Risk Assessment Report for enVisiAIn:

AI-Augmented Vision Technology in Healthcare

Douglass Brown

Security Policies and Procedures

The Evergreen State College

Professor Arlecia Tyus

May 26, 2026

Risk Assessment Report for enVisiAIn

Executive Summary

enVisiAIn is a fictitious health technology company that develops AI-augmented smart glasses, a mobile application, and a clinical dashboard for blind and low-vision users, elderly individuals, and rehabilitation clinics. The system helps users identify objects, read signs, detect hazards, recognize approved contacts, navigate physical spaces, and receive clinical or emergency support.

This report identifies, analyzes, prioritizes, and recommends treatment strategies for the company's major cybersecurity and privacy risks. The assessment focuses on patient safety, privacy, operational reliability, regulatory compliance, AI innovation, and secure partnerships. The highest-priority risks are unauthorized access to patient data, smart glasses firmware compromise, ransomware disruption, improper use of AI training data, third-party vendor breach, insecure remote access, cloud misconfiguration, and phishing or social engineering.

Organization Overview

enVisiAIn's product ecosystem includes smart glasses, a phone application, and a clinical dashboard. The glasses collect visual and biometric signals through cameras and sensors embedded in the frames. The phone application manages user settings, alerts, caregiver permissions, and support requests. The dashboard allows authorized rehabilitation clinics and support staff to monitor device performance and patient progress.

The company is both direct-to-consumer and business-to-business. Some users purchase the device and application directly, while clinics use the dashboard to support patient care.

enVisiAIn may process live camera feeds, retinal scans, biometric readings, voice commands, GPS location, medical history, insurance information, emergency contacts, clinician notes, and AI-generated recommendations. The company's design principle is to keep sensitive processing on device when feasible and send only minimized, anonymized, or de-identified data to the cloud when needed.

Methodology

This report uses a qualitative risk assessment method aligned with NIST Special Publication 800-30, Revision 1. NIST explains that risk assessments support leadership decisions by identifying threats, vulnerabilities, likelihood, impact, and possible responses (National Institute of Standards and Technology [NIST], 2012). The report also uses the NIST Cybersecurity Framework 2.0 because it frames cybersecurity risk through governance, identification, protection, detection, response, and recovery (NIST, 2024).

Likelihood is rated Low, Medium, or High. Impact is rated Low, Medium, High, or Critical. Critical risks may cause patient harm, a major data breach, regulatory exposure, ransomware disruption, or compromise of systems used for real-world navigation.

Key Assets

Asset	Description	Sensitivity
Patient and clinical data	Medical history, clinician notes, care plans	Critical
Biometric, video, and location data	Retinal scans, sensor data, live video, GPS routes	Critical
Smart glasses firmware	Device behavior, updates, and sensor control	Critical
Mobile app and dashboard	User controls, caregiver support, clinic workflows	High/Critical
AI models and cloud systems	Computer vision models, APIs, analytics, backups	High/Critical
Source code and vendor integrations	Build pipelines, hospitals, clinics, cloud providers	High

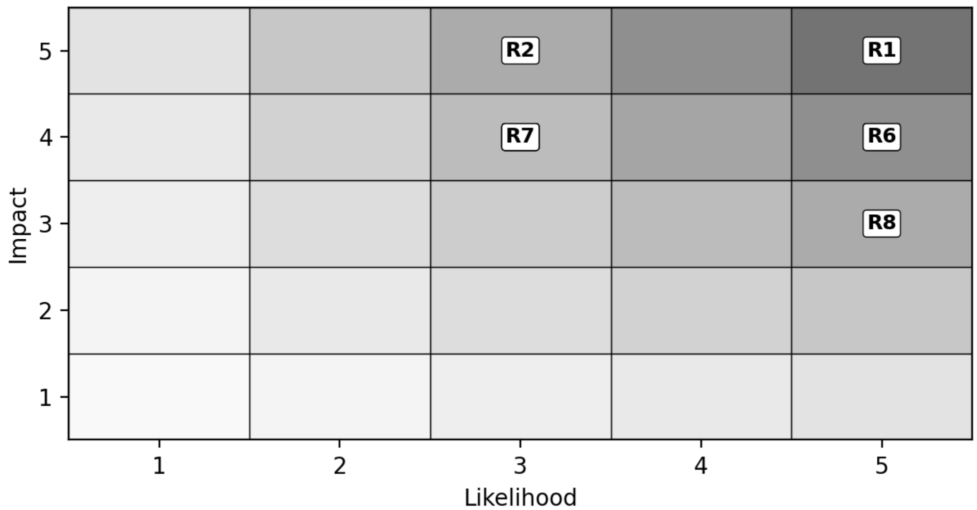
Risk Identification and Analysis

The risks below were selected because they connect directly to enVisiAIn's mission and business priorities. The company's most serious risks are those that could expose sensitive patient data, reduce trust, interrupt clinical support, or compromise systems used for safe navigation.

