Acta Scientific MEDICAL SCIENCES (ISSN: 2582-0931)

Volume 7 Issue 5 May 2023

Review Article

Do the Benefits of Telehealth Outweigh the Security Risks?

Allison Eagen*

Department of Medical Sciences, USA

***Corresponding Author:** Allison Eagen, Department of Medical Sciences, USA.

Received: March 30, 2023

Published: April 18, 2023

Abstract

Telehealth is a rapidly evolving adjunct to the healthcare environment providing numerous benefits on many levels. This approach has branched out into many areas including virtual physician visits, access to allied health specialties and therapies, and patient monitoring for prophylactic and post care. Today's healthcare environment can see telehealth use through technological avenues such as video conferencing, the internet, imaging transmission, streaming media, portals, remote application use and monitoring devices. While these benefits can be felt by many stakeholders, there are also numerous risks to this growing field. While the documented benefits to this technology are numerous and well documented, do these benefits of telehealth outweigh the security risks?

Keywords: Telehealth; Security Risks; Healthcare

Background

Telehealth technology can extend its roots all the way back to the use of the phone to transmit radiologic images in 1948. While evolutionary at the time, this technology has truly evolved significantly and now broadly encompasses multiple uses and benefits. Mayo Health defines telehealth as the "use of digital information and communication technologies, such as computers and mobile devices, to access health care services remotely and manage your health care" (Mayo Clinic, 2017, Telehealth: Technology meets healthcare, para. 2) [1]. As such this technology has extended to include physician sessions from the patient's home in the form of virtual appointments, allied health services such as psychological emergency or non-emergency services, physical, occupational and speech services, dental and additional home health services. This practice also includes chronic disease management and monitoring services. Furthermore, telehealth also includes consumer and professional education as well as patient portal services (Center for Connected Health Policy, 2019, About telehealth, para. 2) [2].

Current issue

The benefits for all of these telehealth practices are numerous. For rural and geriatric populations, this methodology can be life changing and even lifesaving. These populations oftentimes have challenges in being able to make their doctor's appointments and overall manage their condition. They may have trouble organizing resources to get them to an appointment. As such, the ability to have a consult with their physician or additional recommended medical services can more so allow them to efficiently obtain these services. Furthermore, these populations may be apt to additionally have chronic medical issues which presents even a greater challenge with the quality and quantity of care needed. They may additionally need to manage multiple clinical services and specialist visits and be additionally challenged financially and by managing the additional resources to obtain all of the needed services to manage their chronic condition. For these populations, they may also not have easy access to the services they need being physically provided within their immediate vicinity. This dilemma is often the

case in rural communities where adjunct allied health services may not readily be available. Using telehealth, the populations in these rural communities can still obtain these valuable services to help manage their condition.

The benefits for chronic conditions have been well documented. A study "commissioned by the National Health Service for Health Evaluation Programme" (US National Library of Medicine National Institutes of Health, 2013, The impact of telehealth on the quality and safety of care: A systematic overview, para. 6) [3] searched the "the Cochrane Library, MEDLINE, EMBASE, LILACS, IndMed and PakMed for systematic reviews published from January 1997 to November 2011" reviewed "81 systematic reviews" summarized that "complex integrated interventions involving telemonitoring, education and additional support, potentially including home visits do have the potential to modestly improve outcomes" (US National Library of Medicine National Institutes of Health, 2013, The impact of telehealth on the quality and safety of care: A systematic overview). For those suffering with chronic conditions, a virtual appointment with the patient's primary physician can allow a more triaged and efficient approach to managing the need for specialty physician services as well as the management of acute needs. Additionally, physicians can more easily communicate between each other and transmit necessary test results and diagnostics for a specialist to have a more complete picture before determining if it is necessary to bring the patient in for a face-to-face visit. Ultimately, this process could be time saving as it is oftentimes hard to easily get in to see a specialist. As such, more acute episodes related to a chronic condition can be more efficiently managed. Additionally, having to travel whether near or far to get medical services can be challenging when you are actually experiencing the symptoms of the medical issue and are truly not feeling well.

The benefits provided through consumer and provider education and use of portals improve overall patient engagement. First, patients can utilize portal services to more easily schedule and maintain appointments. The engagement extends to reviewing communication and diagnostic results posted from their physician as well as pose questions in return for their provider. These practices help with enforcing the patient's engagement in their condition, trust in their provider and the care being received and openness to communicate more effectively with their provider. Additionally, patient engagement may improve with a portal's ability to more easily manage and fill the pharmaceutical component which is a key component to managing the disease. Alerts can be provided through various means to ensure that the patient does not miss doses and properly refills and manages their prescriptions. Utilizing patient education resources will also assist the patient and their family and care support team in overall engagement in their condition. The provider can also benefit from using telehealth to review educational resources to find the most optimal care for the patient whether they are having a virtual appointment or face-to-face appointment.

