Journal of Pediatric Rehabilitation Medicine: An Interdisciplinary Approach 13 (2020) 389–392
DOI 10.3233/PRM-200760
IOS Press

Short Communication

Changes in the office for civil rights enforcement policy on telehealth remote communications in response to COVID-19

Thomas J. Mortell* and Austin T. Strobel
Hawley Troxell Ennis and Hawley LLP, Boise, ID, USA

Abstract. The novel coronavirus, the cause of COVID-19, has sent shockwaves throughout the world, shuttered many businesses essentially overnight, and has left billions living worldwide in quarantine. Not surprisingly, the health care industry has been significantly affected by the COVID-19 pandemic. This article focuses on how COVID-19 has influenced the Office for Civil Rights' (OCR's) enforcement of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules as they relate to telehealth remote communications, and opines about whether the COVID-19-related changes to HIPAA Privacy Rule and Security Rule enforcement might last beyond the current crisis.

Keywords: COVID-19, safety protocols, construction, industry

1. Background

This article touches on telehealth services and the two key components of HIPAA that cover them – the HIPAA Privacy Rule and HIPAA Security Rule. Therefore, a brief overview of these key concepts is helpful. The U.S. Department of Health and Human Services (HHS) defines "telehealth" as "the use of electronic information and telecommunications technologies to support and promote long-distance clinical health care, patient and professional health-related education, and public health and health administration... Telehealth services may be provided, for example, through audio, text messaging, or video communication technology, including videoconferencing software [1]." In other words, "telehealth services" describes healthcare that is provided remotely through technological means. In addition to HIPAA, other federal and state laws regulate the provision of telehealth services. For example, Medicare Part B only pays for telehealth services conducted through "audio and video equipment permitting two-way, real-time interactive communication between the patient and distant site physician or practitioner. Telephones, facsimile machines, and electronic mail systems do not meet the definition of an interactive telecommunications system [2]." Some states define telehealth slightly differently. For example, the authors' home state, Idaho, defines "telehealth services" as "health care services provided by a provider to a person through the use of electronic communications, information technology, asynchronous store and forward transfer or synchronous interaction between a provider at a distant site and a patient at an originating site [3]." However, the initial physician-patient relationship must be established "by use of two-way audio and visual interaction [4]."

The HIPAA Privacy Rule, codified at 45 C.F.R. Parts 160 and 164, applies to disclosures of protected health information (PHI) by covered entities and by their business associates. A detailed primer of the HIPAA Privacy

*Corresponding author: Thomas J. Mortell, Hawley Troxell Ennis and Hawley LLP, Boise, ID, USA. E-mail: TMortell@hawleytroxell.com.

Rule and its various exceptions is beyond the scope of this article. However, in general, the HIPAA Privacy Rule prevents the unauthorized disclosure of PHI unless one of HIPAA's various exceptions applies. The HIPAA Security Rule, also codified at 45 C.F.R. Parts 160 and 164, creates certain security requirements for covered entities and their business associates that maintain and store patient PHI. The HIPAA Security Rule applies to a subset of PHI, known as electronic protected health information (e-PHI), which is PHI that is "creat[ed], receiv[ed], maintain[ed] or transmit[ted]" in electronic form [5]. As stated by HHS, "[t]he Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that organizations called 'covered entities' must put in place to secure individuals' 'electronic protected health information' (e-PHI) [5]." Though a complete analysis of the HIPAA Security Rule is beyond the scope of this article, generally, the Security Rule "requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI [5]." This includes "[e]nsuring the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit[,]" "[i]dentify[ing] and protect[ing] against reasonably anticipated threats to the security or integrity of the information, [p]rotect[ing] against reasonably anticipated, impermissible uses or disclosures[,]" and "[e]nsuring compliance by their workforce [5]." For purposes of the Security Rule, "confidentiality" means that "e-PHI is not available or disclosed to unauthorized persons [5]." Broadly, the Security Rule requires covered entities to undergo a risk analysis and implement security measures that manage and reduce security risks [5].

In short, the HIPAA Privacy Rule and HIPAA Security Rule focus on maintaining the privacy and confidentiality of PHI and e-PHI. Violations of either the HIPAA Privacy Rule and/or the HIPAA Security Rule can subject covered entities and/or business associates to enforcement actions and civil monetary penalties. In this day and age where nearly everything – including many aspects of healthcare services – can be performed remotely through electronic means, telehealth services provide a unique compliance challenge for covered entities to maintain the security and confidentiality of PHI, and to prevent disclosure of PHI to unauthorized individuals.

