Jim Thomas City of Hope - How to Protect Patient Information in the Era of Telehealth

RANCHO MISSION VIEJO, CA, USA, July 28, 2020 /EINPresswire.com/ -- Innovations in telehealth and other digital practitioner-to-patient communications offer promising solutions to the challenges facing today's health care delivery.


Jim Thomas City of Hope

However, these technologies also carry inherent risk - especially when it comes to patient privacy and PHI. Jim Thomas City of Hope explains. "While COVID-19 has certainly jumpstarted the launch of telehealth as an everyday convenience, the idea of digitizing healthcare has been slowly taking hold for years."

And while the realm of healthcare seems to be years behind other industries in the digitization of records and other normal practices, Jim Thomas City of Hope believes there are security reasons behind that pace.

"HIPAA regulations require health care professionals to protect patient information first. They don't care if it causes inefficiency - and that's how it should be," says Jim Thomas City of Hope. "But now the pandemic means we have to find workarounds. And those workarounds aren't always perfect from a security standpoint."

FaceTime, Google Duo, Zoom calls - these are all platforms that doctors have used to communicate with their patients remotely. "Most of us don't think twice about it - we have virtual meetings all day long," says Jim Thomas City of Hope. "But these digital connections aren't anywhere near as private as an in-person conversation with your doctor."

While FaceTime and Google Duo are relatively safe, Jim Thomas City of Hope says they're still

open to hacking. All video streaming services face the possibility. It's much less likely in a direct phone call format, but it is possible. Zoom and Skype calls have recently come under fire for their security breaches while solutions like MS Teams are built on platforms that are entirely HIPAA compliant.

Teachers holding classes had unexpected drop-ins from uninvited guests - some of whom shouted obscenities, played pornographic content, or started spouting racist propaganda. This also happened in business meetings.

"To be fair, many of the 'call bombing' problems came from a lack of education and knowledge on the user end," says Jim Thomas City of Hope.
"They weren't setting their meetings to 'Private.' But that brings up questions about the security of patient information on all ends. What policies can doctors and healthcare facilities put in place to protect patient information, and what responsibility do they have to educate us as the end-user?" asks Jim Thomas City of Hope.

"Security is a feedback loop, not a one-way street. Everyone has to be involved," explains Jim Thomas City of Hope.

There are many telemedicine companies who are addressing these kinds of security issues with specially designed video conferencing platforms that integrate with patient information platforms. These companies promise closed-circuit sessions are completely private. "The possibilities of telehealth are so exciting," enthuses Jim Thomas City of Hope. "We just have to make sure we don't sacrifice our privacy by moving forward too quickly."

Caroline Hunter
Web Presence, LLC
+1 786-233-8220
email us here