In the area of monitoring devices, telehealth can vastly improve the ability to improve the management of care and outcomes for patients. Medical issues demonstrated through critical vital sign recognition from remote monitoring can pre-emptively help to get patient's the care they need before the situation becomes worse or it is too late. This form of monitoring can be lifesaving for elderly patients or those that cannot independently monitor their condition. Additionally, this monitoring can assist with chronic conditions through alerts when signs are remotely seen such as those suffering from depression or chemical dependencies.

Finally, the cost benefits from telehealth are also numerous for the provider, the patient and society as a whole in helping to manage overall healthcare costs to society. Providers can utilize virtual appointments to bill for services and more efficiently manage office staff and time. This practice may assist in capturing billed time for missed appointments. Additionally, there is a cost saving benefit through the coordination efforts with specialists and additional providers as test results and additional information can be shared ahead of time preventing duplication and a more efficient approach to care. Patients will experience a cost benefit by not spending time on transportation costs and costs associated with coordination of care between providers if some face-to-face appointments can be prevented through physician to physician communication. Furthermore, hospital visits and stays can possibly be eliminated through preemptive monitoring and overall improved care for chronic conditions. More so, emergency room visits can possibly be eliminated. Those in rural communities or with limited funds may utilize the emergency room as their first and only method to manage their condition. This form of management is very costly for society and also overall inefficiently provides care to society as a whole. Finally, the patient may not be receiving optimal care as

they are seeing a new and different provider with each occasion. The financial implications of this route of medical management and fragmented care have a cyclically negative effect on increasing healthcare costs for society as the emergency room visits are more costly, uncoordinated care leads to poor management for chronic conditions and ultimately could lead to more frequent and extended hospital visits in which the cycle continues upon discharge.

While all of these benefits to telehealth are substantial and impactful, there are also several security risks associated with telehealth. Risks include the amount of potential entryways for hackers as the ability to control all access points to receipt, transmission and storage of data is limited. Any application located or accessed from a smartphone has the potential for third party access which can be anyone even those with malicious attempts. In addition, virtual physician visits require an extra level of security in accessing a portal unit or videoconferencing system to communicate with the physician. The physician must ensure that the person they are communicating with is truly the intended patient. Another concern is with remote monitoring and its potential to overstep the bounds of privacy in monitoring the patient and gathering unintended information such as substance abuse issues or other private issues which the patient intended to remain private. An excess of security controls could negate the ability for access from those individuals that benefit the most from its convenience and availability.

Finally, the use of telehealth could actually lead to fragmented healthcare. Examples include a patient that is primarily relying on telehealth for physician visits. This patient could potentially slip through the cracks in receiving needed face-to-face visits and medication oversite. Additionally, they could end up receiving overlapping and unnecessary medical treatment, care and medications without appropriate coordination of care by a primary provider.

As telehealth breaches and breaches in additional consumer areas become more and more mainstream and reported, the consumers for telehealth technologies may become less and less trusting of the use and ability of the technologies to protect their privacy. In turn, the patient may withhold information or selectively use the services further negating the benefits and leading to overall fragmented care for the patient.

Additionally, the use of telehealth technology can be costly to implement and train employees on use and security controls. The security controls needed for the use of this technology can also be costly such as encryption controls, access monitoring and device management such as mobile phone use and management and the possibility of bring your own device controls. Education and training can be costly to employees as well as patients. Patients will need to be adequately trained on how to access the telehealth technology as well as transparent communication regarding their own part in the process for vigilantly monitoring and safeguarding their privacy and protection. Finally, costs related to any breaches can have long-term effects for the patient whose data was stolen, the business entity and society as a whole.

Alternatives/recommendations to address the issue

Recommendations for proper management of telehealth technology to balance the benefits from this technology use with the associated risks begins with a thorough risk analysis. The risk analysis should begin with an assessment and identification of all devices and methods used to capture, transmit and store protected health information (PHI) and electronic protected health information (ePHI) data. Next, the organization will want to monitor how data is collected. Within this analysis, the organization should extend its analysis beyond the surface level of the videoconference that occurs during a virtual appointment or the monitoring device but through each level regarding where and how the data transmits from this initial entry point to the final delivery point and all potential access channels at all levels. One recommendation specific to telehealth use is for a more comprehensive approach during this phase as there may be multiple areas of entry associated with business associates and vendors as well as the data collection and device use by the patient.

In the next phase, again the recommendation is for a very extensive approach to assessing all potential threats and vulnerabilities associated with the telehealth technology. As an example, if a patient or provider is utilizing a smartphone device to transmit data, then the vulnerabilities for hacking data are numerous. If the telehealth technology is an application, then there is a clear vulnerability in how the application is monitored and any potential third party access.

