Protecting patient data in 2026

The healthcare sector is facing a critical cybersecurity challenge in 2026, with insider threats and patient data vulnerabilities driving risk. Below are key insights from The State of Human Risk 2026 Report, highlighting the unique risks healthcare organizations face.

mimecast

HUMAN RISK IN HEALTHCARE

Insider-driven incidents threaten patient data

52% OF HEALTHCARE ORGANIZATIONS REPORT AN INCREASE IN MALICIOUS INSIDER THREATS, NEARLY MATCHING THE RISE IN INCIDENTS CAUSED BY NEGLIGENT EMPLOYEES (54%)

● underscoring why intent is no longer the right lens for managing insider risk.

A SINGLE INSIDER-DRIVEN DATA BREACH COSTS $14.5M ON AVERAGE

● emphasizing the need for proactive monitoring and protection.

Compliance and governance struggles

INSIDER-DRIVEN DATA LOSS

67%

of healthcare organizations worry about insider-driven data loss, and 59% lack confidence in their ability to quickly retrieve data for regulatory or legal requirements.

MANUAL PROCESSES DOMINATE

34%

rely on outdated compliance methods that cannot keep pace with growing volumes of sensitive patient data.

AI-driven threats add complexity

85%

of healthcare respondents are concerned about sensitive data leaks through generative AI tools.

49%

only 49% of organizations have implemented specific AI usage policies.

To mitigate these risks, healthcare organizations must:

- Integrate behavioral analytics to identify high-risk users.
- Automate compliance and data governance processes.
- Implement AI-powered tools for real-time threat detection.

mimecast

DOWNLOAD THE REPORT