Lookout for Hospital Systems

Hospitals must align with HITRUST and other privacy regulations. Lookout delivers mobile security to enable a modern approach to patient care.

Industry-Wide Security Challenges

As hospitals modernize their internal technological ecosystems, frameworks such as HITRUST help them create a more secure environment, especially when it comes to mobile devices. Security teams must extend their security strategy from traditional endpoints out to the mobile devices that are used by staff to access patient charts and other PII. Mobile malware, phishing attempts, and application attacks are becoming more prevalent, so it's necessary for hospital systems to ensure full protection against malicious actors while aligning with stringent compliance parameters.

Industry Challenges

1. Significantly modernizing internal systems to begin leveraging mobile
2. Stringent privacy regulations and frameworks
3. Accessing bedside patient data via mobile apps and devices

Real World Use Case for Hospitals

HITRUST's Common Security Framework (CSF) has been adopted by many hospitals on top of the tight compliance regulations under HIPAA. As employees use smartphones and tablets more frequently, they're leveraging cloud-based applications to access patient data in all parts of a hospital as well as from home. HITRUST helps security and compliance teams put policies in place that prevent any unauthorized code or apps from being executed. As a best practice, it's also key to understand how apps interact with each other like how a Top 5 healthcare system in the U.S. identified when unauthorized apps had access the address book containing PII on corporate-owned iPads.

Lookout Critical Capability

Lookout Mobile Endpoint Security grants visibility into all applications and their behavior on mobile devices, which can help an organization align with the HITRUST framework. This allows admins to put tight policies in place that restrict employees from loading any unauthorized applications onto the device by blacklisting all except a handful of apps, blocking any apps with access to PII and other sensitive data on the device, or block that device's access to the corporate network.

Why Lookout

Lookout Mobile Endpoint Security ensures continuous security and compliance on every device, leveraging a large data set fed by over 170 million devices, and the analysis of over 70 million mobile apps. With the Lookout Security Cloud, it's easy to deploy Lookout and apply security policies across the entire organization for both managed and unmanaged devices. Users receive alerts on malicious apps, network connections, and system anomalies at the OS level in real time; accompanied by simple on-device remediation capabilities. Learn how a Top 5 healthcare system in the U.S. is protecting patient data on iPads.