THREATSVIEW
Make it Simple

Regional Hospital Group Achieves HIPAA-Aligned Posture and Protects Patient Data

Client profile

A private hospital group operating six facilities across the UAE and Oman, handling protected health information for over 1.2 million patients and connected to insurance and national health systems.

The Challenge

Following an internal audit, the group identified gaps in vulnerability visibility across electronic medical record (EMR) systems, IoMT (Internet of Medical Things) devices, and clinician web portals. Compliance with HIPAA-equivalent local data-protection regulations required documented evidence of controls, but the security team had no central system to map controls to evidence or track exceptions.

Why ThreatsView

The combination of the Security Management Module (for unified vulnerability tracking) and the GRC & Resilience Module (for HIPAA, ISO 27001:2022, and local data-protection mapping) addressed both gaps in one platform.

Implementation highlights

- Qualys VMDR integrated for infrastructure scanning.
- Microsoft Defender for Endpoint findings piped in for incident context.
- Custom asset categories created for clinical vs. administrative systems.
- Uploaded HIPAA Security Rule controls and mapped evidence.

Results & impact

- Achieved 94% control coverage against the HIPAA Security Rule mapping within six months.
- Reduced time spent preparing quarterly compliance reports by approximately 70%.
- Identified and remediated 14 critical-severity findings on internet-facing patient portals that had been buried in scanner output for over a year.
- Established a documented exception register with formal risk acceptance workflows for legacy medical devices that couldn't be patched.

> *"We finally have a defensible answer when the regulator asks 'how do you know?'"*
>
> **— IT Risk & Compliance Manager**