The highest-impact risk is unauthorized access to patient data because it could expose medical records, biometric data, video, and location information. Device compromise is also critical because the smart glasses support navigation and safety. Operational risks such as ransomware, cloud misconfiguration, insecure remote access, and vendor breach are prioritized as High because they can interrupt care, expose data, or damage trust. AI training data misuse is also High because enVisiAIn must innovate without violating consent, privacy, or patient expectations.

ID	Risk	Likelihood	Impact	Priority	Recommended Treatment
R1	Unauthorized access to patient data	High	Critical	Critical	Mitigate: MFA, RBAC, encryption, logs, access reviews
R2	Smart glasses firmware compromise	Medium	Critical	Critical	Mitigate: secure boot, signed updates, attestation, testing
R3	Ransomware disruption	High	High	High	Mitigate/Recover: EDR, segmentation, backups, playbooks
R4	Improper AI training data use	Medium	High	High	Mitigate: de-identification, consent, data lineage, review
R5	Third-party vendor breach	Medium	High	High	Mitigate/Transfer: vendor reviews, BAAs/DPAs, clauses
R6	Insecure remote access	High	High	High	Mitigate: zero-trust, managed devices, MFA, monitoring
R7	Cloud misconfiguration	Medium	High	High	Mitigate: CSPM, least privilege, encryption, testing
R8	Phishing and social engineering	High	Medium	Medium/High	Mitigate: phishing-resistant MFA, filtering, training

Figure 1. enVisiAIn Risk Heat Map



Recommended Treatment Strategies

The recommended strategy is defense in depth. enVisiAIn should not rely on one tool or department to manage risk. The company should combine administrative safeguards, technical safeguards, secure product design, privacy engineering, vendor governance, and incident response.

First, enVisiAIn should strengthen identity and access management through role-based access control, least privilege, multifactor authentication, privileged access management, conditional access, and quarterly access reviews. Clinical staff, customer support, engineers, executives, and vendors should have separate permission models.

Second, enVisiAIn should protect data through encryption, data minimization, and privacy-by-design practices. Patient-identifiable processing should remain on device when feasible. Cloud processing should use minimized, anonymized, or de-identified data unless identifiable data is specifically required for an approved business or clinical purpose.

Third, enVisiAIn should secure AI and software development. AI training should use approved datasets, data lineage tracking, and model risk review. The software development lifecycle should include secure coding standards, code review, dependency scanning, secrets scanning, static and dynamic testing, and vulnerability remediation deadlines. Firmware should be signed and updated only through trusted channels.

Fourth, enVisiAIn should improve resilience through an incident response plan, breach notification workflow, ransomware playbook, disaster recovery plan, and business continuity plan. Backups should be encrypted, immutable where possible, and tested regularly. Patient-facing systems and the clinical dashboard should have clear recovery time objectives.

Finally, vendors and remote users should be governed tightly. Vendor contracts should include security obligations, breach notification requirements, audit rights, and restrictions on unauthorized data use. Remote access should use managed devices, strong authentication, logging, and time-limited access for vendors.

Business Priority Alignment

The recommended strategies support enVisiAIn's business priorities. Protecting patient data supports privacy, compliance, and trust. Securing firmware supports patient safety and product reliability. Ransomware resilience protects clinical operations. AI governance supports innovation without sacrificing consent or privacy. Vendor management allows the company to work with clinics, hospitals, insurers, cloud providers, and research partners while reducing supply-chain exposure.

The highest priority is user trust. If users believe the smart glasses are unsafe, invasive, or vulnerable to hacking, the product will fail regardless of its technical sophistication. Security must therefore be treated as a product feature, a patient-safety requirement, and a business survival issue.

Conclusion

enVisiAIn's AI-augmented vision technology could improve independence and safety for blind and low-vision users, elderly individuals, and rehabilitation patients. However, the same technology creates serious cybersecurity and privacy responsibilities because the company handles medical records, biometric readings, retinal scans, video, GPS location, voice commands, clinical notes, and AI-generated recommendations.

The highest-priority risks are unauthorized access to patient data, smart glasses firmware compromise, ransomware disruption, improper AI training data use, third-party vendor breach, insecure remote access, cloud misconfiguration, and phishing. These risks should be addressed through defense in depth, strong governance, secure design, vendor oversight, AI risk management, and continuous risk assessment. For enVisiAIn, cybersecurity is part of patient care because protecting systems, devices, data, and access helps protect the people who depend on the company's technology to move through the world safely.

References

National Institute of Standards and Technology. (2012). Guide for conducting risk assessments (Special Publication 800-30, Revision 1). U.S. Department of Commerce. https://csrc.nist.gov/pubs/sp/800/30/r1/final

National Institute of Standards and Technology. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). U.S. Department of Commerce. https://www.nist.gov/itl/ai-risk-management-framework

National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0. U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29

U.S. Department of Health and Human Services. (2025). Guidance on risk analysis requirements under the HIPAA Security Rule. Office for Civil Rights. https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html