COVID-19 AND THE HIPAA PRIVACY RULE: ASKED AND ANSWERED

Stacey A. Tovino, JD, PhD*

I. INTRODUCTION

On January 31, 2020, Health and Human Services (HHS) Secretary Alex M. Azar II used the authority vested in him under Section 319 of the Public Health Service Act[1] to formally determine that a public health emergency (PHE) existed in the United States due to the severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2), the virus that causes coronavirus disease 2019 (COVID-19).[2] Six weeks later, on March 13, 2020, President Donald Trump used the authority vested in him under Section 201 of the National Emergencies Act[3] to formally proclaim that a national emergency existed.[4] Both Secretary Azar's PHE determination and President Trump's national emergency proclamation implicated Section 1135 of the Social Security Act (SSA),[5] which gives the Secretary

*Professor of Law, and Faculty Lead, MLS in Healthcare Law Program, University of Oklahoma College of Law, Norman, Oklahoma.

1. Public Health Service Act § 319, 42 U.S.C. § 247d(a) (2018) ("If the Secretary determines, after consultation with such public health officials as may be necessary, that . . . a disease or disorder presents a public health emergency[] or . . . a public health emergency, including significant outbreaks of infectious diseases or bioterrorist attacks, otherwise exists, the Secretary may take such action as may be appropriate to respond to the public health emergency, including making grants, providing awards for expenses, and entering into contracts and conducting and supporting investigations into the cause, treatment, or prevention of a disease or disorder. . . .").

2. Alex M. Azar II, *Determination that a Public Health Emergency Exists*, HHS (Jan. 31, 2020), https://www.phe.gov/emergency/news/healthactions/phe/Pages/2019-nCoV.aspx. Secretary Azar made his PHE determination retroactive to January 27, 2020. *Id.*

3. National Emergencies Act § 201, 50 U.S.C. § 1621(a) (2018) ("With respect to Acts of Congress authorizing the exercise, during the period of a national emergency, of any special or extraordinary power, the President is authorized to declare such national emergency. Such proclamation shall immediately be transmitted to the Congress and published in the Federal Register.").

4. Declaring a National Emergency Concerning the Novel Coronavirus Disease (COVID-19) Outbreak, Proclamation No. 9994, 85 Fed. Reg. 15,337, 15,337 (Mar. 13, 2020). State governors likewise used their powers under state statutes and state constitutions to declare statewide emergencies. For example, Oklahoma Governor J. Kevin Stitt used the power vested in him under Article VI of the Oklahoma Constitution to issue Executive Order 2020-07, declaring an emergency across all seventy-seven Oklahoma counties. Okla. Exec. Order No. 2020-07 (Mar. 15, 2020), https://www.sos.ok.gov/documents/executive/1913.pdf (last visited Mar. 1, 2021).

5. Social Security Act § 1135, 42 U.S.C. § 1320b-5(b)(7) (2018).

the authority to waive sanctions and penalties that arise from noncompliance with certain provisions within the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[6] Privacy Rule.[7] These provisions relate to honoring a patient's request to opt out of a health care provider's facility directory,[8] obtaining a patient's agreement to speak with family members or friends,[9] distributing a notice of privacy practices,[10] giving patients the right to request privacy restrictions,[11] and giving patients the right to request confidential communications.[12] Effective March 15, 2020, the Secretary formally issued such waiver (hereinafter HIPAA Rules Waiver) with respect to these five provisions but clarified that the waiver only applied: (1) to HIPAA-covered[13] hospitals that have instituted a disaster protocol; (2) for a period of up to seventy-two hours from the time the covered hospital implements its

6. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (Aug. 21, 1996) (codified as 42 U.S.C. *passim*), *amended in part by* Health Information Technology for Economic and Clinical Health Act (HITECH), Pub. L. No. 111-5, 123 Stat. 115, 226 (Feb. 17, 2009) (codified as 42 U.S.C. §§ 17937, 17953).

7. HHS's privacy regulations, which implement section 264(c) of HIPAA, are codified at 45 C.F.R. pt. 164(E).

8. *See* 45 C.F.R. § 164.510(a)(2) (2019) ("A covered health care provider must inform an individual of the protected health information that it may include in a directory and the persons to whom it may disclose such information (including disclosures to clergy of information regarding religious affiliation) and provide the individual with the opportunity to restrict or prohibit some or all of the uses or disclosures . . . ").

