



Our Risk Management Team is here to help you minimize and mitigate Medical Professional Liability risk.



## HIPAA Compliance in Telehealth After the Pandemic

The COVID-19 pandemic created a vital need for increased availability of telehealth services nationwide. As a result, the U.S. Department of Health and Human Services (DHHS) Office of Civil Rights (OCR), charged with enforcing HIPAA Rules, announced in March that it will exercise enforcement discretion during the declared public health emergency (PHE). As part of this discretion, DHHS reported it will not impose penalties for HIPAA noncompliance when physicians and other health care professionals act in good faith to provide telehealth services using any non-public facing audio or video chat applications. Non-public facing applications include Apple FaceTime, Facebook Messenger, Google Hangout, and Skype. Public facing applications, such as Facebook Live, Twitch, and TikTok, should never be used for telehealth services. The OCR noted that health care practices seeking additional privacy protections for video telehealth services should provide such services through technology vendors that are "HIPAA compliant" and able and willing to sign a HIPAA business associate agreement (BAA). The OCR lists potential vendors that claim to meet both conditions, but the agency noted that it does not endorse or certify any of them.<sup>[ii]</sup>

The OCR has not specified an expiration date, but simply says "[it] will issue a notice to the public when it is no longer exercising its enforcement discretion based upon the latest facts and circumstances."<sup>[iii]</sup> It is unclear how closely this will follow the end of the declared PHE, but physicians and practices planning to continue telehealth services after the PHE expires should look now for a HIPAA compliant vendor able and willing to sign a BAA. According to the Arizona Telemedicine Program, "If you're a provider already using a HIPAA-compliant platform, keep using it! And if you're starting services and you *can* use a HIPAA-compliant platform, *do* – you're going to have to move to one after the PHE is over anyway."<sup>[iiii]</sup>

### What is HIPAA Compliant?

Selection of a vendor who will sign a BAA is an indispensable component of creating a HIPAA compliant telehealth program, but technology alone cannot make you HIPAA compliant. Before you select a software vendor, learn what the HIPAA Privacy, Security, and Breach Notification Rules require you to do to ensure the confidentiality and integrity of your patients' protected health information (PHI). These are the basics:

- HIPAA requires practices to protect PHI integrity by using a system of secure communication with only authorized users.
- Practices must complete and document a security risk analysis of the storage and movement of PHI through the practice. The practice must address vulnerabilities identified in this analysis in order to decrease the risk of breach.<sup>[iv]</sup>
- The HIPAA Security Rule requires practices to implement administrative, physical, and technical controls to safeguard electronic PHI by protecting against disclosures and threats to the security of the information.<sup>[v]</sup>
  - Administrative safeguards include staff training and contingency planning for emergencies that damage electronic systems.<sup>[vi]</sup>
  - Physical safeguards focus on securing access to the practice's physical structures and electronic equipment.<sup>[vii]</sup>
  - Technical safeguards include procedures to limit access, verify the identity of those with access, and encrypt information transmitted over a network. Practices must maintain and periodically review activity logs of all systems containing PHI. Unauthorized access must be reported and corrected. Practices are also required to create policies to protect PHI from alteration/destruction.<sup>[viii]</sup>
- Documentation of HIPAA compliance activities, generally in the form of policies and procedures and other documentation of required actions and assessments, is essential and must be retained for 6 years.<sup>[ix]</sup> This is distinct from the required or recommended periods for retention of *patient medical records*.
- The type and extent of security measures implemented can vary depending, in part, on the size, complexity, and capabilities of a particular practice.<sup>[x]</sup>

### Selecting a Software Vendor

Understanding the HIPAA Rules and compliance requirements prepares the practice to select a software vendor. Some vendors market their software as "HIPAA Compliant," but the OCR and other enforcement agencies do not "certify" or otherwise vet vendors. Security features vary widely among vendors, so practices contemplating telemedicine should undertake a careful selection process to ensure the company offers the required security measures. To comply with the Rules, require the vendor to sign a BAA documenting how it will protect PHI.<sup>[xi]</sup> The HHS website provides guidance on sample BAA provisions.<sup>[xii]</sup> Consider the following when selecting a vendor:

- Ask vendors to put in writing their administrative, physical, and technical safeguards.
- If you have an electronic medical record (EMR), ask your vendor if a telehealth function is available. Otherwise, evaluate how smoothly a vendor's product will integrate with the current EMR or other technologies the practice uses.
- Consider how user friendly the platform is for both clinicians and patients, especially if the practice has a patient population that may not be tech savvy. Ask for a demonstration prior to purchasing.
- Evaluate the quality of the vendor's customer service including availability of training and troubleshooting.
- Even with a BAA in place, the practice must perform and document due diligence to verify HIPAA compliance.
- Utah Medicaid requires participating physicians and other health care professionals to use a HIPAA compliant means of communicating (i.e., Skype for Business, Updox, VSee, Zoom for Healthcare, Doxy.me, Google G Suite Hangouts Meet) to the greatest extent possible during the COVID-19 emergency.<sup>[xiii]</sup>

MICA's Senior Risk Management Consultants are available to help you with questions or concerns. You are welcome to call or email our Hotline at 800.352.0402 x2137, 602.808.2137, or [rm\\_info@mica-insurance.com](mailto:rm_info@mica-insurance.com).

