The State of New Hampshire
Insurance Department
21 South Fruit Street, Suite 14
Concord, NH 03301
(603) 271-2261 Fax (603) 271-1406
TDD Access: Relay NH 1-800-735-2964

Commissioner

Alexander K. Feldvebel
Deputy Commissioner

Bulletin

Docket No: INS 20-001-AB

To: All persons conducting insurance business in New Hampshire

From: Alex Feldvebel, Acting Commissioner AF

Date: January 2, 2020

Re: Chapter 420-P Insurance Data Security Law

During its 2019 session, the legislature enacted a new chapter, RSA 420-P, relating to insurance data security. RSA 420-P becomes effective January 1, 2020.

Reporting Requirements: Effective **January 1, 2020**, licensees (unless excepted) must notify the Commissioner that a cybersecurity event has occurred within three (3) days, pursuant to RSA 420-P:6, if:

1) New Hampshire is the licensee's domicile or home state and the cybersecurity event has a reasonable likelihood of materially harming a consumer residing in New Hampshire or there is a reasonable likelihood of materially harming any material part of the normal operations of the licensee; or

2) The licensee reasonably believes that the cybersecurity event involves nonpublic information of 250 or more consumers residing in New Hampshire and the event (a) impacts the licensee; (b) has a reasonable likelihood of materially harming any NH consumer; or (c) has a reasonable likelihood of materially harming any material part of the licensee's normal operations.

A "cybersecurity event" is defined as "an event resulting in unauthorized access to, disruption or misuse of, an information system or nonpublic information stored on such information system.

The term shall not include the unauthorized acquisition of encrypted nonpublic information if the encryption, process, or key is not also acquired, released, or used without authorization." RSA 420-P:3(IV).

Reporting Cybersecurity Events to the Department: An online form is available to make a cybersecurity event notification. The form can be found on the Department's website at https://www.nh.gov/insurance/legal/cybersecurity.htm. The person making the report for a licensee will be required to set up a username and password prior to accessing the form. The Department recognizes that all pertinent information may not be known at the time of the initial report. The licensee should make a good faith effort to provide as much information as possible in the initial report. After submitting the initial report, the person making the report will be able to login and provide updated information to the form as it becomes known to the licensee.

Information Security Program: Licensees (unless excepted) must develop, implement, and maintain a comprehensive written information security program that complies with the requirements of RSA 420-P:4. Licensees will have until **January 1, 2021**, to implement a security program that is compliant with RSA 420-P:4.

Certification: Beginning **March 1, 2021**, all licensees domiciled in New Hampshire must submit a written statement to the Commissioner certifying that the licensee is in compliance with the requirements of RSA 420-P:4 unless a licensee falls within an exception, pursuant to RSA 420-P:9, or a safe harbor provision, pursuant to RSA 420-P:10 or RSA 420:P:11. Any licensee that (1) establishes and maintains an information security program that is compliant with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and by Parts 160 and 164 of Title 45 of the Code of Federal Regulations for protected health information and maintains other nonpublic consumer information in the same manner, or (2) establishes and maintains an information security program that is compliant with N.Y. Comp. Codes R. & Regs. Title 23, section 500 must submit a written statement to the Department certifying compliance with either RSA 420-P:10 or RSA 420-P:11. Additional guidance regarding how to file certifications will be provided in a subsequent bulletin.

Third-party Service Providers: Licensees will have until **January 1, 2022**, to require any third-party service providers to implement appropriate administrative, technical, and physical measures to protect and secure the information systems and nonpublic information.