9. *Id.* § 164.510(b)(1)(i) ("A covered entity may, in accordance with paragraph[] (b)(2), . . . disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, the protected health information directly relevant to such person's involvement with the individual's health care or payment related to the individual's health care."); *id.* § 164.510(b)(2) ("If the individual is present for, or otherwise available prior to, a use or disclosure permitted by paragraph (b)(1) of this section and has the capacity to make health care decisions, the covered entity may use or disclose the protected health information if it: (i) Obtains the individual's agreement; (ii) Provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection. . . .").

10. *Id.* § 164.520(c)(2) ("A covered health care provider that has a direct treatment relationship with an individual must: (i) Provide the notice: (A) No later than the date of the first service delivery, including service delivered electronically, to such individual after the compliance date for the covered health care provider; or (B) In an emergency treatment situation, as soon as reasonably practicable after the emergency treatment situation.").

11. *Id.* § 164.522(a)(1)(i) ("A covered entity must permit an individual to request that the covered entity restrict: (A) Uses or disclosures of protected health information about the individual to carry out treatment, payment, or health care operations; and (B) Disclosures permitted under § 164.510(b).").

12. *Id.* § 164.522(b)(1)(i) ("A covered health care provider must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the covered health care provider by alternative means or at alternative locations.").

13. *See infra* text accompanying notes 41–45 (explaining which health care providers are covered by the HIPAA Privacy Rule).

disaster protocol; and (3) until the termination of either Secretary Azar's PHE or President Trump's national emergency.[14]

In addition to the HIPAA Rules Waiver, HHS has also issued three HIPAA-related Notices of Enforcement Discretion since the beginning of the PHE. On April 7, 2020, for example, HHS published in the *Federal Register* a Notice of Enforcement Discretion for business associates (hereinafter Business Associate Enforcement Discretion).[15] As background, the HIPAA Privacy Rule traditionally allows a business associate (BA)[16] of a covered entity to use and disclose protected health information (PHI)[17] for public health and health oversight purposes—but only when expressly permitted to do so by the BA's business associate agreement (BAA) with the covered entity.[18] During the COVID-19 pandemic, HHS learned that a number of federal, state, and local public health authorities, health oversight agencies, and emergency operations centers had requested PHI from BAs or had requested the BAs to perform certain public health data analytics on such PHI for the purpose of ensuring the health and safety of the public during the COVID-19 pandemic.[19] However, some BAs did not respond because their BAAs did not expressly permit them to make the requested uses and disclosures.[20] To encourage these important public health and health oversight activities, HHS determined that it would not impose penalties for violations of the HIPAA Privacy Rule relating to uses and disclosures of PHI by BAs during the PHE for these activities.[21]

On April 21, 2020, HHS published in the *Federal Register* a second Notice of Enforcement Discretion regarding the HIPAA Privacy,[22]

14. U.S. Dep't Health & Human Servs., *COVID-19 & HIPAA Bulletin: Limited Waiver of HIPAA Sanctions and Penalties During a Nationwide Public Health Emergency*, HHS (Mar. 15, 2020), https://www.hhs.gov/sites/default/files/hipaa-and-covid-19-limited-hipaa-waiver-bulletin-508.pdf [hereinafter HIPAA Rules Waiver].

15. Enforcement Discretion Under HIPAA To Allow Uses and Disclosures of Protected Health Information by Business Associates for Public Health and Health Oversight Activities in Response to COVID-19, 85 Fed. Reg. 19,392 (Apr. 7, 2020) [hereinafter Business Associate Enforcement Discretion].

16. A business associate may be summarily defined as a person who needs to access, use, or disclose the PHI of a covered entity in order to provide certain functions or services to or on behalf of the covered entity other than in the capacity of a workforce member of that covered entity. *See* 45 C.F.R. § 160.103 (2019) (defining business associate with greater specificity).

17. *See infra* text accompanying notes 47–48 (defining PHI).

18. Business Associate Enforcement Discretion, 85 Fed. Reg. at 19,392.

19. *Id.* at 19,393.

20. *Id.*

21. *Id.*

22. *See* HIPAA Privacy Rule, 45 C.F.R. §§ 164.500–.534 (2019).

