To: Carole Johnson (Administrator of HRSA)

From: Rachel Freundlich

Date: July 23, 2023

Re: Ensuring Privacy and Confidentiality for Patients Using Telehealth

Statement of Issue: What policy should be implemented to ensure patient confidentiality when using Telemedicine?

Medicine has adopted technology in many ways to improve its services, treatments, and care. One of the ways in which technology is changing the forefront of medicine is the relatively recent implementation of telehealth. Sessions can occur over a web-based platform that allows the patient and provider to see each other, discuss the issues at hand and develop health improvement and treatment plans. However, this poses a threat to the privacy of patients. Whereas appointments used to take place in an office designated for these matters, providers can now conduct these sessions from home. Furthermore, the development of Electronic Medical Records presents the issue of healthcare workers carrying around private information regarding their patients on their own cell phones and home computers. It is imperative that extensive measures are put in place to prevent patient's information from becoming exposed and to ensure patients that their private health information is just as secure as it was before technology was an integral part of medicine and healthcare.

- **American hospitals are becoming increasingly reliant on telemedicine** with 76% of US hospitals reporting using a form of telemedicine to interact with patients[1]. Providers use this form of medicine to strengthen the patient-provider relationship and improve communication.
- **Patients can not confirm their identity** when using audio services and messaging during appointments. Although confirming the patient's identity at the beginning of each visit is outlined in the official guide from the HHS[2], this is challenging when appointments are audio and showing a photo ID is not possible.
- **Standard communication apps such as FaceTime and Zoom are permitted to use for appointments.** These interfaces do not comply with HIPAA requirements and can not be relied upon to store data securely. This compromises the privacy of patient information. Post COVID-19, providers are required to transition to secure platforms, however this has not been fully implemented at this time[3].
- **PHI is stored electronically on various platforms and can be accessed from private devices** which can compromise patient privacy. Patient files are liable to be read by third parties and others not entitled to the information.
- **During the COVID-19 pandemic, the use of telehealth increased tremendously.** However, certain populations in need of medical attention are reluctant to utilize this resource. Adolescents, elderly and individuals struggling

with mental health are weary of confidentiality and hesitant to share private information through online platforms[4].

Landscape

Defining stakeholders is critical in order to properly implement a new policy. Successfully instituting a new policy to improve patient confidentiality in Telemedicine requires collaboration of many groups. In order to enact new policy, the federal government and policymakers must successfully pass policy. For state mandated policies, each state government must recognize the need for new policy. However, they must partner with the clinicians, Insurance companies, federal health agencies, communications technology companies, and patient associations. Each of these groups represents important players in Telemedicine, ranging from those practicing medicine, receiving care, providing funding, providing reimbursement and providing the technological services necessary to successfully utilize Telemedicine.

Policy Options

- A state mandate regulating electronic medical records to be accessed through servers that are secure and protected through a multi-step verification process. This would protect patient information from lingering on a provider's private desktop. Enforcing a strict verification policy would ensure patient confidentiality when information must be accessed on private devices during Telehealth sessions.
    - ***Advantages***: Instituting a multi-step verification process to view patient medical records will limit access. Storing patient files in this manner should not be challenging to implement as most medical services have this system in place for company-owned devices. 66% of patients in a study reported that they were concerned about the privacy of their personal medical information[5]. This would be one way of addressing this concern. Each state would determine for itself how to fund the implementation of this policy, and therefore the composition of each state would be taken into account.
    - ***Disadvantages***: These servers would cost money to install and it would need to be determined where this money would come from. Medical offices would either increase the cost of their services to insurance companies or patients to cover these funds[6]. Alternatively, this would negatively impact provider salaries. Implementing this would take time as each clinic and private office determined how they would fund this.

May be inconvenient for providers who need to access information quickly during appointments.

