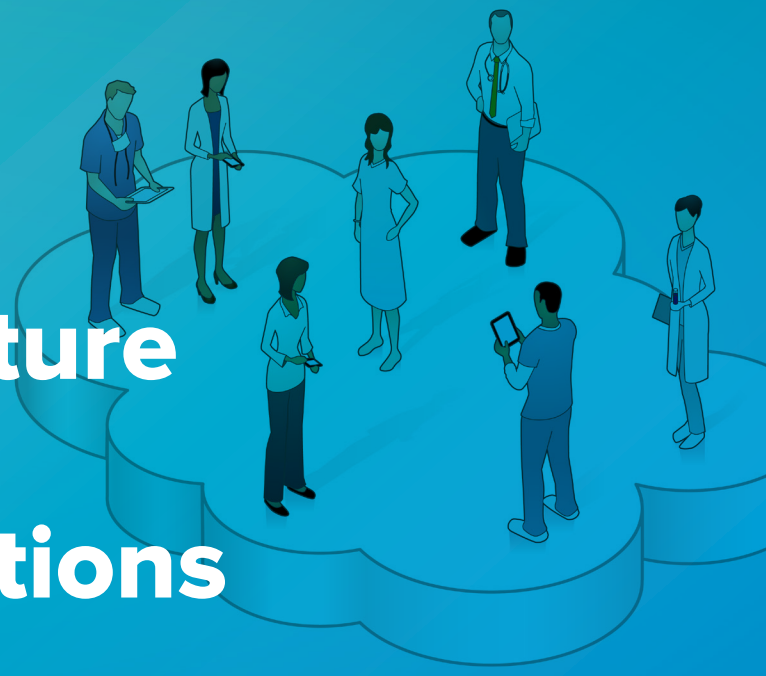
MICRO FOCUS
Government Solutions



# Securing the Future of Cloud-Based Healthcare Solutions

## Overview

The case for cloud-based electronic health records (EHRs) is a compelling one: streamlined operations, ease of access, improved information sharing and analysis—and the opportunity for innovations yet to be developed. But cloud-based EHRs also come with risks.

Healthcare organizations cannot afford to transition to the cloud if they cannot adequately protect those records from unauthorized access, improper use or data breaches.

The problem is that controls of traditional on-premise EHRs were not developed with the cloud in mind. Some of those advantages of a cloud-based platform—the ease of access and information sharing—also represent vulnerabilities if improved controls are not put in place.

The risks are real. As we have seen, healthcare systems are under constant cyber attack. Healthcare organizations, on average, face more than twice the number of cyberattacks compared to other industries.

In part, that is because of the nature of the data itself. A recent report from the Department of Health and Human Services' Office of Inspector General notes that healthcare data can be up to 10 times more valuable to cyber criminals than credit card numbers. And in part, it is because healthcare organizations are often seen as "soft targets," since they have not invested in cybersecurity technologies at the rate of other industries.

But these risks are also addressable. A multi-pronged-approach to cybersecurity can ensure that your organization can take full advantage of the cloud as a platform for innovation without compromising the security and privacy of data.

### The Challenges of Migrating to Cloud-Based Solutions

In moving health solutions to the cloud, consider the following questions:

- How do you integrate data from legacy applications?
- How do you manage identities across different environments?
- What are your options for authenticating those identities?
- Do you have the ability to detect suspicious activity?
- How do you monitor the activity of your most privileged users?
- How do you protect the data throughout its lifecycle?

MICRO FOCUS
Government Solutions

## The Need for Multi-Factor Authentication

One of the most important security controls for any data is identity. Technology leaders want to know exactly who is accessing data, when they are accessing it, and how.

Multi-factor authentication (MFA) can provide that additional layer of security when it comes to identity, requiring users to identify themselves with something other than a password. That may mean typing in a code sent to a mobile device or an email, using a common access card, or even confirming a biometric marker.

Healthcare organizations need systems that can govern MFA access, setting the rules that each user must follow in order to access information.

These controls ensure that only the person who is supposed to access data can do so. They also help notify administrators when a person's identity is tried, unsuccessfully, to access data, alerting them to a possible anomaly.

## The Benefits of Adaptive Controls

Identity is not the only control. Healthcare organizations also need to monitor end-user behavior. Adaptive controls can help monitor user behavior to look for larger anomalies that can be the sign of a breach.

Adaptive controls monitor all access requests to find patterns. The system can remediate these requests, approving ones that appear normal. That decision gets remembered over time and becomes a unique factor to each organization.

For example, a healthcare organization may have users that access data 24 hours per day, while others may be limited to certain time windows. Too much activity over an abnormal time period may be the sign of a larger problem.

By monitoring who accesses data and how it is used, healthcare organizations can know that their patient data is being used properly in the cloud-based environment.

## Making Secure Cloud-Based Health IT a Reality

We have a long history of working on health solutions in the most demanding healthcare environments. Some of the largest unified electronic health record platforms depend on Micro Focus technology to provide identity, access management, multifactor authentication and additional security capabilities to protect sensitive PHI data.

**Our portfolio of offerings include:**

**Verastream Host Integrator**
Make legacy applications and data accessible to cloud-, web- and mobile-based apps

**Identity and Access Governance**
Use integrated identity information to manage access controls across local, mobile and cloud environments

**Advanced Authentication**
Provide a single multi-factor authentication (MFA) framework for all applications and devices, with the broadest MFA method support

**Sentinel & Change Guardian**
Integrate identity information with security monitoring to detect and respond to suspicious activity

**Privileged Account Management**
Provide continuous monitoring of high-value systems by enforcing controls and recording risky, privileged account activities for all credential-based systems

**Voltage SecureData**
Provide continuous protection to PHI data at rest, in motion and in use across local, mobile and cloud environments