Medidata Statement on Recently Disclosed Industry Security Vulnerabilities

October 30, 2026

Medidata is aware of several significant security vulnerabilities disclosed across the technology industry in recent weeks as a result of AI-accelerated vulnerability discovery. Protecting the confidentiality, integrity, and availability of our customers' data, including clinical trial data entrusted to us by sponsors and CROs, is our highest priority.

We are responding through the incident and risk management processes of our Information Security and Privacy Management System, which is aligned to ISO/IEC 27001:2022.

This includes the PHP (CVE-2026-109618 and CVE-2026-10961), Node.js (CVE-2026-111497) and several others coming from the Generative AI toolsets.

Our Unified Protection Group continuously monitors guidance from vendors, government agencies, and industry partners to ensure that we remain aligned with current rules and legislation.

Our Threat Intelligence Group monitors for specific technical vulnerabilities for all available sources, and this supports our strong security posture.

Customers with specific questions may contact their Medidata account representative or asksecurity@mdsol.com.

You can find details on our control regime, vulnerability scan data, copies of penetration tests, SOC 1 and 2 reports with privacy and security trust principles, certificates and statements of applicability for ISO 27001:2014, ISO 27018:2019 & ISO 27701:2019, and more at our Information Security portal, http://www.medidata.com/trust.