Securing your virtual care practice

Securing your virtual care practice at a glance:

- Robust patient and clinician lifecycle management
- Enforced least privilege access
- Advanced access management

Since virtual care depends on new communication technologies, infrastructures, and remote environments, they raise new privacy and security concerns. To protect this regulated information, OpenText™ identity and access management (IAM) offers an identity-centric platform designed to extend beyond traditional boundaries.

Telemedicine has been around for years as a specialized service designed to serve rural communities and help specialists follow up with their remote patients. But since the COVID-19 pandemic, it has become more common for everyday practice.

Why virtual care is expanding

Experts forecast that telemedicine will grow to $23.5B in the next three years with an annual CAGR of more than 44 percent.[1] There are many reasons virtual care is an attractive option:

Additional choice for urgent care: Trips to the ER are 12 times more expensive than using a physician's office.[2] While alternative urgent care facilities have helped mitigate that cost, offering virtual care as another option will go even further. According to UnitedHealth Group, $32B is wasted annually on trips to the ER. Beyond the cost, telemedicine can help patients avoid long drives and long wait times.

1 Grandview Research, *U.S. Telehealth Market Size, Share & Trends Analysis Report*

2 UnitedHeatlh Group, *The High Cost of Avoidable Hospital Emergency Department Visits*, 2019

Improved outcome for patients with chronic diseases: Traditional approaches to managing chronic disease involve several months between visits. Gathering necessary information like blood pressure or blood sugar readings more frequently helps physicians be timelier in their adjustments. As part of the telemedicine model, wearable devices allow for more-frequent medication adjustments or other treatments.

Expanded reach and specialty care: Some patients have a condition that requires interstate access to the right specialist. While primary care doctors have the expertise to correctly diagnose and treat most of their patients' ills, sometimes it is not easy to access the expertise needed to diagnose and treat certain conditions. While early visits likely require on-site appointments and procedures, remote and video technology enables follow-ups without interstate travel.

Security barriers to virtual care

Healthcare providers and administrators require the same information during virtual care compared to an on-site visit. But the way it is gathered can be quite different, especially for urgent care, if the patient's profile information hasn't been onboarded into the clinic's EHR system. For example, clinics will need a reliable way to gather and confirm identity and insurance information.

Unless virtual care is an integrated part of a longer-term practice where remote monitoring technology is already in use, clinicians are limited in directly gathering vitals like blood pressure or specimens with each patient. Beyond health assessment, important identity and insurance information also needs to be onboarded and disseminated to multiple agencies. Doing this securely and quickly while maintaining compliance takes forethought and planning with the right fit digital technology.

Identity powers virtual care

When an organization's security paradigm is identity based, they're able to apply it across various devices and disparate environments.

Patient and clinician lifecycle management

OpenText identity and access management offers the most robust patient lifecycle management on the market. It normalizes patient identity information across all types of identity repositories and leverages its pub/sub architecture to quickly enforce centralized policies.

Enforce need to know access

While it is essential for clinicians to have access relevant EHRs, the most effective security practice is to avoid granting permissions to those who don't. OpenText Identity Governance enables effective access governance management by presenting only the relevant information to the approver to make the right decision when granting permissions to sensitive digital information.

Advanced access management

Providers need to deliver quick EHR access to their clinicians while protecting against imposters. Even though providers face daunting privacy mandates, their patients expect convenient access to their ePHI and billing information from anywhere. OpenText IAM's standards-based authentication and authorization platform offers various clients, gateway, and SDK solutions to accommodate any access requirement.

Virtual care is going mainstream

"Virtual care's potential to reshape the health care delivery landscape and patient experience is clearer than ever. The COVID-19 pandemic mainstreamed virtual health, and the momentum continues as it becomes a part of the health care ecosystem. Demand continues to be robust."

Spokesperson,
United Healthcare

OpenText Identity and Access Management ›

Conclusion

The OpenText identity and access management platform offers a holistic identity control platform by:

- Taking advantage of automated provisioning and governance for all identity stores.
- Offering adaptive intelligence for both entitlement management and context-based access control
- Enabling organizations to verify identity claims by matching authentication strength and authorization levels to currently measured risk.

Clinics benefit from identity-based security through improved recognition and response protections along with improved usability, enabling more attention to patient outcomes.

opentext™