Security,[23] and Breach Notification[24] Rules (collectively HIPAA Rules) in the context of covered health care providers' "good faith provision" of nonpublic facing telehealth (hereinafter Telehealth Enforcement Discretion).[25] Nonpublic facing telehealth products include Skype, Zoom, FaceTime, Facebook Messenger, and Google Hangouts. Although HHS did not define the "good faith provision" of nonpublic facing telehealth, HHS did state that enforcement discretion would not be applied to situations involving bad faith.[26] Examples of bad faith provided by HHS included violations of state licensing laws, violations of professional ethical standards resulting in documented disciplinary actions, and the use of public-facing (versus nonpublic facing) remote communication products, such as Facebook Live, Twitch, and TikTok.[27]

On May 18, 2020, HHS published in the *Federal Register* a third Notice of Enforcement Discretion, this time for community-based testing sites (CBTSs) (hereinafter CBTS Enforcement Discretion).[28] In its CBTS Enforcement Discretion, HHS announced that it would not impose penalties for noncompliance with the HIPAA Rules by covered health care providers and their BAs who participate in good faith in the operation of a CBTS during the PHE.[29] As background, CBTSs include "mobile, drive-through, or walk-up sites that only provide COVID-19 specimen collection or testing services to the public."[30] Although OCR encourages covered health care providers and BAs operating CBTSs to implement a number of reasonable safeguards[31] to protect the privacy

23. HHS's security regulations, which implement section 262(a) of HIPAA (42 U.S.C. § 1320d-2(d)(1)), are codified at 45 C.F.R. pt. 164(C). This Article refers to this as the HIPAA Security Rule.

24. HHS's breach notification regulations, which implement section 13402 of HITECH (42 U.S.C. § 17932), are codified at 45 C.F.R. pt. 164(D). This Article refers to this as the HIPAA Breach Notification Rule.

25. Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency, 85 Fed. Reg. 22,024, 22,024 (Apr. 21, 2020) [hereinafter Telehealth Enforcement Discretion].

26. *Id.* at 22,025.

27. *Id.*

28. Enforcement Discretion Regarding COVID-19 Community-Based Testing Sites (CBTS) During the COVID-19 Nationwide Public Health Emergency, 85 Fed. Reg. 29,637 (May 18, 2020) [hereinafter CBTS Enforcement Discretion].

29. *Id.*

30. *Id.*

31. Reasonable safeguards mentioned by HHS in the CBTS Enforcement Discretion include: (1) "Using and disclosing only the minimum PHI necessary except when disclosing PHI for treatment"; (2) "Setting up canopies or similar opaque barriers at a CBTS to provide some privacy to individuals during the collection of samples"; (3) "Controlling foot and car traffic to create adequate distancing at the point of service to minimize the ability of persons to see or overhear screening interactions at a CBTS"; (4) "Establishing a 'buffer zone' to prevent members of the media or public from observing or filming individuals who approach a CBTS, and posting signs prohibiting filming"; (5) "Using secure technology at a CBTS to record and transmit electronic PHI"; and (6) "Posting a Notice

and security of individuals' PHI, OCR stated that it would not impose penalties for HIPAA Rules violations that occur in connection with those operations to the extent they are in good faith.[32]

In addition to the HIPAA Rules Waiver and the three Notices of Enforcement Discretion, HHS has also released a number of less formal guidance documents, bulletins, answers to frequently asked questions, and webinars explaining the application of particular HIPAA Rules to situations raised by the COVID-19 pandemic. For example, HHS released three guidance documents explaining: (1) the situations in which the HIPAA Privacy Rule allows a covered entity to share the name or other identifying information of an individual who has been infected with or exposed to SARS-CoV-2 with law enforcement, paramedics, other first responders, and public health authorities without the individual's prior written authorization (First Guidance);[33] (2) that covered health care providers must obtain prior written authorization from patients or their legal representatives before giving journalists, news reporters, and other members of the media access to patients or their PHI (Second Guidance);[34] and (3) that the HIPAA Privacy Rule permits, in certain situations, a covered health care provider to use PHI to identify and contact patients who have recovered from COVID-19 to provide them with information about donating blood and plasma that could help other COVID-19 patients (Third Guidance).[35]

By further example, and also since the beginning of the PHE, HHS released two bulletins designed to: (1) ensure that covered entities and their BAs are aware of the ways that patient information may be shared under the HIPAA Privacy Rule during outbreaks of infectious disease, including COVID-19, and to remind the public that most of the protections set forth in the HIPAA Privacy Rule are not set aside during

---

of Privacy Practices (NPP), or information about how to find the NPP online, if applicable, in a place that is readily viewable by individuals who approach a CBTS." *Id.* at 29,637–38.

32. *Id.* at 29,638.

33. *COVID-19 and HIPAA: Disclosures to Law Enforcement, Paramedics, Other First Responders and Public Health Authorities*, HHS, https://www.hhs.gov/sites/default/files/covid-19-hipaa-and-first-responders-508.pdf (last visited Mar. 1, 2021).

