HIPAA and Telehealth

Background

The Health Insurance Portability and Accountability Act of 1996, or HIPAA, is a health privacy law that protects personal health information. HIPAA only covers certain groups: health plans, health providers, health care clearing houses, and business associates. With the transition to telehealth and other means of electronically communicating with patients during the COVID-19 pandemic, new and complex privacy and security issues have arisen.

Key Legal Concerns

A primary concern for HIPAA-covered entities is what to do if sensitive health care data is intercepted by or made available to a third party. Many telehealth appointments are conducted over Zoom, so the possibility of security vulnerabilities in the software raises concern for providers. The U.S. Department of Health and Human Services' Office for Civil Rights released a Frequently Asked Questions document, where they state that covered providers will not be subject to penalties for breaches of HIPAA rules if they "occur in the good faith provision of telehealth during the COVID-19 nationwide public health emergency.[1]"

This does beg the question: what falls under "good faith provision?" If an organization or provider does not take some precaution that would prevent third parties from accessing patient data, are they still acting in good faith even though they may not have been aware of the vulnerabilities? For example, if a health care provider uses the "Zoom for Healthcare" package

1. U.S. Department of Health and Human Services Office for Civil Rights, FAQs on Telehealth and HIPAA during the COVID-19 nationwide public health emergency, https://www.hhs.gov/sites/default/files/telehealth-faqs-508.pdf
2. *See* HIPAA Journal, Zoom Security Problems Raise Concern About Suitability for Medical Use, https://www.hipaajournal.com/zoom-security-problems/

despite the possible and known security risks with the Zoom platform, and as a result of a leaked encryption key patient data becomes vulnerable, would they be in violation of HIPAA[2]? Right now, the rules seem to be flexible and relaxed, but many providers may choose to offer convenient telehealth visits after COVID-19 has become less widespread. It is possible that in order to continue providing telehealth services, providers may need to establish a cybersecurity operation to maintain compliance in the future and protection or encryption of data.

Another question raised by the Center for Connected Health Policy is who will fall under the "business associate" category of entities covered by HIPAA.[3] Skype issued a statement in 2011 stating that they are not a business associate as contemplated in HIPAA, nor have they "entered into any contractual arrangements with covered entities to create HIPAA-compliant privacy and security obligations.[4]" The Health Information Technology for Economic Clinical Health Act of 2009, or HITECH Act, elaborated further by defining a "conduit." A conduit is an "entity that transports information, but does not access it except on a random or infrequent basis as necessary to perform the transportation services.[5]" However, this is a narrow exception that is only supposed to exclude entities that act as courier services (for example, the U.S. Postal Service) that provide "mere data transmission services.[6]" Therefore, it is paramount for services, such as Zoom, that allow recording of meetings to closely examine the relationship they have with sensitive data in order to determine whether they are covered under HIPAA rules.

Overall, the recent widespread usage of telehealth during the pandemic has rushed another technological advancement on health care providers that they may not be ready for. As a result, it appears that the compliance regulations have been relaxed in order to give covered entities "wiggle room" to develop the technological infrastructure. These relaxed guidelines

3. Center for Connected Health Policy, HIPAA and Telehealth, https://www.cchpca.org/sites/default/files/2018-09/HIPAA%20and%20Telehealth.pdf
4. *Id.*
5. *Id.*
6. Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the HITECH Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5570, 5571 (January 25, 2013) https://www.govinfo.gov/content/pkg/FR-2013-01-25/pdf/2013-01073.pdf

come with additional grey areas and raise important cybersecurity questions post-pandemic. Ultimately health information technology services will need to use this time to develop responses and technologies that assist providers as the industry moves forward into technological advancement.

3. Center for Connected Health Policy, HIPAA and Telehealth, https://www.cchpca.org/sites/default/files/2018-09/HIPAA%20and%20Telehealth.pdf
4. *Id*.
5. *Id*.
6. Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the HITECH Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5570, 5571 (January 25, 2013) https://www.govinfo.gov/content/pkg/FR-2013-01-25/pdf/2013-01073.pdf