Top 5 Security Risks Hiding in Connected Healthcare Apps

How MedTech and healthcare analytics teams can uncover and fix hidden security gaps before attackers or auditors find them.

The Growing Risk Landscape

Healthcare and MedTech applications are becoming prime targets for attackers due to their reliance on APIs, third-party integrations, and sensitive data exchange. As more systems move to the cloud, these applications face increasing exposure risks that traditional network defenses cannot mitigate.

According to the 2024 Verizon Data Breach Investigations Report, more than 80% of healthcare breaches involve web applications or third-party vendors. With personal health information (PHI) now among the most valuable data types on the black market, the importance of robust application security has never been higher.

1. Insecure APIs and Endpoints

Poorly configured or unprotected APIs often leak sensitive data such as PHI, credentials, or access tokens. Healthcare platforms relying on FHIR or custom APIs must enforce authentication, authorization, and data validation at every layer.

2. Improper Access Controls

Access misconfigurations expose internal dashboards or PHI repositories to unauthorized users. Adopting least-privilege principles and conducting regular access reviews help ensure only authorized personnel can access sensitive systems.

3. Outdated Encryption Standards

Using deprecated encryption protocols (e.g., TLS 1.0/1.1) or unencrypted backups leaves data vulnerable to interception. Healthcare apps must enforce strong encryption for both data in transit and data at rest.

4. Third-Party Integrations

Third-party vendors such as billing services, analytics platforms, or external data processors can introduce vulnerabilities. Perform due diligence and require evidence of HIPAA-aligned security controls from all partners.

5. Insufficient Logging and Monitoring

Many breaches go undetected for weeks due to poor visibility. Comprehensive audit logging and alerting help identify suspicious activity early and reduce breach impact.

How to Strengthen Healthcare App Security

- Conduct a penetration test on all public-facing APIs and web interfaces.
- Perform vendor security reviews to assess third-party risk exposure.
- Implement strong encryption across all systems handling PHI.
- Establish real-time monitoring and alerting for suspicious activities.

• Document controls and results to demonstrate HIPAA and HITECH compliance.

Sources & References

- Verizon Data Breach Investigations Report (DBIR) 2024

- U.S. Department of Health and Human Services – Office for Civil Rights (HHS OCR) Data Portal

- OWASP API Security Top 10 (2023)

- HIPAA Journal 2024 – Healthcare Breach Statistics