HALL

Hall Attorneys
A Professional Corporation
www.hallattorneys.com

FOR IMMEDIATE RELEASE

Hall Attorneys and Co-Counsel File Class Action Following McKesson Healthcare Data Breach

McKesson says exfiltrated data was associated with a subset of customers in its Oncology & Multispecialty and Medical-Surgical units; a threat actor claims approximately one terabyte and 284 million raw patient-related records.

Filed complaint: www.hallattorneys.com/dockets/mckesson

DALLAS, Texas - September 1, 2026 - Hall Attorneys, P.C. and co-counsel filed a putative class action on August 31, 2026 against McKesson Corporation and CoverMyMeds LLC in the U.S. District Court for the Northern District of Texas, Dallas Division. The matter is Hall v. McKesson Corporation et al., No. 3:26-cv-02958-D, ECF No. 1.

The complaint arises from the August 2026 cybersecurity incident McKesson says involved unauthorized access to third-party applications and data exfiltration. It alleges the defendants failed to reasonably safeguard personally identifiable information and protected health information.

McKesson identifies two affected business units

In an August 29 customer update, McKesson said its investigation confirmed that unauthorized access to certain third-party applications and the exfiltration of certain data was associated with a subset of customers within its Oncology & Multispecialty and Medical-Surgical business units.

McKesson said it had reasonable assurance there was no ongoing unauthorized activity, but that its investigation remained open and it was still determining the nature and scope of the information involved. The company said it expects to provide complimentary credit monitoring and identity-protection services, together with a dedicated information line, to partners, customers, and their patients whose data was exfiltrated.

McKesson has not publicly named every affected customer or application, identified all data elements involved, or announced a final number of affected people. A customer relationship alone therefore does not establish that a facility or any particular patient was affected.

The alleged scale and sensitivity of the data

The complaint discusses reporting that ShinyHunters claimed it removed approximately one terabyte of data over four days and obtained approximately 284 million raw patient-related records or database rows. The group reportedly said those rows do not represent 284 million unique patients and that it had not completed a unique-person count.

The actor reportedly claims the data includes combinations of:

- Identity and contact: names, addresses, dates of birth, Social Security numbers, telephone numbers, and email addresses.
- Patient and benefit identifiers: patient identifiers, Medicaid numbers, and medical-record numbers.
- Clinical and treatment information: medications, prescriptions, allergies, illnesses, disabilities, appointments, and physician information.
- Care and logistics: medication shipments, invoices, and information about healthcare providers and clinics.

McKesson has not confirmed the threat actor's volume or asserted data fields. If confirmed, the reported data would be exceptionally sensitive because it could connect a patient's identity and government or benefit identifiers to detailed information about treatment, medical conditions, and care providers.

Who should check with a healthcare provider?

Patients may want to make an inquiry if they received care from a facility that may be a customer of either identified business unit. McKesson says its Oncology & Multispecialty operations support health systems, independent community practices, specialty pharmacies, and specialty practices, including oncology and other complex-care providers.

McKesson says its Medical-Surgical operations serve physician offices, health systems, laboratories, ambulatory surgery centers, urgent-care and community clinics, oncology clinics, home-health and hospice agencies, home-infusion pharmacies, skilled-nursing facilities, assisted-living facilities, and other long-term-care settings.

Receiving care at one of these facilities does not establish that the facility used McKesson. A McKesson customer relationship does not establish that the customer was within the affected subset or that any particular patient's data was exfiltrated. A supply relationship by itself also does not show that patient data was present in an affected application.

How to verify whether your provider used the impacted lines

- Contact the privacy office: ask for the HIPAA privacy officer, compliance office, health information management or medical-records department, patient relations office, or facility administrator. Front-desk and clinical staff may not know the organization's vendors.
- Ask a two-part question in writing: Was the facility a customer of McKesson's Oncology & Multispecialty or Medical-Surgical business unit? Did McKesson identify the facility, any application it used, or any associated patient data as part of the August 2026 incident?
- Ask about your own data: if the provider confirms it was among the affected customers, ask whether your information was stored in or transmitted through an affected third-party application, what categories were involved, and when written notice will issue.
- Check for clues, not proof: search the provider's website, privacy notices, patient portal, bills, infusion paperwork, home-care or supply records, and shipment labels for McKesson, McKesson Medical-Surgical, The US Oncology Network, Ontada, or iKnowMed. Those names may justify a follow-up question but do not prove impact.
- Request and preserve the response: keep the contact's name and title, the date, the exact question, and any written answer. If the provider is waiting for McKesson's determination, ask which office will issue patient notices and how to update your contact information.

The filed case

The complaint proposes a Nationwide Class, an Iowa Subclass, and a McKesson Pharmacy-Technology Subclass. It asserts negligence, breach of implied contract, and unjust enrichment.

Requested relief includes damages and restitution; remediation of proven security deficiencies; stronger identity and access controls; appropriate independent security assessment; data minimization and protection; improved monitoring and data-loss prevention; and meaningful identity and medical-identity protection services.

Information for patients and caregivers

Patients and caregivers may contact Hall Attorneys if a provider confirms it used one of the two McKesson business units and was within the affected subset, if they receive an incident notice, or if they experience healthcare-themed phishing, medical-identity misuse, prescription fraud, identity theft, expense, or substantial lost time.

PRESERVE RELEVANT RECORDS

Keep the complete incident notice; written questions to the provider and its answers; documents showing the provider's relationship to either identified McKesson business unit; suspicious messages; account, insurance, or benefit statements; fraud reports; monitoring records; receipts; and a dated log of time spent responding.

Privacy warning: In an initial message, do not send passwords, complete account numbers, Social Security numbers, medical records, or identification documents through ordinary email or a standard contact form.

Sources and important documents

McKesson August 29 update: mckesson.com/cybersecurity
Reported breach details: BleepingComputer
Case overview: hallattorneys.com/investigations/mckesson
Filed complaint: hallattorneys.com/dockets/mckesson

MEDIA AND CASE INQUIRIES
Nicholas Hall | Hall Attorneys, P.C.
nhall@hallattorneys.com | +1 713 428 8967
www.hallattorneys.com

Hall Attorneys is a Texas-based law firm focused on complex litigation. This release summarizes allegations in a filed complaint. The defendants have not yet had an opportunity to respond, no findings have been made, and no class has been certified. Sending information does not create an attorney-client relationship.