- A federal mandate requiring providers to log on to virtual and audio appointments through a specified server/app with data protection and end-to-end encryption. This would prevent conversations and appointments from occurring over regular cell phone calls and digital platforms. It would be necessary for providers to connect to private wifi to utilize these services.
    - ***Advantages***: Requiring providers to be connected to a private wifi when conducting appointments ensures that providers will not be in public areas during the appointment. This may assure patients that although they are not in the same room as their provider, their conversation is just as private and protected. Secure platforms that use end-to-end encryption will add an extra layer of security[7]. Using a platform that is only accessed through password protected wifi will force the provider to be in a private setting. This may also increase the audio/visual connection as the service would be more reliable and better supported to fill this purpose.
    - ***Disadvantages***: Requiring providers to use certain platforms would limit those who can use telemedicine. Some providers may not always be able to connect to private wifi which would limit the available time providers can meet with patients. Furthermore, if the app requires that both patient and provider connect through the app this will limit the patient population that can benefit from its services.
- A federal mandate requiring providers to conduct appointments from either an official office or a recognized home office. This would ensure that appointments occur in a private location. Providers would be allowed to rent office space or designate a private room for sessions.
    - ***Advantages***: Patients would be reassured that their appointments were private and not taking place in public settings. The Department of Human Services "expects healthcare providers" to conduct appointments in a private setting[8]. However, this is not a requirement. Mandating a private setting would alleviate patient concern. Relatively simple to incorporate into policy as most clinicians already work within an office setting.
    - ***Disadvantages***: May be difficult to enforce. It may not be possible to confirm the provider's locations during the appointment. May limit provider availability by limiting the location they can conduct appointments. This does not require patients to be in private locations at the time of the meeting. This can risk patient confidentiality and increases the risk of the conversation being overheard.

Policy Recommendation: With the increasing use of Telemedicine across the country, it is crucial to implement new policy to increase patient confidentiality and improve patient satisfaction. Because this is a federal concern, it would be most appropriate for the federal government to enact a policy requiring providers to conduct appointments from recognized private spaces. As mentioned above, this alleviates the concern that providers can conduct appointments from public locations. Although this may limit provider availability, appointments typically take place during a provider's typical work day. It would be assumed that the provider is already in their official office and therefore it should not be problematic to enforce this policy. Furthermore, if a provider typically works remotely, they will likely already have a designated room for work to comply with other HIPAA standards. Although patients are not required to be in private settings, providers can encourage patients before the appointment to ensure they have access to a private area.

Sources:

1. Hyder MA, Razzak J. Telemedicine in the United States: An introduction for students and residents. *Journal of Medical Internet Research*. 2020;22(11):e20839. doi:https://doi.org/10.2196/20839

2. Protecting patients' privacy | Telehealth.HHS.gov. telehealth.hhs.gov. Accessed July 24, 2023. https://telehealth.hhs.gov/providers/best-practice-guides/telehealth-for-behavioral-health/preparing-patients-for-telebehavioral-health/protecting-patients-privacy#:~:text=Confirm%20the%20patient%27s%20identity%20at

3. Telehealth for providers: What you need to know - centers for Medicare ... Accessed July 24, 2023. https://www.cms.gov/files/document/telehealth-toolkit-providers.pdf.

4. Houser SH, Flite CA, Foster SL. Privacy and Security Risk Factors Related to Telehealth Services – A Systematic Review. *Perspectives in Health Information Management*. 2023;20(1):1f. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9860467/

5. Hale TM, Kvedar JC. Privacy and Security Concerns in Telehealth. *AMA Journal of Ethics*. 2014;16(12):981-985. doi:https://doi.org/10.1001/virtualmentor.2014.16.12.jdsc1-1412.

6. Snoswell CL, Taylor ML, Comans TA, Smith AC, Gray LC, Caffery LJ. Determining if Telehealth Can Reduce Health System Costs: Scoping Review. *Journal of Medical Internet Research*. 2020;22(10):e17298. doi:https://doi.org/10.2196/17298

7. Koster P, Asim M, Petkovic M. End-to-end security for personal telehealth. *Studies in Health Technology and Informatics*. 2011;169:621-625. Accessed July 24, 2023. https://pubmed.ncbi.nlm.nih.gov/21893823/

8. *FAQs on Telehealth and HIPAA during the COVID-19 Nationwide Public Health Emergency*. https://www.hhs.gov/sites/default/files/telehealth-faqs-508.pdf