

Last Updated on September 29, 2026

Pavillon International Inc. was the victim of a data privacy incident that involved certain electronic health information of its current and former patients.

What Happened: On July 31, 2026, Pavillon was alerted to suspicious activity within its computer network. Upon receipt of the alerts, Pavillon took immediate action to secure its network and partnered with external cybersecurity specialists to investigate. As part of the investigation, Pavillon learned on August 7, 2026, that an unauthorized actor accessed portions of its network, and that some data was taken without authorization. Pavillon then undertook a comprehensive review of its servers to determine what sensitive information, if any, was accessible and to whom that information belonged. The review determined that information belonging to certain current and former patients and employees was present and accessible on the servers at the time of the incident.

What Information Was Involved: The information involved varied for each person but generally included personally identifiable information (“PII”) and protected health information (“PHI”) including name in combination with medical diagnostic and/or treatment information, health insurance information, and demographic information. At this time, we have no evidence of misuse of any PII or PHI for fraud or identity theft.

What We Are Doing: Upon learning of the incident, we took immediate steps to secure our network and partnered with professionals to conduct a thorough investigation which included a comprehensive review of our files for PII and PHI. We reported the event to federal law enforcement. Additionally, we are reviewing our existing controls and policies and procedures we have in place for additional ways to remain resilient against threats moving forward.

What You Can Do: As a general matter, it is best practice to remain vigilant for incidents of identity theft and fraud, from any source, by reviewing and monitoring your account statements, credit reports, and explanation of benefits (EOBs) for suspicious activity and errors. If you discover any suspicious or unusual activity on your accounts, promptly contact your financial institution or the service provider.

For More Information: If you have any questions or concerns, please contact our dedicated assistance line at (833) 516-8785, Monday through Friday, 8:00 a.m. – 8:00 p.m. EST, excluding major U.S. holidays.