# Telemedicine Cybersecurity Guidance

The Department of Health and Human Services (HHS), the Food and Drug Administration (FDA), and Centers for Disease Control and Prevention (CDC) have all started promoting use of telemedicine in response to the COVID-19 pandemic. At the same time the Office of Civil Rights (the enforcement arm of HHS) issued a "Notification of Enforcement Discretion for Telehealth…" indicating OCR would exercise discretion and will not impose penalties for noncompliance with regulatory requirements under the HIPAA Rules in connection with telehealth **during the COVID-19 emergency**.

So, what does this all mean and what concerns are important when implementing a telemedicine solution?

While all the regulations making up HIPAA still apply (even if relaxed) and a good faith effort should be made to be compliant during the emergency, we recommend the following areas be addressed before implementing any telemedicine solution.

## Guidance

- HIPAA Privacy Agreements may be needed for patients.
- The chosen vendor will need to sign a Business Associate Agreement.
- Only authorized users should have access to ePHI and telemedicine solution.
- The telemedicine solution must utilize encryption end-to-end.
- Stored recordings must be encrypted and retained inside a HIPAA environment.
- Identity verification is required for provider-side and patient-side.
- Avoid public facing applications like Facebook Live, TikTok, Twitch or similar applications.

HHS provided the following solutions as vendors that represent their solutions as HIPAA compliant:

- Skype for Business / Microsoft Teams
- Updox
- VSee
- Zoom for Healthcare
- Doxy.me
- Google G Suite Hangouts Meet
- Cisco Webex Meetings / Webex Teams
- Amazon Chime
- GoToMeeting
- Spruce Health Care Messenger