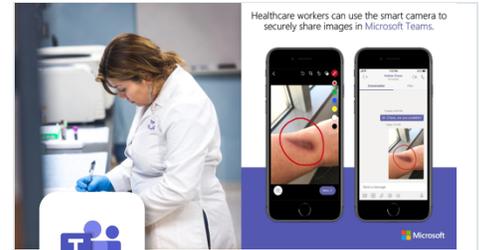


How Lookout secures Microsoft Teams for medical professionals

Lookout helps medical professionals comply with HIPAA through secure mobile collaboration.

The collaboration hub for Office 365 users

Microsoft Teams is the place to create and make decisions as a team. Bringing everything together in a shared digital workspace to chat, meet, share files, and work together with Office 365 apps. With apps for both iOS and Android, Microsoft Teams offers medical professionals a truly mobile-first way of collaborating in real-time to deliver fast, high-quality patient care. Whether you use mobile as a companion experience or as your primary communications app, Teams offers all the features you need to respond to urgent messages, access patient medical records, and keep in touch with your team.



Microsoft Teams + Lookout:

1. Group chat, meetings, and web conferencing
2. Collaborate with Office 365 apps
3. Lookout Continuous Conditional Access to sensitive medical records

Securing Mobile Collaboration

In today's digital world, medical professionals use mobile devices to share sensitive images and electronic medical records with globally and locally distributed teams in order to tackle the most difficult diagnoses. Highly sensitive medical information being share via mobile makes for an attractive target for malicious cybercriminals. To mitigate the risk of cyberattacks targeting medical information, Lookout has integrated with Microsoft Endpoint Manager App Protection for BYO devices to provide Continuous Conditional Access for Microsoft Teams. This integration enables healthcare organizations to continuously monitor the health of mobile devices and dynamically block risky devices accessing medical records shared among healthcare professionals within Microsoft Teams.

Lookout Critical Capability

Lookout protects iOS and Android devices against all mobile threats including; phishing attacks via email, text messages and social media apps, malicious apps, operating system vulnerabilities and malicious Wi-Fi networks. These threats can lead to leaked or exposed sensitive data, which according to IDC, is the top mobile security incident organizations have experienced in the last year¹. By leveraging Lookout Continuous Conditional Access, which dynamically monitors the health of the endpoint, you can continuously protect sensitive medical information from being leaked or exposed on mobile devices.

Why Lookout

Lookout Mobile Endpoint Security ensures continuous security and compliance on every device, leveraging a large data set fed by over 180 million devices, and the analysis of over 100 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 and remediation steps on malicious apps, network connections, and system anomalies in real time; accompanied by continuous device health checks to provide continuous conditional access to sensitive corporate applications and data to ensure employee devices aren't leveraged by malicious actors to steal assets.

¹ IDC Enterprise Mobility Decision Maker Survey 2018, Nov 2018: <https://www.idc.com/getdoc.jsp?containerId=US44434018>