2. OCR's response to the COVID-19 pandemic

In February 2020, prior to the widespread outbreak of the COVID-19 pandemic in the United States, the OCR issued a Bulletin which served primarily as a reminder that the protections afforded patients by the HIPAA Privacy Rule "are not set aside during an emergency [6]." Notwithstanding this initial early reminder, OCR quickly pivoted to adjust enforcement standards for telehealth remote communications to assist overburdened healthcare providers to respond to a quickly changing landscape of shelter-in-place orders and social distancing policies that disconnected patients and their healthcare providers (at least physically) seemingly overnight.

The OCR's response to the quickly changing healthcare landscape caused by COVID-19 was the Notification of Enforcement Discretion issued by OCR on March 17, 2020 [7]. In simple terms, the Notification of Enforcement Discretion announced that OCR would exercise its enforcement discretion and not impose penalties against covered entities for HIPAA violations arising out of the good faith provision of telehealth services during the COVID-19 nationwide public health emergency [7]. The Notification of Enforcement Discretion applies to telehealth services during the duration of the crisis, and need not be related to COVID-19 treatment [8]. Though it should not be deemed a relaxation of OCR standards, the guidance announces a temporary exercise of enforcement discretion for telehealth services performed through technologies that "may not fully comply with the requirements of the HIPAA Rules [8]." Critically, this does not mean that technology vendors that do not comply with the HIPAA Rules are "approved" by OCR, only that the OCR will not pursue enforcement measures against covered entities for using such vendors during the Nationwide Public Health Emergency. OCR also notes that telehealth services should still be conducted in private between the patient and provider. If services cannot be conducted in private, practical safeguards such as "using lowered voices, not using speakerphone, or recommending that a patient move to a reasonable distance from others when discussing PHI" should be implemented [1]. Notably, this exercise of enforcement discretion does not relieve the covered entity from its responsibility to engage security safeguards and notify patients of potential risks. Indeed, "[p]roviders are encouraged to notify patients that these third-party applications potentially introduce privacy risks, and providers should enable all available encryption and privacy modes when using such applications [8]."

The fine print of the Notification of Enforcement Discretion is that telehealth services must be provided using a "non-public facing remote communication product [8]." The OCR provided additional guidance in the "FAQs on Telehealth and HIPAA during the COVID-19 nationwide public health emergency" that defines what the OCR deems to be a "non-public facing remote communication product." Per OCR, a "non-public facing" product is one that "as a default, allows only the intended parties to participate in the communication [1]." By contrast, a "public facing" product is one that is "designed to be open to the public or allow wide or indiscriminate access to the communication [1]."

Notably, the Notification of Enforcement Discretion expressly lists many well-known person-to-person communication platforms, including Apple FaceTime, Facebook Messenger video chat, Google Hangouts video, Zoom, and Skype, as "non-public facing [8]". OCR does not take the position that this is an exhaustive list of permissible platforms for telehealth services during the global pandemic. However, covered entities would be wise to stay within the "safe harbor" of listed "non-public facing" platforms if these well-known person-to-person video platforms for telehealth may not, under normal circumstances, comply with HIPAA. OCR also expressly notes that well-known video communication platforms such as Facebook Live, Twitch, TikTok, and "similar video communication applications" are deemed by OCR to be "public facing" remote communication products, and should not be used for telehealth services even during the pandemic [8].

The Notification of Enforcement Discretion also creates a "good faith" standard as a prerequisite for a covered entity to be entitled to the benefit of OCR's COVID-19 enforcement discretion. OCR also issued additional guidance on this "good faith" standard in its "FAQ on Telehealth and HIPAA during the COVID-19 nationwide public health emergency." There, OCR states that it will "consider all facts and circumstances" in evaluating whether telehealth has been provided in good faith. Though perhaps not ideal, OCR seems to have defined "good faith" by negative implication only, providing examples of what OCR deems to be "bad faith." OCR identifies that a "bad faith" provision of telehealth might include things like: (1) conduct in furtherance of a criminal act, such as fraud, identity theft, and intentional invasion of privacy; (2) further uses or disclosures of PHI transmitted via telehealth that are prohibited by HIPAA; (3) violations of state licensing laws or professional ethical standards that result in discipline related to treatment offered via telehealth; and (4) use of a "public facing" remote communication product to provide telehealth services [1]. A reasonable assumption might be that the provision of telehealth services that does not implicate any of the four "bad faith" elements is a "good faith" provision of telehealth services, though that may be a bridge too far. Black's Law Dictionary defines "good faith" as "[a] state of mind consisting in (1) honesty in belief or purpose, (2) faithfulness to one's duty or obligation, (3) observance of reasonable commercial standards of fair dealing in a given trade or business, or (4) absence of intent to defraud or to seek unconscionable advantage [9]." Given OCR's lack of a concrete definition on the meaning of "good faith" for purposes of the Notification of Enforcement Discretion, covered entities should avoid providing telehealth services in ways that violate the OCR's defined "bad faith" categories, and evaluate other uses of telehealth with the Black's Law Dictionary's definition of "good faith" in mind. If concerns arise, covered entities should consult with their legal counsel on these issues.

