Whittaker, Jetta L (HSS)

From: Office-JNU-HSS-SDS E-News (HSS sponsored)
Sent: Monday, April 13, 2020 2:49 PM
To: Office-JNU-HSS-SDS E-News (HSS sponsored); sds-e-news
Subject: SDS E-Alert: HIPAA and Updated Telehealth Remote Communications During the COVID-19 Emergency Declaration
Attachments: february-2020-hipaa-and-novel-coronavirus.pdf

April 13, 2020

SDS E-Alert: HIPAA and Updated Telehealth Remote Communications During the COVID-19 Emergency Declaration

SDS would like to pass along this updated emergency notice from the U.S. Department of Health and Human Service about appropriate HIPPA compliant telehealth remote communications during the COVID-19 National Public Health Emergency. This updated emergency notice can be found at: https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html

The original guidance, issued in February 2020, is attached or can be found at: https://www.hhs.gov/sites/default/files/february-2020-hipaa-and-novel-coronavirus.pdf

In short, this recently updated emergency notice says:

- Providers may use non-public facing remote communication products to contact clients;
- The Office of Civil Rights is using discretion on HIPAA compliance as long as good faith efforts are employed during the COVID-19 national health emergency;
- This applies to telehealth provided for any reason, not just the diagnosis and treatment of health conditions related to COVID-19;
- Health care providers may use popular applications that allow for video chats, including Apple FaceTime, Facebook Messenger video chat, Google Hangouts video, Zoom, or Skype, to provide telehealth without risk that OCR might seek to impose a penalty for noncompliance with the HIPAA Rules during the emergency;
    - Guidelines for use
        - Take action to avoid showing/sharing information unnecessarily
        - Be aware of who is in the surrounding area
        - Do not text or request HIPAA information

        - notify clients that these third-party applications pose privacy risks, and providers should enable all available encryption and privacy modes when using such applications.58
- Providers CANNOT USE public facing aps like Facebook Live, Instagram Live, Snapchat Twitch, TikTok, and similar video communication applications.