URGENT TELEHEALTH IMPLEMENTATION

Edafio Guidance for adopting Telehealth solutions in response to COVID-19

Published March 19, 2020 by Edafio Healthcare and Cybersecurity Consulting Teams

INTRODUCTION

On March 13, 2020, President Trump announced an emergency declaration under the Stafford Act and the National Emergencies Act. Consistent with the emergency declaration, the Centers for Medicare and Medicaid Services (CMS) underline expanded Medicare's telehealth benefits on March 17, 2020. In turn, many state based insurance providers are following suit, including Arkansas Medicaid.

In addition, the Office for Civil Rights (OCR) announced on March 17, 2020,

> *"effective immediately, that it will exercise its enforcement discretion and will waive potential penalties for HIPAA violations against health care providers that serve patients through everyday communications technologies during the COVID-19 nationwide public health emergency."*

Read their full guidance at HHS.gov.

This expansion of coverage and temporary regulatory relief provides flexibility for Healthcare Providers to increase their telehealth activity. There by helping to ensure that all Americans—particularly high-risk individuals—have access to care and benefits that can help keep them healthy while helping to contain the spread of novel coronavirus COVID-19.

However, this journey is not without areas of concern that organizations need to consider and address to protect your organization and your patients. This guide will assist you in making the best decision in implementing telehealth while considering the protection of patient information from intentional or unintentional uses and disclosures.

ADDRESSING CONCERNS

It's crucial to realize that while your telehealth patient care needs are urgent and near-term, the implementation of a telehealth solution presents some challenges that organizations must rapidly consider. What are your obligations regarding Patient Privacy, potential telehealth impacts to billing, patient medical records, and what happens if you use this on a long-term basis?

HIPAA Privacy Rule and Patient Notifications

Patient Privacy Notification - When using non-HIPAA compliant telehealth platforms, providers are encouraged to notify patients that third-party applications potentially introduce privacy risks, and providers should enable all available encryption and privacy modes when using such applications. A waiver has been put in place for certain HIPAA Privacy provisions, but the HIPAA Privacy rule has not been suspended.

We want to ensure care is accessible to all patients during this emergency, but covered entities must still implement reasonable safeguards to protect patient privacy.

EMR Record Accuracy

Chief among these are the need to capture patient care notes within the EMR to ensure their medical record is updated and to enable accurate billing.

Templates – Whether using your EMR or an alternative telehealth solution. Our recommendation is to utilize visit templates to accurately capture and maintain integrity of the patient's medical record. *If using an alternative solution, this might involve printing out your own template.*

Long-Term Adoption - Once your providers adopt and adapt to a telehealth solution they may want to use it far beyond the current pandemic response. At some point in the future the solution will need to be HIPAA compliant once the current enforcement guidance is reverted.

IDEAL IMPLEMENTATION

In taking the long view it is our recommendation that your telehealth solution be part of your EMR partner's solution set or at bare minimum tightly integrated into your EMR via a software interface (e.g., API). Utilizing your EMR's telehealth solution will ensure long term HIPAA compliance and an easier workflow transition.

Some EMR examples that currently offer telehealth include

- Epic: MyChart
- eClinicalWorks: Healow App
- Modernizing Medicine
- e-MDs: UpDox
- Athena: NextPatient

If an EMR integrated solution is unavailable or is impractical for accelerated implementation, please see our alternative recommendations below.

ALTERNATIVE RECOMMENDATIONS

Healthcare Providers types and sizes vary widely so we want our guidance to be timely and action-able for each of our healthcare partners. Edafio associates are available to assist in quickly getting this set up and running smoothly for you so that your patient's and staff's safety are of top priority. The following recommendations provide solutions that could be used on a long-term basis but are easier to deploy on an ad-hoc basis.

Medium to Large Practice Recommendations

Doxy – Doxy.me offers an easy to use and healthcare focused telemedicine solution that ranges from $35 per month for individual providers to $450 a month for a clinic version (for 10 providers). You can review their Healthcare Features. They are HIPAA compliant with end-to-end encryption and a signed BAA.

Zoom – Zoom.us/Healthcare offers an easy to use video conferencing solution that is high-quality and HIPAA compliant for $200 a month for 10 hosts. (Hosts would be providers). For details on their Healthcare offering we'd recommend reviewing their Healthcare Datasheet, they also offer a guide to their HIPAA Compliance.

Microsoft Teams – Microsoft Teams offers an enterprise class audio/video conferencing solution for healthcare providers that is HIPAA compliant. They are offering the full product free for six months. Read more about its integration with healthcare on this blog post.

Small Practice Recommendations

Many of us use a variety of texting and video apps in our personal lives, but precious few offer some basic level of encryption and privacy, so we recommend providers thoughtfully consider the.following apps. However, certain aspects of these should be considered prior to using them on an ad-hoc basis.

Two Important Notes

Pro: All the apps we list support end-to-end encryption. This means that all messages, audio, and video is scrambled in a way the prevents anyone other than the intended recipient from being able to view the message or video. This prevents eavesdropping by any Third Party, including the application developer.

Con: All of these apps require mobile phone numbers. Providers should be mindful that exposing their direct or personal number during a time of increasing infections and uncertainty could lead to patients calling or texting the provider at will. This could impact times of rest and could overwhelm the usefulness of the app as a method of patient care.

Encrypted Communication Apps

• **Apple FaceTime** – FaceTime is a video chat function of all iPhone & iPad devices. It's easy to use and well known. However, it does not support Android devices which limits the patient population that could utilize it.

• **Signal** – Signal is seen as the gold standard for communication apps. It's free and supports a wide variety of devices (e.g., iPhone, Android) including Windows computers. It traditionally hasn't been as well-known as WhatsApp.

• **WhatsApp** – Global communication platform, encrypted by the people who make Signal, and supports a wide variety of devices (e.g., iPhone, Android) including Windows computers. It's owned by Facebook, but the encryption gives it a level of trust and confidence beyond Facebook Messenger

AVOID THESE

The Office of Civil Rights also specifies that Facebook Live, Twitch, TikTok, other public-facing video communication **"should not be used in the provision of telehealth."**

Edafio would strongly advise to avoid Facebook Messenger as well. It is not encrypted by default and is very susceptible to patient impersonation and social engineering/hacker activities.

IN CONCLUSION

Edafio recognizes how critical these solutions are to taking care of patients in this especially trying period. If you have questions regarding telehealth, Healthcare practices, Cybersecurity concerns, or need help supporting your staff and technical environment Edafio is here for you.

We're proud to be a partner and advocate for Healthcare in the state of Arkansas and that is even more true today. Thank you for what you are doing for all of us.Call us at **501.222.4100** or visit us online at Edafio.com.