How Does Telemedicine Work? The Future of Healthcare Technology in the Era of COVID-19

by Jenny Kanevsky | Dec 30, 2020 | Healthcare | 0 comments

According to the Monthly Telehealth Regional Tracker, US telehealth claim lines (an individual service or procedure listed on an insurance claim) increased by 4,132% from June 2019 to June 2020. This significant increase is due in large part to the COVID-19 pandemic. More telehealth is necessary, but it is also good. For all patients, virtual visits and greater record access means added convenience. Once isolated rural patients get remote consultations, elderly and mobility-challenged patients receive in-home health monitoring, and medical professionals efficiently exchange information.

Because of increased mobile device use and a growing remote workforce, continued COVID-19 restrictions, and consumer demand, healthcare organizations are looking to telemedicine as a viable patient care delivery mechanism. Hospitals and providers seek to adapt and ensure patients receive the highest level of care while maintaining HIPAA compliance and safeguarding Protected Health Information (PHI). The implementation of a secure, cost-effective, and administratively manageable remote care program is complex.

It's important to understand the fundamentals of how telemedicine works, the drivers for its growth, and its compliance requirements.

What is Telemedicine?

Telemedicine covers various aspects of remote care. Real-time audio or video visits between a provider and a patient are most common, though follow-up communications, appointment reminders, and medication adherence continue to grow. Other telemedicine features include data sharing between providers, patient tracking and remote monitoring, and the use of devices to record and remotely relay health information. These functions lead to a better patient care experience, empowered providers, and streamlined administrative and IT processes. Secure, well-implemented telemedicine is progress.

How Does Telemedicine Work?

Healthcare systems need technology, tools, and security support to launch a successful telemedicine program. Company-issued or personal smartphones and tablets enable timely information access and mobile communication, so providers and patients can easily navigate the remote care process. Mobile data security and management are essential and PHI is a top cyberattack target. Endpoint solutions that protect data, not just devices, can eliminate most transmission risks and enable HIPAA compliance. Successful, secure telemedicine implementation also requires effective Bring Your Own Device (BYOD) policies and protocols.

The traditional mobility management solution is Mobile Device Management (MDM). However, MDM has drawbacks. Individual devices must be managed, maintained, and controlled by IT, meaning high administrative and financial costs. Because MDM solutions allow organization data, meaning PHI and other sensitive information, to transfer to and reside on mobile devices, data is difficult to control and protect. As a result, security and HIPAA compliance are at risk.

Also, MDM allows IT control of and visibility into mobile devices. For providers and staff, this means a potential invasion of privacy. IT will do a remote wipe if a device is compromised, deleting all data, including any personal information stored on the device. Many employees circumvent MDM BYOD solutions to avoid this, rendering these solutions useless, wasting resources, and creating a cyber-threat. Telemedicine works when technologies address consumer demand, provider needs, and organizational security compliance and administrative concerns.

Telemedicine Drivers

Telemedicine is not new, but its demand rapidly increased due to COVID-19. Before the pandemic, hospitals established remote care to serve rural and elderly patients. However, as technologies improve and COVID-19 persists, providers extend telemedicine's uses far beyond pandemic needs.

According to Forbes, overall future visit percentages are likely to stay higher than pre-pandemic levels. Patients and providers find them more efficient, and they are less costly than in-person visits. Patients avoid commute times and long waits. Employers benefit since employees miss less work. Hospitals require lower in-patient and scheduling overheads, and doctors can provide care from anywhere.

McKinsey & Company report societal changes from the pandemic and consumer preference for virtual and at-home services. An ever-increasing push to decrease healthcare costs will likely continue to drive telehealth demand. Some insurers are even testing virtual-first health plans that offer lower premiums.

Telemedicine Solutions

Telemedicine is here to stay. Hospitals implementing it must balance security, regulatory compliance, and management considerations to ensure effective, efficient PHI and enterprise data protection.

Mobile devices are telemedicine cornerstones but can place PHI at high risk. BYOD policies should be flexible and user-friendly to encourage employee acceptance and adherence. Traditional MDM solutions do not effectively protect mobile devices and data. They provide limited mobile data protection and require strict BYOD protocols designed to control how, when, and where employees can use their devices. MDM threatens telemedicine success and puts organizations at significant risk of HIPAA-related violations.

Hypori Virtual Mobility™ is a secure, centrally managed, budget-conscious solution that maintains 100% separation of personal and enterprise data. With the Hypori® app, providers have access to and can interact with patient data without putting it at risk. No data ever resides on the mobile device. If a provider's device is compromised, the patient data remains protected from breach or identity theft.

Hypori controls the data, not the device, and enables flexible BYOD policies. A powerful, central administrative hub increases IT department efficiency. By streamlining mobility through a virtual operating system, organizations easily control data and network protection at a lower cost than MDM solutions. As telemedicine grows, it needs technology that empowers providers, meets consumer demand, and addresses industry cybersecurity needs. Hypori is a scalable, HIPAA-compliant-enabled, secure, centrally managed, budget-conscious BYOD solution that both providers and patients will embrace.