New Hampshire Enacts New Insurance Data Security Law

Alysa Z. Hutnik

August 14, 2019

Effective January 1, 2020, New Hampshire's new Insurance Data Security Law will impose certain information security requirements on entities that (1) are licensed under the state's insurance laws and (2) handle "nonpublic information." "Nonpublic information" is defined as information that is not publicly available and falls into one of the two following categories:

1. Information that because of name, number, personal mark, or other identifier could identify a consumer when combined with the consumer's Social Security number, driver's license number, financial account number, credit or debit card number, security code or PIN that would permit access to the consumer's financial account, or biometric records.

2. Information or data, except age or gender, that can be used to identify a particular consumer and that relates to the past, present, or future physical, mental, or behavioral health or condition of any consumer or a member of the consumer's family; the provision of health care to any consumer; or payment for the provision of health care to any consumer.

The law will require that licensees:

- **Conduct a Risk Assessment:** Conduct risk assessments that identify and mitigate "reasonably foreseeable" internal or external threats to the business and its nonpublic information, including nonpublic information accessible to or held by third-party service providers.

- **Implement an Information Security Program:** Use the results of the risk assessment to create an information security program. The program must be managed by the board and detail the licensee's plan for responding to cybersecurity events (an event "resulting in the unauthorized access to, disruption or misuse of, an information system or nonpublic information stored" on an information system).

- **Respond to Cybersecurity Events:** Conduct a "prompt investigation" of all cybersecurity events and, in most circumstances, notify the Insurance Commissioner, within three business days, of any cybersecurity event that has a "reasonable likelihood" of materially harming a New Hampshire consumer or any material part of the licensee's normal business operations. This notice must include specific information, including a copy of the licensee's privacy policy.

The law includes a limited safe harbor for companies that are in compliance with HIPAA if the licensees have established and maintained HIPAA-required privacy, security, and data breach notification programs and procedures to protect both "protected health information," as defined by HIPAA, and any other nonpublic information. The companies must submit written statements indicating that they (1) are HIPAA-compliant; and (2) protect any other nonpublic information in the

same way that they do protected health information. These companies are still required to comply with the Insurance Data Security Law’s cybersecurity event notification requirements.

The law provides for additional limited exemptions for companies complying with other laws, including the New York Cybersecurity Regulation.

Licensees have one year from the effective date to comply with the risk assessment and information security program requirements, and two years from the effective date to ensure that third-party service providers are implementing appropriate security measures.

We recommend that companies take steps now to assess the applicability of the statute and determine how to best integrate its requirements into existing business practices.