opentext™ | Cybersecurity

Flyer

Securing Your Virtual Care Practice

Since virtual care depends on new communication technologies, infrastructures, and remote environments, their use raises new privacy and security concerns. To protect this regulated information, NetIQ offers an identity centric platform designed to extend beyond traditional boundaries.

Securing Your Virtual Care Practice at a Glance

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."

Spokesman for United Healthcare

Identity-Powered Security

For your virtual care environment, you need security that can aggregate and manage identity information across all your digital services.

Telemedicine has been around for years as a specialized service designed to serve rural communities as well as help specialists follow up with their remote patients. But the recent pandemic has put it front and center as it was a core strategy to deter the spreading of COVID-19.

Why Clinics Are Expanding Their Virtual Care Practice

Although pandemic waivers will likely be phased out in 2023, experts forecast that telemedicine will grow to $23.5B in the next three years with an annual CAGR of over 44%[1]. At this same time, clinics are expanding their practice into a full virtural care service.

Additional option for urgent care—trips to 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 ER. Beyond the cost, telemedicine can help patients avoid long drives and long wait times.

1. **www.grandviewresearch.com/industry-analysis/us-telehealth-market**
2. **www.unitedhealthgroup.com/newsroom/posts/2019-07-22-high-cost-emergency-department-visits.html**

Improved outcome for patients with chronic diseases—today, traditional approaches to managing chronic diseases usually mean a cadence of several months between visits. Gathering necessary information like blood pressure or blood sugar readings regularly and 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.

Expand the reach and speciality 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 95% of their patients' ills, the expertise needed to accurately diagnose and treat but no easy way to obtain the other 5%. While early visits will likely require onsite visits and procedures, today's remote and video technology enables follow-ups without interstate travel.

Security Barriers to Virtual Care

While it's true that there is a diverse set of circumstances and preferences that prevent virtual care from being the only form of healthcare, it does offer some compelling advantages.

While the information needed for virtual care is mostly the same, 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. But beyond health assessment, important identity and insurance information 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—NetIQ 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—whiles its essential for clinicians to have access relevant EHRs, the most effective security practice is to avoid granting permissions to those who don't. NetIQ's Identity intelligence engine 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 patiants expect convenient access to their ePHI and billing information from anywhere. NetIQ's standards based authentication and authorization platform offers various clients, gateway, and SDK solutions to accommodate any access requirement.

Summary

In short, the NetIQ 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 synergized with improved usability, enabling more attention to patient outcomes. To learn more visit our website. Also, check out our NetIQ Unplugged channel.

Connect with Us

www.opentext.com

761-000102-003 | O | 10/23 | © 2023 Open Text