Illinois Department of Insurance

JB PRITZKER
Governor

DANA POPISH SEVERINGHAUS
Director

TO: All Regulated Entities
FROM: Dana Popish Severinghaus, Director of Insurance dps
DATE: March 1, 2024
RE: Company Bulletin 2024-05 - Change Healthcare Cybersecurity Event

---

The Illinois Department of Insurance ("Department") continues to monitor the recent cybersecurity incident which occurred February 21, 2024, to Change Healthcare and its impact on health systems in Illinois and across the nation. The Department will be vigilant in enforcing The Illinois Insurance Data Security Law (215 ILCS 215/et Al), effective January 1, 2024.

The Department reminds all licensees, including a licensee's use of third-party services, of their statutory obligations to notify the Department of all cybersecurity events by submitting notice by email to DOI.DataSecurity@illinois.gov within three (3) business days after a determination a cybersecurity event has occurred. Such notification must meet as many of the data requirements of 215 ILCS 215/20 as possible and the impacted licensee has a continuing obligation to update the Department regarding material changes to previously provided or new information.

Issuers are encouraged to make the necessary accommodations to minimize the impact to covered individuals and their access to care. This may include updates to websites and development of public-facing materials that communicate how insureds can obtain assistance accessing their benefits affected by the incident. Additionally, issuers should implement alternative business processes, including but not limited to, the continued submissions of claims and payment to providers.

Initial Notification of Cybersecurity Event to Department

Initial notification of a cybersecurity event to the Department shall include as much of the following information as possible:

1. the date of the cybersecurity event;

2. a description of how the information was exposed, lost, stolen, or breached, including the specific roles and responsibilities of third-party service providers, if any;

3. how the cybersecurity event was discovered;

4. whether any lost, stolen, or breached information has been recovered and if so, how it was

recovered;

5. the identity of the source of the cybersecurity event;

6. whether the company has filed a police report or has notified any regulatory, government, or law enforcement agencies and, if so, when such notification was provided;

7. a description of the specific types of information acquired without authorization, including types of medical information, types of financial information, or types of information allowing identification of the consumer;

8. the period during which the information system was compromised;

9. the number of total Illinois consumers affected by the cybersecurity event (best estimate). Update this estimate with each subsequent report to the Director;

10. the results of any internal review identifying a lapse in either automated controls or internal procedures, or confirming that all automated controls or internal procedures were followed;

11. a description of efforts being undertaken to remediate the situation which permitted the cybersecurity event to occur;

12. a copy of the company's privacy policy and a statement outlining the steps the company will take to investigate and notify consumers affected by the cybersecurity event; and

13. the name of a contact person who is both familiar with the cybersecurity event and authorized to act for the company.

Companies and related licensees must conduct their cybersecurity investigation in accordance with Section 15 of the Insurance Data Security Law. 215 ILCS 215/15. This notification requirement is in addition to all reporting requirements under the Illinois Personal Information Protection Act which includes additional notifications to the Illinois Attorney General and individual consumers. 815 ILCS 530/1 et seq.

As this cybersecurity event has nationwide impact, the Department remains in communication with its regulatory partners in other states to assess next steps in relation to this breach. Depending on whether a multi-state response is contemplated, the Department may issue subsequent communications to regulated entities to further evaluate the scope of impact of the breach.

Questions about this bulletin may be directed to DOI.DataSecurity@illinois.gov.