3. Sea-change or temporary change?

Those hoping that OCR's COVID-19-related exercise of enforcement discretion might signal a broader amendment of enforcement standards that could last beyond the coronavirus pandemic are likely in for disappointment. Even the title of OCR's recent "FAQ on Telehealth and HIPAA during the COVID-19 nationwide public health emergency" (emphasis added) suggests that OCR's recent guidance in enforcement policy is a temporary change meant to address the particular and unprecedented pandemic the world is currently experiencing. Going beyond just the title, the phrasing of the FAQ Responses themselves are also highly suggestive that the recent OCR enforcement policy guidance is merely temporary and likely does not signal a broad sea-change in HIPAA enforcement standards. The Response to Question 4 in the "FAQ on Telehealth and HIPAA during the COVID-19 nationwide public health emergency" specifically states that enforcement discretion applies "during the COVID-19 nationwide public health emergency [1]." The Response to Question 5 in the same document notes that the Notification of Enforcement Discretion does not have a defined duration tied to a specific date, but that "OCR will issue a notice to the public when it is no longer exercising its enforcement discretion based upon the latest facts and circumstances." This denotes both that OCR intends to

revoke the Notification of Enforcement Discretion at some point, and seems to tie that future date to when the "latest facts and circumstances" of COVID-19 will permit a return to previous standards [1]. At this point, OCR's guidance in enforcement cannot reasonably be seen as anything but a temporary change to deal with a very specific crisis.

That being said, it will be interesting to see if, in the long term, the guidance regarding HIPAA enforcement standards – which allow the use of well-known person-to-person communication platforms – will normalize telehealth services even further, and contribute to the proliferation of the use of telehealth for healthcare services that formerly were included in in-person visits. As the availability of health care services in rural areas continues to contract, access to care through means that are easier and less expensive certainly make sense. Telehealth services and well-known person-to-person communication platforms further those efforts. If telehealth does become the new normal, OCR may eventually have to consider permanently amending its enforcement standards for telehealth. In 10 years, perhaps COVID-19 will be seen as a flashpoint for telehealth and the first real domino to fall to initiate a new normal in the provision of healthcare services.

This article is informational only, contains the opinions of its authors, and does not constitute legal advice. The reader should conduct their own analysis of the text of the *Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency* in close communication with legal counsel.

Conflict of interest

The authors have no conflict of interest to report.

References

[1] FAQs on Telehealth and HIPAA during the COVID-19 nationwide public health emergency [Internet]. Office for Civil Rights, Department of Health and Human Services; 2020. Available from: https://www.hhs.gov/sites/default/files/telehealth-faqs- 508.pdf.
[2] 42 C.F.R. §410.78(3).
[3] Idaho Code §54-5703.
[4] Idaho Code §54-5705(1).
[5] Summary of the HIPAA Security Rule [Internet]. Department of Health and Human Services; 2013. Available from: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.
[6] Bulletin: HIPAA Privacy and Novel Coronavirus [Internet]. Office for Civil Rights, Department of Health and Human Services; 2020. Available from: https://www.hhs.gov/sites/default/files/february-2020-hipaa-and-novel-coronavirus.pdf.
[7] OCR Announces Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency [Internet]. Office for Civil Rights, Department of Health and Human Services; 2020. Available from: https://www.hhs.gov/about/news/2020/03/17/ocr-announces-notification-of-enforcement-discretion-for-telehealth-remote-communications-during-the-covid-19.html.
[8] Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency [Internet]. Office for Civil Rights, Department of Health and Human Services; 2020. Available from: https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html.
[9] Black's Law Dictionary [Internet]. West (Thompson Reuters Corporation); 2019. GOOD FAITH.