FORTINET

NAC PROVIDES SECURE BYOD AND AIDS HIPAA COMPLIANCE AT UC IRVINE MEDICAL CENTER

> *"With 100% visibility and control over every device and user on our network, we can define and enforce granular policies to manage risk and ensure compliance."*
>
> *— Jeff Barnes*
> *Information Security Officer*
> *University of California, Irvine*

School of Medicine
University of California • Irvine

A world-class academic medical center with a full range of acute and general-care services, University of California's Irvine Medical Center is at the forefront of medical education and research and prides itself on delivering the highest quality patient care.

At UC Irvine Medical Center, mobile devices such as iPhones and iPads are a way of life for doctors, professors, medical students, and staff. When Allscripts, which supplies the medical center's electronic medical record (EMR) system, announced it was developing a mobile app, "We knew our doctors and medical personnel would be clamoring to use this application," explains Adam Gold, Director of Emerging Technologies at UC Irvine Medical Center. "The time had come when we needed a BYOD strategy that would enable our staff to securely use their own devices at the medical center."

Several challenges would need to be overcome along the way. The most pressing concern was protecting HIPAA-compliant data. Gold recognized that security had to start at the endpoint, so only approved, secure devices are allowed on the network.

MANAGING SECURE EMR ACCESS AND HIPAA CONCERNS

Physicians, instructors, students, and hospital staff interact with the EMR system differently, and varied access levels had to be easy to define and applied automatically. The hospital also had to enforce its security policies without appearing heavy-handed, so users could get on the network easily with personal devices while EMR access continued to be protected.

Concerns about regulatory compliance were particularly daunting. Hospitals are subject to internal and external audits to verify that sensitive HIPAA information like patient records and research data is secure and protected from misuse. Demonstrating compliance is hard enough when all devices are under internal control, but a BYOD environment adds an even greater layer of uncertainty. With HIPAA fines that can reach millions of dollars, ensuring and documenting compliance is crucial. UC Irvine required complete endpoint visibility, and the ability to define access levels, for every device connecting to its network.

DETAILS

CUSTOMER: UC Irvine Medical Center

INDUSTRY: Medical

LOCATION: Irvine, California

BUSINESS IMPACT

- Automatically identifies every device and user accessing the network, and blocks unsafe devices and unauthorized users
- Automatically provisions network access according to the user's specific profile
- Help desk calls were reduced by 30% because users can manage their own devices
- Ability to demonstrate regulatory compliance with a few clicks

DEPLOYMENT

- Network Access Control

USING NAC FOR FULL VISIBILITY AND CONTROL TO DEMONSTRATE HIPAA COMPLIANCE

UC Irvine Medical Center chose the Fortinet Network Access Control (NAC) solution to solve the problem of visibility and access control, while providing traceability to demonstrate HIPAA compliance across the operation. To address the BYOD and mobile access security challenge, the NAC solution integrated with mobile device management (MDM) software. MDM software enables the medical center to have stronger control over BYOD and hospital-owned mobile devices. To access the network, mobile devices must download the MDM app. This app ensures that each device is provisioned for safe access, correlates devices with owners, and confirms that each device has the minimum required antivirus and system patches, before the device can access the network. MDM software can also help locate or wipe devices that are lost or stolen to prevent unauthorized network access. These controls are critical to ensure the integrity of the network and HIPAA compliance.

NAC also enables UC Irvine to identify every endpoint and device connected to its network in real time. It can identify any potential unauthorized device and quarantine it immediately. NAC keeps a history of activity for each individual device and endpoint, so it can identify any suspicious activity, as well as provide records of all data access.

In addition, NAC enables the medical center to easily control permission and access, ensuring that each device accesses only the necessary data for their particular function. NAC's ability to offer role-based access permissions is another key criterion for keeping HIPAA-compliant data secure.

UC Irvine is very pleased with the solution. The medical center even saw a 30% reduction in help desk calls, as NAC provides an automated help and remediation page. NAC offers the HIPAA-compliant security they require, along with an efficient, user-friendly experience that keeps productivity high in the fast-paced medical environment.

FORTINET®

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
8 Temasek Boulevard #12-01
Suntec Tower Three
Singapore 038988
Tel: +65-6395-7899
Fax: +65-6295-0015

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990