Insurance Data Security Act

Information Security Program Checklist for Agents (8-18-20)

What is An Information Security Program (§ 38.2-623 of the Code)?

A. Commensurate with

- the size and complexity of the licensee;
- the nature and scope of the licensee's activities, including its use of third-party service providers; and
- the sensitivity of the nonpublic information used by the licensee or in the licensee's possession, custody, or control,
- each licensee shall develop, implement, and maintain a comprehensive written information security program that:

☐ is based on the licensee's assessment of the licensee's risk, and

☐ contains administrative, technical, and physical safeguards for the protection of

☐ nonpublic information and

☐ the licensee's information system.

B. Each licensee's information security program shall be designed to:

☐ Protect the security and confidentiality of nonpublic information and the security of the information system;

☐ Protect against any reasonably foreseeable threats or hazards to the security or integrity of nonpublic information and the information system;

☐ Protect against unauthorized access to or use of nonpublic information, and minimize the likelihood of harm to any consumer; and

☐ Define and periodically reevaluate a schedule for retention of nonpublic information and a mechanism for its destruction.

Basic Requirements for an Information Security Program

Each licensee shall:

☐ Designate someone to oversee their information security. This can be one or more employees, an affiliate, or an outside vendor who is responsible for the information security program.

☐ Control who sees and can access sensitive information. Do they have passwords and door locks? Locks on cabinets and drawers? Do you restrict areas of your offices? Do you immediately revoke access for all terminated employees?

☐ At physical locations containing nonpublic information, restrict access to nonpublic information to authorized persons only. Do you have locks on file cabinets and controls on

access to keys? Do you restrict access to paper files on/in desks? Do you have secure locks on doors?

- ☐ Protect against environmental hazards. Do you have a fire extinguisher or sprinkler system? Are files, boxes, and other physical media left on the floor or out in the open? Is the office clean? Are there any other issues that may result in damage from rain, fire, or other environmental impacts?

- ☐ Dispose of nonpublic information securely regardless of the format (i.e., paper and electronic). Examples: Do you have a record retention policy that is rigorously enforced? Do you regular purge of out of date files and information on former and current customers? Do you have a cross-cut shredder of a shredding vendor? Do you utilize the municipal waste management services? All waste management services in Virginia have processes for disposal of sensitive information.

- ☐ Stay informed regarding emerging threats or vulnerabilities.

- ☐ Send information securely over the internet. Do you use an encryption when you send files over the internet? That can be as simple as using WinZip.

- ☐ Train your employees on cybersecurity. Do you use a cybersecurity awareness training service?

- ☐ Design the information security program to mitigate any unique risks to your organization. That may include, but isn't limited to, risks associated with specialized technology, personnel, or unique client needs. This may require a risk assessment conducted by an outside professional.

Written Incidence Response Plan Required

A. As part of its information security program, each licensee shall establish a written incident response plan designed to promptly respond to, and recover from, any cybersecurity event:

   - ☐ Do you have a written incidence response plan?

B. Does your incident response plan address the following?

   - ☐ The internal process for responding to a cybersecurity event, including a point of contact for all third-party service providers you use;

   - ☐ The goals of the incident response plan;

   - ☐ The definition of clear roles, responsibilities, and levels of decision-making authority;

   - ☐ External and internal communications and information sharing;

   - ☐ Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;

   - ☐ Documentation and reporting regarding cybersecurity events and related incident response activities; and

- ☐ The evaluation and revision, as necessary, of the incident response plan following a cybersecurity event.

Update the Information Security Program as Needed

Each licensee shall monitor, evaluate, and adjust, as appropriate, the information security program consistent with

- any relevant changes in technology,
- the sensitivity of its nonpublic information,
- internal or external threats to information, and
- your own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems.
  - ☐ Do you have a written process for updating your information security program?
  - ☐ Have you updated your information security program in response to changes in its business?

Duties if the Licensee Has a Board of Directors

If you have a board of directors, the board or an appropriate committee of the board shall, at a minimum,

- ☐ Require your information executive management or its delegates to develop, implement, and maintain the licensee's information security program, and
- ☐ Report in writing:
  - ☐ The overall status of the information security program,
  - ☐ Your compliance with this law, and
  - ☐ Material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, third-party service provider arrangements, results of testing, cybersecurity events or violations and management's responses thereto, and recommendations for changes in the information security program.
- ☐ If executive management delegates any of its responsibilities under this section, it shall oversee the development, implementation, and maintenance of your information security program prepared by the delegate and shall receive a report from the delegate complying with the requirements above.

Use of Third-Party Service Providers (Effective July 1, 2022)

if you use a third-party service provider, you shall:

- ☐ Exercise due diligence in selecting your third-party service provider; and
- ☐ Require the third-party service provider to implement appropriate administrative, technical, and physical measures to protect and secure the information systems and nonpublic information that are accessible to, or held by, the third-party service provider.

Other Duties with respect to a Cybersecurity Event

A. Duty to Investigate a Suspected Cybersecurity Event

The requirements for investigating a suspected cybersecurity event is set forth in § 38.2-624 of the Code.

B. Duty to Report Cybersecurity Events to the Commissioner of Insurance and Provide Notice to Consumers

The duty to report cybersecurity events to the Commissioner and to notify consumers is set forth in §§ 38.2-325 and 38.2-626, respectively.

C. Insurer Duty to Notify Producer-Cybersecurity Event Involving Producer's Customer

§ 38.2-625 G:

- ☐ If there is a cybersecurity event involving nonpublic information that is in the possession, custody, or control of a licensee that is an insurer or its third-party service provider and for which a consumer accessed the insurer's services through an independent insurance producer, the insurer shall notify the producers of record of all affected consumers as soon as practicable as directed by the Commissioner. The insurer is excused from this obligation for those instances in which it does not have the current producer of record information for any individual consumer.

Exemptions Applicable to Agents and Agencies

§ 38.2-629:

A licensee subject to HIPAA that has established and maintains an information security program pursuant to such statutes, rules, regulations, or procedures established thereunder shall be considered to meet the requirements of § 38.2-623 (information security program), provided that licensee is compliant with, and submits a written statement certifying its compliance with, the same, and certifies that it will protect nonpublic information not subject to HIPAA in the same manner it protects information that is subject to HIPAA.

Any such licensee that investigates a cybersecurity event and notifies consumers in accordance with HIPAA and any HIPAA-established rules, regulations, or procedures shall be considered compliant with the requirements of §§ 38.2-624 (duty to investigate) and 38.2-626 (notice to consumers).

An employee, agent, representative or designee of a licensee, who is also a licensee, is exempt from §§ 38.2-623 (information security program), 38.2-624 (duty to investigate), 38.2-625 (notice to the Commissioner), and 38.2-626 (notice to consumers) and need not develop its own information security program or conduct an investigation of or provide notices *to the Commissioner and consumers relating to a cybersecurity event, to the extent that the employee, agent, representative, or designee is covered by the information security program, investigation, and notification obligations of the other licensee.*

A licensee affiliated with a depository institution that maintains an information security program in compliance with the Interagency Guidelines Establishing Standards for Safeguarding Customer Information (Interagency Guidelines) as set forth pursuant to §§ 501 and 505 of the federal Gramm-Leach-Bliley Act, P.L. 106-102, shall be considered to meet the requirements of § 38.2-623 (information security program) and any rules, regulations, or procedures established thereunder, provided that the licensee produces, upon request, documentation satisfactory to the Commissioner that independently validates the affiliated depository institution's adoption of an information security program that satisfies the Interagency Guidelines.