34. *Guidance on Covered Health Care Providers and Restrictions on Media Access to Protected Health Information about Individuals in Their Facilities*, HHS, https://www.hhs.gov/sites/default/files/guidance-on-media-and-film-crews-access-to-phi.pdf (last visited Mar. 1, 2021) [hereinafter Second Guidance].

35. *Updated Guidance on HIPAA and Contacting Former COVID-19 Patients about Plasma Donation*, HHS (Aug. 2020), https://www.hhs.gov/sites/default/files/guidance-on-hipaa-and-contacting-former-covid-19-patients-about-blood-and-plasma-donation.pdf [hereinafter Third Guidance].

PHEs (First Bulletin);[36] and (2) "ensure that entities covered by civil rights authorities keep in mind their obligations under laws and regulations that prohibit discrimination on the basis of race, color, national origin, disability, age, sex, and exercise of conscience and religion in HHS-funded programs" as well as under the HIPAA Privacy Rule (Second Bulletin).[37] In addition, HHS released one set of frequently asked questions (Telehealth FAQs) addressing issues that lie at the intersection of telehealth, COVID-19, and the HIPAA Rules.[38] Finally, HHS gave a webinar on April 24, 2020, summarizing some of the formal and informal documents referenced above.[39]

Notwithstanding the issuance of these waivers, notices of enforcement discretion, guidance documents, bulletins, frequently asked questions, and webinars (collectively HHS Guidance), news reporters, attorneys, students, and members of the general public still have great difficulty understanding how the HIPAA Rules apply to issues raised by the COVID-19 pandemic. Since Secretary Azar determined on January 31, 2020 that a nationwide PHE existed, the Author has been contacted by a wide variety of journalists, lawyers, law students, and community members with both basic and complex COVID-19-related questions not addressed, or insufficiently addressed, by the HHS Guidance. This Article answers these questions and, in so doing, hopefully provides a guide for the proper use and disclosure of PHI under the HIPAA Rules during public health emergencies.

This Article proceeds as follows: Part I provides background information regarding the HIPAA Rules. Part II identifies and answers HIPAA-related questions that have been asked of the Author during the COVID-19 pandemic and that are not addressed, or are insufficiently addressed, by the HHS Guidance issued to date. Part III proposes amendments to HHS's process for releasing future guidance on the application of the HIPAA Rules during public health emergencies.

---

36. *Bulletin: HIPAA Privacy and Novel Coronavirus*, HHS (Feb. 2020), https://www.hhs.gov/sites/default/files/february-2020-hipaa-and-novel-coronavirus.pdf [hereinafter First Bulletin].

37. *Bulletin: Civil Rights, HIPAA, and the Coronavirus Disease (COVID-19)*, HHS (Mar. 28, 2020), https://www.hhs.gov/sites/default/files/ocr-bulletin-3-28-20.pdf.

38. *FAQs on Telehealth and HIPAA During the COVID-19 Nationwide Public Health Emergency*, HHS, https://www.hhs.gov/sites/default/files/telehealth-faqs-508.pdf (last visited Mar. 1, 2021) [hereinafter Telehealth FAQs].

39. U.S. Dep't Health & Human Servs., *Update on HIPAA and COVID-19*, HEALTHIT (Apr. 24, 2020), https://www.healthit.gov/sites/default/files/page/2020-04/OCR%20COVID-19%20Slide%20Deck%20ONC%20Webinar.pdf.

II. THE HIPAA RULES[40]

A. The HIPAA Privacy Rule

The HIPAA Privacy Rule regulates covered entities[41] and BAs.[42] Covered entities include individual and group health plans,[43] health care clearinghouses,[44] and health care providers that transmit health information in electronic form in connection with certain standard transactions.[45] A BA is a person or organization that provides certain enumerated services to or on behalf of a covered entity, other than in the capacity of a workforce member of the covered entity, and who needs access to PHI to perform the service.[46] The HIPAA Privacy Rule regulates covered entities and BAs when they are using, disclosing, or requesting PHI.[47] With four, rarely-implicated exceptions, PHI is individually identifiable health information.[48] Health information that has been properly de-identified, however, is not regulated by the HIPAA Rules.[49] One permissible method of de-identifying information involves the removal of eighteen different identifiers including, but not limited to, names, "[a]ll geographic subdivisions smaller than a [s]tate," "[a]ll elements of dates (except for year) for" individuals eighty-nine years of