When the organization assesses their current security controls for telehealth technologies they should actually go through multiple levels of testing the telehealth methodology to thoroughly evaluate the control mechanism. This step should be frequent and ongoing. Every time there is any change in any software or hardware component the security controls will need to be reevaluated. Thorough testing at all phases will enable an extra level of analysis for vulnerabilities, loopholes and unsecured access points. Additionally, encryption techniques can be assessed by sending test data outside the system and determining if that test data is protected. Furthermore, access control logs can be assessed as testing occurs through a test hack or break in the system. Internal or contracted security personnel can employ a thinking outside the box analysis to act as potential hackers in testing their ability to improperly access test data to ensure that current security control mechanisms are providing thorough protection. Possible biometric means to serve as login procedures can be tested as a methodology for ensuring that the correct patient is logging in and utilizing the technology.

In determining the likelihood of vulnerabilities with any telehealth technology often obtained in part or wholly by outside vendors, the organization will want to evaluate the vendors breach history before entering into any contractual relationship with the vendor. If there are previous incidents in the vendor's past, the primary healthcare organization may stipulate more extensive security control mechanisms be set in place as a stipulation to entry into any contract. Furthermore, the breach policy will also need to be thoroughly evaluated with the vendor to ensure that liability for any incidents are shared liabilities. This shared responsibility will help ensure a shared goal for privacy protection and implementation of security controls.

Another recommendation is clear and extensive documentation as well as frequency of performing ongoing risk analysis. This step cannot be understated with the use of telehealth technologies, but for some organizations can actually be an area which is under assessed as these technologies are oftentimes seen as adjunct techniques for the healthcare organization.

Telehealth technology falls under the guidelines set within the Health Insurance Portability & Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH Act). However, "healthcare laws, reimbursement policies, and privacy protection rules struggle to keep up with this fast-growing industry" (AMA Journal of Ethics, 2014, Privacy and security concerns in telehealth) [4]. As with multiple areas covered under these policies, the recommendations are not clearly stated and are open to interpretation for the specific use and function of the healthcare entity. As such, with the risks for using telehealth technologies tipping the scale, the interpretation for these mandates should lean more towards a fine and detailed interpretation versus a broad interpretation. Additionally, state and regional laws should be thoroughly assessed and also finely translated to ensure that there are no security loopholes associated with the use of this technology.

Conclusion

Since the inception of teleradiology in 1948, the use of telehealth has truly evolved. In 2010, the Centers for Medicare & Medicaid Services (CMS) recognized the use of telehealth and the data obtained from it as meaningful use increasing the reimbursement from using this technology. This support was further backed when "the Health Resources and Services Administration received $16 million in 2016 to expand access to telehealth services in rural areas" (InTouch Health, 2019, A brief history of telehealth, para. 10) [5].

While the use of telehealth technologies will continue to evolve and continued research will need to be conducted to further assess the societal benefits, the need for extra vigilance and extensive security control mechanisms will also continue to evolve. As with all technologies, they should never be thought of as a one-time event or a one and done setup but as a continued evolution and process to achieve improved outcomes and improved safety controls. If an organization can truly achieve and maximize their security control mechanisms, then they can reap the extensive benefits for using telehealth technologies. When these two juxtapositions of benefits and risks are evaluated effectively by the healthcare organization, then the chosen telehealth technology can be effectively used to achieve improved outcomes and patient satisfaction within the organization while still maintaining adequate and necessary privacy protection to the consumer's data [6-15].

Bibliography

1. Mayo Clinic. "Telehealth: Technology meets healthcare" (2017).
2. Center for Connected Health Policy. "About telehealth" (2019).
3. US National Library of Medicine National Institutes of Health. "The impact of telehealth on the quality and safety of care: A systematic overview" (2013).
4. AMA Journal of Ethics. "Privacy and security concerns in telehealth" (2014).
5. InTouch Health. "A brief history of telehealth" (2019).
6. Agora. "Telehealth could be the answer to the healthcare crisis" (2018).
7. American Journal of Managed Care. "Leveraging remote behavioral health interventions to improve medical outcomes and reduce costs" (2015).
8. EVisit. "History of telemedicine" (2018).
9. EVisit. "10 pros and cons of telemedicine" (2018).
10. Global Journal of Medical Research. "Advantages and challenges to using telehealth medicine" (2015).
11. HealthIT. "Telemedicine and telehealth" (2017).
12. Health Resources and Services Administration. "Telehealth programs" (2019).
13. National Academy of Sciences. "The evolution of telehealth: Where have we been and where are we going?" (2012).
14. SAGE Journals. "Telehealth: A balanced look at incorporating this technology into practice" (2018).
15. 24By7 Security. "Security and privacy for telemedicine" (2016).