### HIPAA Resources

1. HIPAA Rules, compliance, and enforcement information <https://www.hhs.gov/hipaa/for-professionals/index.html>
2. American Medical Association HIPAA Privacy and Security Rules guidance <https://www.ama-assn.org/practice-management/hipaa/hipaa-privacy-security-resources>
3. American Medical Association: *HIPAA Privacy and Security Toolkit* <https://tbhcoe.matrc.org/wp-content/uploads/2018/07/HIPAA-Toolkit.pdf?189db0&i189db0>
4. American Telemedicine Association: *Quick-Start Guide to Telehealth* <https://info.americantelemed.org/covid-19-resources-quickstart-guide-landing>
5. The Office of the National Coordinator for Health Information Technology: *Guide to Privacy and Security of Electronic Health Information* <https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf>
6. National Consortium of Telehealth Resource Centers: *HIPAA and Telehealth a Stepwise Guide to Compliance* <https://www.telehealthresourcecenter.org/wp-content/uploads/2019/07/2019-HIPAA.pdf>
7. Southwest Telehealth Resource Center webinar: *Reving Up Your Telemedicine Practice in the Time of COVID* <https://swtrc.wistia.com/medias/fwcw1c3hyn?wtime=1m14s>

### Telehealth Resources

1. American Medical Association: *Telehealth Playbook* <https://www.ama-assn.org/system/files/2020-04/ama-telehealth-playbook.pdf>
2. Arizona Medical Association COVID-19 Telemedicine page (including information on partnership with CompuGroup Medical for free six month subscription to a telemedicine platform and Telemedicine Guidance for Arizona Physicians) <https://www.azmed.org/page/COVID19Telemedicine>
3. Arizona Telemedicine Program: *Telemedicine Checklist* <https://telemedicine.arizona.edu/blog/telemedicine-checklist>
4. CMS: *General Provider Telehealth and Telemedicine Toolkit* <https://www.cms.gov/files/document/general-telemedicine-toolkit.pdf>
5. DHHS Telehealth <https://telehealth.hhs.gov/providers/>
6. Mid-Atlantic Telehealth Resource Center: *Resources for COVID-19 Toolkit* (nationwide applicability) <https://www.matrc.org/matrc-telehealth-resources-for-covid-19/>
7. National Organization of State Offices of Rural Health: *Telehealth Technologies and Preparing to Select a Vendor* <https://nosorh.org/wp-content/uploads/2016/11/NOSORH-Telehealth-Vendor-Fact-Sheet-FINAL.pdf>
8. National Telehealth Technology Assessment Resource Center: *Clinician's Guide to Video Platforms* <http://telehealthtechnology.org/toolkit/clinicians-guide-to-video-platforms/>
9. University of Arizona Telemedicine Program and Southwest Telehealth Resource Center for Arizona, Utah, Colorado and Nevada <https://southwesttrc.org/>
10. Utah Department of Health telehealth resources <https://coronavirus.utah.gov/telehealth/>
11. Utah Medical Association telehealth resources [https://utahmed.org/WCM/COVID-19/Telehealth\\_and\\_Other\\_Info/wcm/ContentAreas/Landing\\_Pages/COVID/Telehealth\\_and\\_Other\\_COVID-19\\_Info.aspx?hkey=41b85f80-agd6-4123-853a-252c6317ae71](https://utahmed.org/WCM/COVID-19/Telehealth_and_Other_Info/wcm/ContentAreas/Landing_Pages/COVID/Telehealth_and_Other_COVID-19_Info.aspx?hkey=41b85f80-agd6-4123-853a-252c6317ae71)

[ii] <https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html>

[iii] <https://www.hhs.gov/hipaa/for-professionals/faq/3020/when-does-the-notification-of-enforcement-discretion-regarding-covid-19-and-remote-telehealth-communications-expire/index.html>

[iiii] <https://telemedicine.arizona.edu/blog/pandemic-silver-lining-federal-telehealth-regulations-relaxed-least-now>

[iv] 45 CFR § 164.308(a)(1)(iii)(A)(B)

[v] 45 CFR § 164.306

[vi] 45 CFR § 164.308(a)

[vii] 45 CFR § 164.310

[viii] 45 CFR § 164.312 & 45 CFR § 164.308(a)(1)(ii)(D)

[ix] 45 CFR § 164.316

[x] 45 CFR § 164.306(b) & (d)

[xi] 45 CFR § 164.308(b)(3) and 45 CFR § 164.314(a)

[xii] <https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html>

[xiii] <https://utahmed.org/docs/COVID/UDOH%20Telehealth%20Guidance%204%206%202020.pdf>

Customer Service 877.215.MICA (6422)

VISIT OUR WEBSITE

FOLLOW US



Questions? Contact us today 1.800.352.0402

Having trouble viewing this email? [Click here](#) to view the web version.