Wisconsin Office of the COMMISSIONER OF INSURANCE

Tony Evers, Governor of Wisconsin
Nathan Houdek, Commissioner of Insurance

DATE: March 14, 2024

TO: Health Insurers, Pharmacy Benefit Managers, and Interested Parties

FROM: Nathan Houdek, Commissioner of Insurance

SUBJECT: Change Healthcare Cyber Attack Impacts and Response

The Office of the Commissioner of Insurance (OCI) has been monitoring the impact of the February 21, 2024, cybersecurity attack on Change Healthcare. We recognize that this cyber disruption has created significant operational challenges that may continue in the weeks to come as Change Healthcare works to restore all their software functions for payers and providers. Updates on Change Healthcare's efforts can be found here.

OCI directs each health insurer and pharmacy benefit manager (PBM) operating in Wisconsin that has been impacted by this cyber disruption to provide prompt assistance to consumers and health care providers to limit interruptions to access of health care services and prescriptions.

Claims Reimbursement
Wisconsin health insurers and PBMs with impacted in-network providers should consider adjusting claim reimbursement processes during this time so health care access is not disrupted. OCI encourages insurers to consider:

- Processes for an in-network provider to obtain advance reimbursement from the insurer during periods where claims, billing, and reimbursement processes are unavailable or delayed due to previous unavailability.
- Additional flexibility in financial arrangements for in-network providers so they may continue to provide services while claims processing and reimbursement is delayed.

Out-of-network Pharmacy Benefit Claims
Due to the Change Healthcare outage, many consumers may need to travel to different pharmacies to find a provider who is equipped to dispense their prescription. OCI encourages health insurers and PBMs to waive penalties on pharmaceutical claims when a consumer obtains their prescription from an out-of-network pharmacy between February 21 and April 21, 2024.

Data Security Law
Health insurers and PBMs licensed in Wisconsin are reminded to remain in compliance with the data security requirements outlined in Wis. Stat. § 601.95. OCI requires licensees to maintain an information security program, take certain steps to promptly investigate cybersecurity events, and notify OCI and consumers when a cybersecurity breach has occurred.

The law defines "Cybersecurity event" as "an event resulting in the unauthorized access to, or disruption or misuse of, an information system or the nonpublic information stored on an information system."

Under Wis. Stat. § 601.953(1) if a licensee learns that a cybersecurity event involving its information systems has occurred, the licensee must conduct a prompt investigation that, at a minimum, includes the following:

- An assessment of the nature and the scope of the event;
- Identification of any nonpublic information that may have been involved; and
- The performance of reasonable measures to restore security.

If a licensee knows that a cybersecurity event has occurred in the information systems maintained by a third party, the licensee must make reasonable efforts to confirm the third-party provider conducted an investigation consistent with this section or document the third-party provider's failure to cooperate under Wis. Stat. § 601.953(2).

Notification of a cybersecurity event must be provided to OCI when there is a reasonable likelihood of material harm to consumers, or the event involves the nonpublic information of at least 250 consumers. Notification must be provided as promptly as possible but no later than three business days after the determination that a cybersecurity event involving nonpublic information has occurred.

Review the requirements of Wisconsin's data security law here to ensure compliance.

Any questions concerning this bulletin may be directed to OCICyberReport@wisconsin.gov.