NORTH DAKOTA
Insurance & Securities

BULLETIN 2025-1

TO: Insurance Companies, Producers

FROM: Jon Godfread, Commissioner

DATE: July 31, 2025

SUBJECT: Insurance Data, Security and Event Reporting **Amending and Supplementing Bulletin 2021-4**

During the 67th Legislative Assembly, the North Dakota Legislature enacted Senate Bill 2075, establishing new requirements for insurance data security. This bulletin serves to inform and guide licensees on the obligations outlined in Senate Bill 2075, codified as **North Dakota Century Code (NDCC) Chapter 26.1-02.2**, and updated by **Senate Bill 2088** during the 69th Legislative Assembly.

The Department emphasizes the critical importance of cybersecurity in the insurance industry, which manages significant amounts of sensitive personal data. Recent increases in ransomware and cyberattacks across industries underscore the financial, reputational, and regulatory risks of inadequate or absent information security programs.

Applicability

All individuals and entities required to be licensed by the North Dakota Insurance Department, including insurance companies, producers and agencies, third-party administrators (TPAs), managing general agents (MGAs), and other licensed organizations—are subject to the requirements of NDCC 26.1-02.2.

Effective Dates

- **Initial Implementation:** August 1, 2021
- **Revisions under Senate Bill 2088:** Effective August 1, 2025

I. Development and Implementation of an Information Security Program

NDCC 26.1-02.2 requires each licensee to conduct a self-assessment and implement a written **Information Security Program (ISP)** that is commensurate with the licensee's

600 E Boulevard Ave
Bismarck, ND 58505-0500

phone: (701)328-2440 | fax: (701)328-4880
insurance.nd.gov | securities.nd.gov

Jon Godfread, Commissioner

size, complexity, and the nature and scope of its activities.

Minimum requirements include:

- Designating one or more employees to oversee the ISP.
- Identifying reasonably foreseeable threats that could lead to a cybersecurity event.
- Assessing the likelihood and potential impact of these threats.
- Reviewing the sufficiency of existing policies, procedures, information systems, and other safeguards.
- Implementing appropriate controls to manage identified threats.

Licensees must also:

- Regularly monitor and update their ISP to adapt to technological changes and new cybersecurity threats.
- Exercise due diligence in selecting third-party service providers, ensuring those providers maintain cybersecurity programs consistent with NDCC 26.1-02.2.

Small Licensee Exception:
Effective August 1, 2025, licensees with less than **$5 million in gross annual revenue** or less than **$10 million in total assets** are still required to implement an ISP but may tailor the program to the scale and complexity of their operations.

II. Cybersecurity Event Investigation

Effective August 1, 2021, licensees must investigate any potential **cybersecurity event** without undue delay. A licensee may retain outside vendors or service providers to assist with the investigation.
At a minimum, the investigation must determine:

- Whether a cybersecurity event has occurred.
- The nature and scope of the event.
- The types of nonpublic information potentially affected.
- Actions taken to restore the security of affected systems.

Licensees must maintain records of all cybersecurity events for **at least five (5) years**.

III. Notification Requirements

Beginning **August 1, 2025**, licensees must notify the North Dakota Insurance Commissioner within **three (3) business days** of determining that a cybersecurity event has occurred that meets one of the following thresholds:

- **Primary Domicile Trigger:**
  North Dakota is the licensee's state of domicile, and notice is required to any resident under **NDCC Chapter 51-30**.
- **Multi-Consumer Trigger:**
  The event involves nonpublic information of **250 or more North Dakota consumers** *and* requires notice to another governmental, regulatory, or self-regulatory agency under state or federal law.

Notification must include:

- Date and discovery details of the cybersecurity event.
- Description of how the data was exposed, lost, stolen, or breached.
- Whether the affected information has been recovered.
- Identity of the source of the breach (if known).
- Law enforcement and regulatory bodies notified.
- Specific types of information involved.
- Duration of system compromise.
- Number of affected North Dakota consumers.
- Internal review findings (e.g., failed procedures or controls).
- Remediation steps underway.
- Copy of the licensee's privacy policy and planned consumer notifications.
- Contact information for an individual with knowledge of the event who is authorized to act on the licensee's behalf.

Submit Report Here: Cyber Breach Notification Form

NDCC 26.1-02.2 incorporates consumer notification standards from **NDCC Chapter 51-30**, available at: https://www.legis.nd.gov/cencode/t51c30.pdf

IV. HIPAA Exception

Licensees subject to the **Health Insurance Portability and Accountability Act (HIPAA)** *may* be exempt from certain requirements of NDCC 26.1-02.2. However, **HIPAA-covered licensees are not exempt** from the **notification requirements** to the Insurance Commissioner as outlined in **NDCC 26.1-02.2-05**.

Contact Information

For questions or additional guidance regarding compliance with NDCC 26.1-02.2, please contact the North Dakota Insurance & Securities Department at Contact Us | North Dakota Insurance Department.

This Bulletin is in effect until rescinded by the North Dakota Insurance Commissioner.