EXECUTIVE BRIEF

New Ways to Think About Delivering Telehealth with Convenience and Compliance

“Safe connectivity and identity verification practices must be at the forefront of telehealth services on both the provider and patient fronts.”

HOW IDENTITY VERIFICATION TECHNOLOGY IS CHANGING THE FACE OF TELEHEALTH

It’s not often that we witness a technology adoption curve skyrocket in the span of a year, especially in healthcare. Yet, that’s exactly what’s taken place in telehealth this year given the growing demand for safe, convenient and socially distant healthcare.

Simply defined, telehealth is the long-distance delivery of healthcare, health education and health information services via electronic information and telecommunication technologies. In a move to fill the demand gap for these remote services, healthcare providers have been rapidly adopting and scaling their telehealth offerings. The U.S Centers for Disease Control and Prevention reported a 154% increase in telehealth visits during the last week of March 2020, compared with the same period in 2019. The usage increase is further confirmed by a McKinsey study showing that telehealth services have seen a sharp increase in consumer adoption. 46% of consumers are using telehealth to replace canceled in-person visits, while in 2019, that figure was only 11%. Moreover, the report found that 76% of consumers are highly or moderately likely to use telehealth in the future.

When considering the possible consequences involved in venturing out to a physician’s or clinician’s office, it is no surprise that the public has demonstrated an increased acceptance and appetite for alternative options for accessing health services. In addition to the comfort and convenience of being at home, patients benefit from telehealth in other tangible ways: there is no time or anxiety exerted from traveling, hunting for parking or sitting in a waiting room with others who may pose a health risk. Providers also benefit from telehealth options, as they are able to serve more patients, realize reduced overhead and even improve patient outcomes through increased engagement.

UNDERSTANDING THE VULNERABILITY FRONTS IN TELEHEALTH

As use of these remote capabilities grows, the need for robust security tools and processes is vital. The same electronic information and telecommunication technologies that make telehealth possible are also the tools that create cybersecurity risks. Therefore, safe connectivity and identity verification practices must be at the forefront of telehealth services on both the provider and patient fronts in order to mitigate the risk present in a virtual care environment.

From the provider front — hospitals, medical practices, health clinics, pharmacies, etc. that employ the administrators, clinicians and other staff who interact with patients — their system infrastructure must be secure. Given that insiders are often healthcare's biggest weakness, providers face security challenges that include:

User Access and Experience — Telehealth demands that providers maintain strict control over user/employee access while also providing a seamless experience when it comes to usability and convenience. The security and penalty stakes are much greater in a healthcare setting, as the Health Insurance Portability and Accountability Act (HIPAA) requires that providers adhere to strict guidelines that appropriately safeguard electronic protected health information (ePHI).

Cyber fraudsters — Digital health records are an appealing target for criminals, as they include comprehensive information on a patient's health background and identity. Human error is often a major factor in breaches, and bad actors look for those vulnerabilities. They use ransomware and malware to gain access to systems, PHI and even to interrupt private telehealth sessions. When IT systems are hacked, patient data may be compromised or stolen, and providers can be penalized severely if proper security was not used to appropriately protect their systems.

Licensure scope — During a traditional healthcare visit, it is reasonable to assume that the provider and patient live in the same state. With a telehealth visit, that may not be the case. Laws and licensing requirements of different states can introduce risk with regard to practicing across state line, even to well-intentioned providers. Therefore, the provider must manage the additional responsibility to ensure that each clinician has the appropriate assigned rights and access to manage that risk.

With regard to the patient front, providers must also consider additional vulnerabilities, including:

Patient identity theft — Providers could unknowingly contribute to identity theft if they are not properly authenticating the patient's identity prior to rendering telehealth services. While established patients may have a copy of their ID on file, new patients likely won't, so a provider needs the ability to confirm that the person receiving care is actually the person listed on the patient record and not someone else who has stolen the identity.

Medical insurance fraud — With the rising cost of healthcare, the incidents of medical fraud are trending upward. Insurance sharing among family members is fraud, and providers must be on guard with proper patient identity verification tools. Even with a driver's license and insurance card, can the provider know with certainty that the patient is not a relative.

Medical device monitoring — Medical devices, such as infusion pumps and heart monitors — which are often sent home with patients for remote monitoring — may not be equipped with appropriate security features when used in a home environment. Therefore, proper security precautions must be taken to thwart hackers from intercepting data that is transmitted or stored on such devices.

BUILDING TRUST, MANAGING SECURITY AND BALANCING USEABILITY

In order to maintain the confidentiality and integrity of patient data and ensure the safety and identity of patients, organizations are establishing telehealth best practices and focusing on tools and strategies to remain safe and compliant, while also maintaining usability and accessibility.

Federal mandates in the U.S. already require hospital staff to display a picture ID badge, so hospital systems can easily use and integrate that same ID to grant staff members access to telehealth systems.

With regard to special access requirements, providers are also finding single sign-on (SSO) technology to be a great solution. Not only can SSO secure user access to various types of equipment within an organization — from computer workstations and electronic health record applications to infusion pumps and health monitors — it can also confirm and enforce access policies, such as user privileges or roles, to ensure that the badge has the appropriate assigned rights, which could even include licensure parameters. Since single sign-on technology provides a detailed log of each user who accessed a system and what they did while on the network, the risk associated with inappropriate access, unauthorized disclosures of ePHI and potential intrusions or malicious activity are reduced.

"Not only can SSO secure user access to various types of equipment within an organization — from computer workstations and electronic health record applications to infusion pumps and health monitors— it can also confirm and enforce access policies, such as user privileges or roles, to ensure that the badge has the appropriate assigned rights, which could even include licensure parameters."

Additionally, with verification processes referred to as Know Your Customer (KYC) or Know Your Patient (KYP), providers can confirm that patients are who they claim to be during a virtual visit. Patients can provide a live image via their smartphone or webcam while biometric analysis and facial recognition provide the ultimate identity confirmation.

Given the breadth and scope of the challenges and vulnerabilities present in telehealth, balancing security and usability can be difficult. But with the right IT tools and technology, along with a keen security awareness, providers can properly manage the user experience, protect data and ensure privacy.

HID Global has been at the forefront of major technology shifts over the years, and we are working to solve many ID verification challenges for the secure delivery of telehealth now, and in the future.

For more information on how your organization can benefit from implementing SSO and other identity verification technologies:

Read our blog post – ***Extended Access Technologies: Improved Patient Care with Advanced Biometrics***

Watch our video – ***A Day in the Life: Secure Access and Authentication in Healthcare***

Check out our infographic – ***Healthcare's Problem with Passwords***

Or, learn more about ***HID's portfolio of RFID-enabled readers*** (ready-made for providers to authenticate themselves using a badge or mobile device) at ***hidglobal.com/products/readers/omnikey.***

hidglobal.com