

The licensee:

- (a) Identifies reasonably foreseeable internal or external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems;

(b) Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information; and

(c) Assesses the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.

**Section 421.6 Manage and control risk.**

The licensee:

(a) Designs 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) Trains staff, as appropriate, to implement the licensee's information security program; and

(c) Regularly tests the key controls, systems and procedures of the information security program. The frequency and nature of such tests are determined by the licensee's risk assessment.

**Section 421.7 Oversee service provider arrangements.**

The licensee:

(a) Exercises appropriate due diligence in selecting its service providers; and

(b) Requires its service providers to implement appropriate measures designed to meet the objectives of this Part, and, where indicated by the licensee's risk assessment, takes appropriate steps to confirm that its service providers have satisfied such obligations.

**Section 421.8 Adjust the program.**

The licensee monitors, evaluates, and adjusts, 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.

**ADDITIONAL PROVISIONS****Section 421.9 Determined violation.**

A contravention of Section 421.2, Section 421.3, or Section 421.10 of this Part shall be deemed to be an unfair method of competition or an unfair or deceptive act and practice in the conduct of the business of insurance in this state, and shall be deemed to be a trade practice constituting a determined violation, as defined in Section 2402(c) of the Insurance Law, in violation of Section 2403 of such law.

**Section 421.10 Compliance date.**

Each licensee shall establish policies and systems and implement an information security program pursuant to this Part by June 1, 2002.

I Gregory V. Serio, Superintendent of Insurance, do hereby certify that the foregoing is the First Amendment to 11 NYCRR 421 (Regulation 173) promulgated by me on February 7, 2002 pursuant to the authority granted by granted by Sections 201 and 301 and Article 24 of the Insurance Law, and in accordance with the provisions of 15 U.S.C. 6801, 6805(a)(6), 6805(b), 6805(c) and 6807 and 15 U.S.C. Chapter 94, to take effect upon publication in the State Register.

Pursuant to the provisions of the State Administrative Procedure Act, prior notice of the proposed amendment was published in the State Register on November 21, 2001. No other publication or prior notice is required by statute.

---

Gregory V. Serio  
Superintendent of Insurance

February 7, 2002