How a Leading University Hospital System Secures Patient Data

The Problem: Protecting Data in a Compliant Manner While Migrating to Full Cloud Adoption

- As a research and testing hospital, employees and staff need to have remote access to sensitive data and securely collaborate with external stakeholders. This often means downloading protected health information (PHI) data to a local disk or USB drive.
- With a high volume of electronic data transfers and remote devices, there are dozens of ways that security can break down leading to compliance violations.
- Their on-premise legacy data loss prevention (DLP) solution was tuned for compliance requirements but had limited visibility and protection capabilities for cloud data. They needed to bridge the gap with a cloud-based DLP solution that could still leverage the policies from the existing solution to take action on data in the cloud.
- With researchers around the globe, keeping data encrypted after it left the infrastructure was critical to ensure continued alignment with HIPAA. This required encryption of PHI data both at rest and in motion; including data on a disk, USB drive or other local resource was critical for this university health system.

Customer Overview

This university healthcare system is ranked as one of the top 10 hospitals in the United States and has over 40,000 employees. They are a global leader in medical research and serve well over two million patients annually.

Industry: Healthcare

Solution: Securing sensitive data in the cloud, while maintaining compliance with Lookout.

Results

- Secure private health information to meet compliance regulations, like HIPAA
- Enable collaboration of sensitive data between medical practitioners, field researchers and external partners in secure manner
- Unified approach to securing cloud and SaaS apps with one solution for scalability, policy management and cost savings
- Integration with existing solutions to provide additional visibility and cloud data protection while leveraging existing DLP policies

The Solution: Bridging the Old and the New to Secure a Hybrid Cloud System

- This leading university hospital system moved confidently through each step of its cloud journey knowing sensitive data would remain safe and HIPAA compliant. Extending the hospital's legacy on-premise DLP to cloud apps with the cloud-delivered Lookout DLP gave the hospital the ability to discover, monitor and protect their sensitive data.

- The integration between cloud and on-premise data protection secures terabytes of data moving in and out of Box and Microsoft 365—both at rest and in transit.

- By integrating with the existing DLP and its policies and workflows, the hospital extended finely-tuned rules and business logic to cloud control points.

- Lookout will continue to help the hospital along each step of its cloud journey. The hospital will be able to stay ahead of any changes to HIPAA and other data privacy regulations by expanding its use of the Lookout Security Platform beyond DLP.

About Lookout

Lookout is an integrated endpoint-to-cloud security company. Our mission is to secure and empower our digital future in a privacy-focused world where mobility and cloud are essential to all we do for work and play. We enable consumers and employees to protect their data, and to securely stay connected without violating their privacy and trust. Lookout is trusted by millions of consumers, the largest enterprises and government agencies, and partners such as AT&T, Verizon, Vodafone, Microsoft, Google, and Apple. Headquartered in San Francisco, Lookout has offices in Amsterdam, Boston, London, Sydney, Tokyo, Toronto and Washington, D.C.

Read the blog at lookout.com/blog/hospital-secures-patient-data-with-lookout.

To learn more about how Lookout can protect your data, visit lookout.com/healthcare.