CASE STUDY

Medical Lab Enhances Cybersecurity Readiness and Compliance with Custom Assessment Plan

Organization Y — Healthcare / Medical Diagnostics Industry

Client Profile

Organization Y is a mid-sized medical laboratory providing diagnostic testing, specimen analysis, and reporting services to hospitals, physician networks, and individual patients. The lab processes a high volume of protected health information (PHI) daily, including patient records, test results, insurance data, and referring-physician communications, all while operating under strict regulatory obligations tied to patient privacy and data protection. As the lab expanded its testing capacity and adopted cloud-based laboratory information systems (LIS) and remote result-reporting tools, leadership recognized that cybersecurity and compliance readiness needed to keep pace with the organization's growth.

Business Challenge

Organization Y had implemented individual security tools over time, but lacked a unified view of how prepared the organization truly was to prevent, detect, and respond to a cyber incident. Leadership identified several areas of concern that were increasing both compliance exposure and operational risk. Chief among them was uncertainty around the lab's compliance posture relative to healthcare data protection requirements, coupled with limited visibility into where sensitive patient data resided and how it was protected across on-premises systems, cloud platforms, and third-party integrations.

The organization also lacked a documented, prioritized plan for closing identified security gaps, relying instead on ad hoc fixes driven by whichever issue surfaced most recently. Business continuity planning was similarly informal, leaving open questions about how quickly the lab could resume testing and reporting operations following a disruptive event such as ransomware or system outage. With growing scrutiny from healthcare partners and referring providers around vendor security, Organization Y needed a clear, evidence-based understanding of its risk profile and a practical path to strengthen it.

Solution — SentraGuarda Custom Cybersecurity Assessment Plan

Organization Y engaged SentraGuarda to design and deliver a custom Cybersecurity Readiness and Compliance Assessment tailored to the operational realities of a clinical laboratory. The engagement was structured around the following focus areas:

Compliance & Data Protection Assessment

- Evaluation of safeguards protecting patient data against applicable healthcare privacy and security requirements, including administrative, technical, and physical control review

Data Discovery & Risk Mapping

- Identification of where PHI resided across the laboratory information system, cloud platforms, and third-party vendor connections, with associated risk scoring

Security Controls & Infrastructure Review

- Assessment of endpoint protection, access management, network segmentation, and monitoring capabilities across lab and administrative environments

Business Continuity & Incident Readiness

- Review of backup and recovery capabilities, incident response planning, and the lab's ability to sustain testing operations during a disruption

Prioritized Remediation Roadmap

- A phased, risk-ranked action plan aligned to business impact, along with an executive summary translating technical findings into investment priorities

Results Delivered

Following the assessment, Organization Y gained a clear, documented understanding of its cybersecurity and compliance posture for the first time. Leadership obtained a consolidated risk picture showing exactly where patient data was exposed and which gaps posed the greatest compliance and operational risk. The prioritized roadmap allowed the lab to sequence remediation efforts by impact rather than urgency alone, making more efficient use of limited IT resources.

The engagement also strengthened the lab's business continuity posture, giving leadership greater confidence in its ability to maintain diagnostic operations through a disruptive event. Perhaps most valuably, Organization Y was able to demonstrate a credible, structured compliance and security program to referring providers and healthcare partners, reinforcing trust in the lab's handling of sensitive patient information.

Outcome

Through SentraGuarda's Custom Cybersecurity Assessment Plan, Organization Y moved from fragmented, reactive security practices to a structured, risk-informed program grounded in its actual compliance and operational needs. The engagement delivered improved visibility into patient data risk, a clear remediation path, stronger business continuity planning, and greater confidence among clinical partners—positioning the lab to protect patient data while continuing to scale its diagnostic services.
