Data Security Essential Strategies for RPM Platform

Remote Patient Monitoring (RPM) platforms manage confidential information, making Data Security a fundamental pillar in their infrastructure and design strategies. Over 90% of healthcare breaches involve patient records, costing $10.1M per incident, highlighting the urgent need for stronger Data Security practices. Robust protection is no longer optional, it's essential for compliance, patient trust, and the advancement of modern Data Security frameworks.

Esvyda addresses these risks by integrating enterprise-grade protections, ensuring Data Security while maintaining seamless care and RPM functionality.

Common Vulnerabilities in RPM Systems

Unauthorized access, weak API integrations, and exposed IoT devices top the list of RPM security gaps. A 2024 study found 68% of healthcare apps had inadequate encryption. Hackers exploit outdated software or misconfigured cloud storage, risking data leaks.

For example, 41% of breaches stem from compromised credentials. Esvyda mitigates these threats with segmented access controls and real-time anomaly detection. Proactive measures are vital to prevent disruptions in patient care

Data Security: Proven Best Practices for Clinics

Clinics mitigate threats by enforcing multi-factor authentication, AES, 256 encryption, and role-based permissions. The Office for Civil Rights lists multifactor controls among top HIPAA corrective actions following recent settlements. Staff cyber-hygiene training decreases phishing click-through rates by 70 percent, according to KnowBe4 benchmarks.

Additionally, rotating encryption keys quarterly limits exposure windows if credentials leak. Real-time SIEM dashboards detect anomalies, while immutable audit logs guarantee forensic integrity. Consequently, care teams spend less time on incident response and more on patient engagement.

Data Security: HIPAA Compliance and Financial ROI

HIPAA's Security Rule mandates risk assessments, workforce education, and encrypted transmission of electronic Protected Health Information.

OCR may impose fines up to USD 1.5 million per violation per year Beyond penalties, payer contracts reward cyber-mature providers with expedited reimbursements and lower scrutiny.

For example, CMS Remote Monitoring codes reimburse faster when platforms auto-populate time-stamped vitals, reducing manual claim edits. Consequently, executive teams view cybersecurity as a profit center: fewer denials, lower cyber-insurance premiums, and elevated patient loyalty.

Why Esvyda Delivers Unmatched Data Protection

At Esvyda, we prioritize Data Security to safeguard Protected Health Information (PHI). Our systems use AES-256 encryption to ensure that patient data is securely stored and transmitted. We have also initiated a SOC 2 readiness process, working with SecureFrame to evaluate and strengthen our infrastructure before undergoing external audits. These actions reflect our commitment to maintaining high standards of security and compliance as we continue enhancing our infrastructure.

Esvyda

eHealth Anytime, Anywhere

Esvyda's eHealth platform's streamlined workflows empower providers to elevate patient care, maximize revenue, and promote population health outcomes.

Our virtual health services seamlessly integrate with health records, medical devices, and wearables, boosting health staff efficiency, patient engagement, and information security.

Get to know us!

Device Type: Blood Pressure Monitor
Model: ES-60B
Serial Number: 1503698521K
Connection: Bluetooth

123/88 mmHg
133/90 mmHg
154/99 mmHg

Contact Us

+1 (408) 905 0341
+1 (408) 660 8666
info@esvyda.com
www.esvyda.com

Support Schedule

Jan – Mar	M -F	5 AM to 4 PM PST
Apr – Oct	M -F	6 AM to 5 PM PST
Nov – Dec	M -F	5 AM to 4 PM PST

Esvyda App!

Download on the App Store
GET IT ON Google Play
Open on Web browser

Blog FAQs About Us Privacy Policy Contact Us

esvyda
eHealth anytime, anywhere