Customer Cybersecurity Information Center

AUGUST 29, 2026

McKesson Cybersecurity Incident Investigation and Response Update

Dear Customer,

McKesson continues to serve customers across all our lines of business and accept orders. Our distribution centers remain operational, and we continue to ship products across our distribution network.

Based on our investigation thus far, including assessments by leading cybersecurity industry experts supporting our response, we've confirmed that the unauthorized access to certain third-party applications and the exfiltration of certain data was associated with a subset of customers within our Oncology & Multispecialty and Medical-Surgical business units.

We have reasonable assurance of no ongoing unauthorized activity in our systems. Customers can continue to connect to and use our systems and services as intended.

We continue to monitor our environment closely and take measures to support the security and reliability of our operations.

In terms of next steps:

- Our investigation remains ongoing and we continue to fully ascertain the scope of information that may have been accessed or acquired.
- We will continue to provide updates as additional information becomes available. Any updates about the nature and scope of this incident will come from our team at McKesson and be posted on McKesson.com/cybersecurity.
- We also expect to provide complimentary credit monitoring and identity protection services, as well as a dedicated information line to answer questions and provide support to partners, customers and their patients whose data was exfiltrated.

We take the security and privacy of our partners, customers and their patients very seriously. We appreciate your patience and partnership as our investigation continues.

Respectfully,

Francisco Fraga

Executive Vice President, Chief Information Officer and Chief Technology Officer

---

AUGUST 28, 2026

Cybersecurity Incident Investigation Underway

Dear Customer,

McKesson is in the early stages of investigating a cybersecurity incident involving third-party applications and unauthorized access and exfiltration of data.

We take the security and privacy of our partners, customers and their patients very seriously. Upon discovery, we immediately activated our incident response protocols, launched an investigation, and engaged leading cybersecurity industry experts to assist in our response.

Our investigation remains ongoing, and we are working to fully ascertain the nature and scope of the incident so that we can provide accurate and concrete information as it becomes available.

Our cybersecurity team and leading cybersecurity industry experts are working to minimize the impact on system availability and business operations. At this time, customers may experience intermittent service degradation that we believe may be related to this incident. We are aware of these issues and continue to monitor the situation closely.

Based on the information currently available, we do not believe any action is required by our customers and we are not proactively disconnecting systems within our environment at this time. If you encounter technical issues with our services, please contact us through your normal support channels.

We understand you have questions regarding this incident. Our team is focused on developing a more complete understanding of the situation. We remain committed to keeping you informed and will continue to

provide updates.

We appreciate your patience and partnership as our investigation continues.

Respectfully,

Francisco Fraga

Executive Vice President, Chief Information Officer and Chief Technology Officer