PG Alert
March 9, 2020

What Privacy and Security Standards Apply Now?
The Use of Telephones to Provide Telehealth Services to Medicare Beneficiaries During the Coronavirus Public Health Emergency
Sean T. Sullivan (Alston & Bird LLP)
Elizabeth Hodge (Akerman LLP)

This Alert is brought to you by Privacy and Security Risk Compliance and Enforcement Affinity Group of the Health Information and Technology Practice Group.

President Trump signed into law March 6 the "Coronavirus Preparedness and Response Supplemental Appropriations Act of 2020," a sweeping emergency funding act that provides $8.3 billion for efforts to combat the coronavirus, or COVID-19 (Appropriations Act).[1] Nestled at the end of the Appropriations Act is the "Telehealth Services During Certain Emergency Periods Act of 2020," plucked from the earlier introduced CONNECT for Health Act, which permits the Secretary of the Department of Health and Human Services to waive the originating site requirement for telehealth services reimbursed by Medicare, although with several added restrictions.

Namely, the waiver may be applied only in the current coronavirus emergency declaration (and any renewals), and it will be available only to physicians and non-physician practitioners who have a pre-existing relationship with the patient within the last three years (or to practitioners within the same practice as the practitioner with an established relationship). Although this provision is narrower than what some in the industry pushed for, it is a promising step in the right direction for telehealth and provides a new tool for practitioners in the battle against coronavirus. Crucially, it will reduce the need for patients to travel to population centers and designated health care facilities for care during the current crisis.

Also included in the telehealth provisions in the Appropriations Act is that the Secretary may waive the restriction on the use of telephones for Medicare-reimbursable telehealth services. Under the existing regulations, Medicare Part B covers telehealth services when they are provided via an "interactive telecommunications system," and "[t]elephones, facsimile machines, and electronic mail systems do not meet the definition of an interactive telecommunications system."[2] However, recognizing that modern smartphones have the capabilities of a powerful videoconferencing workstation—or a typical telemedicine cart—and are already in the pockets or purses of most Medicare beneficiaries, the Appropriations Act calls for the waiver of "the restriction on use of a telephone . . . but only if such telephone has audio and video

capabilities that are used for two-way, real-time interactive communication." This could, ostensibly, include any smartphone-based videoconferencing solution, such as FaceTime, Skype, WebEx, and the like.

However, the Appropriations Act makes no reference to privacy and security standards, nor to the Health Insurance Portability and Accountability Act (HIPAA), related statutes, or their implementing regulations. This has already led to confusion among practitioners preparing to implement the anticipated waiver and provide telehealth services under these new rules via smartphones.

Under HIPAA, covered entities must implement reasonable safeguards to protect patient Protected Health Information (PHI) from unauthorized disclosures, and PHI may only be used or disclosed in certain circumstances, when needed for patient care, or other important purposes. **These standards are not relaxed during public health emergencies, and the Appropriations Act does not waive or permit the Secretary to waive any HIPAA requirements.**

The Office for Civil Rights (OCR) recently published guidance to reaffirm when PHI may be shared under the HIPAA Privacy Rule during the coronavirus crisis (or any other emergency situation), and to remind providers and business associates that the HIPAA Security Rule requires the same administrative, physical, and technical safeguards during public health emergencies as during non-emergency situations.[3]

In particular, practitioners providing care and treatment to patients via telehealth over telephones should remember that:

- Communication methods, even over smartphones, should maintain the confidentiality, integrity, and availability of patient PHI, which generally means that the videoconferencing and other technology platforms should be secure and encrypted;[4]
- Practitioners should have HIPAA-compliant business associate agreements (BAA) in place with technology vendors prior to sharing PHI or providing patient care via videoconference;[5]
- Patient information may be disclosed without patient authorization or a BAA only for:
    - Treatment of patients, including the coordination or management of health care and related services by one or more health care providers and others, consultation between providers, and the referral of patients for treatment,[6]
    - Public health activities, including to public health authorities (such as the CDC or local health departments) to prevent or control disease, to a foreign government agency at the direction of a public health authority, or to persons at risk of contracting or spreading a disease (if authorized by state law),[7]
    - Disclosures to family and friends involved in the patient's care and to identify, locate, and notify family members of the patient's condition,[8]

    - Disclosures to prevent serious and imminent threat, consistent with applicable state or other law and the practitioner's standards of ethics, and professional judgment about the nature and severity of the threat to health and safety,[9]
    - Disclosures of limited facility directory information acknowledging the individual is a patient and describing the individual's condition in general terms, e.g., good, stable, critical, where the patient has not objected to or restricted release of PHI,[10]
    - Payment, including activities to obtain payment or fulfill coverage responsibilities,[11] and
    - Health care operations, including administrative, financial, legal, and quality improvement activities of a covered entity, such as quality improvement, peer review, business development, and management;[12]
- Health care providers may not disclose to the media or the general public information about an identifiable patient or specifics of that patient's care and treatment without a written authorization from the patient (or his or her personal representative);[13] and
- Practitioners should make reasonable efforts to limit any PHI disclosed to that which is considered the "minimum necessary" to accomplish the intended purpose of the use or disclosure.[14]

While the telehealth waiver will enable health care providers to reduce the risk of exposure to the coronavirus for their patients and their workforce members, providers must remember their data privacy and security obligations under HIPAA.

---

[1] H.R. 6074 (Mar. 6, 2020), *available at* https://www.govinfo.gov/content/pkg/BILLS-116hr6074enr/pdf/BILLS-116hr6074enr.pdf.
[2] *See* 42 C.F.R. § 410.78(a)(3).
[3] OCR, "BULLETIN: HIPAA Privacy and Novel Coronavirus," (Feb. 2020), *available at* https://www.hhs.gov/sites/default/files/february-2020-hipaa-and-novel-coronavirus.pdf.
[4] 45 C.F.R. §§ 164.306(a)(1).
[5] 45 C.F.R. §§ 164.502(e), 164.314(a).
[6] 45 C.F.R. § 164.506(c).
[7] 45 C.F.R. § 164.512(b).
[8] 45 C.F.R. § 164.510(b).
[9] 45 C.F.R. § 164.512(j)(1)(i).
[10] 45 C.F.R. § 164.510(a).
[11] 45 C.F.R. § 164.506(c).
[12] *Id*.
[13] 45 C.F.R. § 164.508.
[14] 45 C.F.R. § 164.502(b); 45 C.F.R. § 164.514(d)(1).