40. In a number of prior publications, the Author carefully reviewed the history, application, and general framework of the HIPAA Rules. *See, e.g.*, Stacey A. Tovino, *Assumed Compliance*, 72 ALA. L. REV. 279 (2020); Stacey A. Tovino, *Going Rogue: Mobile Research Applications and the Right to Privacy*, 95 NOTRE DAME L. REV. 155 (2019); Stacey A. Tovino, *A Timely Right to Privacy*, 104 IOWA L. REV. 1361 (2019); Stacey A. Tovino, *Remarks on Patient Privacy: Problems, Perspectives, and Opportunities*, 27 ANNALS HEALTH L. 243 (2018); Stacey A. Tovino, *The HIPAA Privacy Rule and the EU GDPR: Illustrative Comparisons*, 47 SETON HALL L. REV. 973 (2017); Stacey A. Tovino, *Teaching the HIPAA Privacy Rule*, 61 ST. LOUIS U. L.J. 469 (2017). With updates and technical changes, the summaries of the HIPAA Rules set forth in Part I of this Article are taken with the permission of the Author from these prior publications.

41. 45 C.F.R. § 160.103 (defining covered entity); *id.* § 160.102(a) (applying the HIPAA Rules to covered entities).

42. *Id.* § 160.103 (defining BA); *id.* § 160.102(b) (applying the HIPAA Rules to BAs).

43. *Id.* § 160.103 (defining health plan).

44. *Id.* (defining health care clearinghouse).

45. *Id.* (defining covered entity).

46. *Id.* (defining BA).

47. *Id.* § 164.500(a) ("[T]he standards, requirements, and implementation specifications of this subpart apply to covered entities with respect to protected health information.").

48. *Id.* § 160.103 (defining individually identifiable health information as a subset of health information that is "created or received by a health care provider, health plan, employer, or health care clearinghouse" and that "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual"); *id.* (listing the four exclusions from the definition of PHI).

49. *Id.* § 164.514(a) ("Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information."); *id.* §§ 164.514(b)(1)–(2) (setting forth two methods for health information to be considered de-identified).

age and younger, "[f]ull face photographic images and any comparable images[,] and . . . [a]ny other unique identifying number, characteristic, or code."[50]

1. The Use and Disclosure Requirements

The HIPAA Privacy Rule contains three groups of regulations: the use and disclosure requirements,[51] the individual rights,[52] and the administrative requirements.[53] In terms of the use and disclosure requirements, the HIPAA Privacy Rule requires covered entities and BAs to adhere to one of three different requirements depending on the purpose of the information use or disclosure.[54] The first use and disclosure requirement allows covered entities and BAs to use and disclose PHI with no prior permission from the individual who is the subject of the PHI—but only in certain situations. That is, covered entities may freely use and disclose PHI without any form of prior permission in order to carry out certain treatment, payment, and health care operations (HCO)[55] activities (collectively TPO activities),[56] as well as certain public benefit activities (PBAs).[57]

HHS discussed the first use and disclosure requirement in several pieces of guidance released during the pandemic. In the First Bulletin, for example, HHS clarified that a covered health care provider is permitted to disclose, without a patient's prior authorization, PHI as necessary to diagnose or treat a patient for COVID or even to treat other patients with COVID.[58] As an illustration, a covered physician may disclose PHI to a laboratory that will test a patient's specimen for the presence of SARS-CoV-2 without the prior written authorization of the patient. As a second illustration, a covered health care provider may disclose, also without prior written authorization, PHI as necessary to

50. *Id.* § 164.514(b)(2) (listing the eighteen identifiers that must be removed from PHI for the information to be considered de-identified).

51. *Id.* §§ 164.502–.514.

52. *Id.* §§ 164.520–.528.

53. *Id.* § 164.530.

54. *Id.* §§ 164.502–.514 (setting forth the use and disclosure requirements applicable to covered entities and BAs).

55. *Id.* § 164.501 (defining treatment, payment, and health care operations).

56. *See id.* § 164.506(c)(1) (permitting a covered entity to use or disclose PHI for its own treatment, payment, or health care operations); *id.* §§ 164.506(c)(2)–(4) (permitting a covered entity to disclose PHI to certain recipients for the recipients' treatment, payment, or health care operations activities, respectively).

57. Covered entities may use and disclose PHI for twelve different public benefit activities (PBAs) without the prior written authorization of the individual who is the subject of the information. *See id.* §§ 164.512(a)–(l).

58. *See* First Bulletin, *supra* note 36, at 3.

refer a patient to a second health care provider who will assume the treatment of the patient for COVID.[59]

In the Third Guidance, HHS also clarified that covered health care providers are permitted to use PHI to identify and contact patients who have recovered from COVID-19 to provide them with information about donating blood and plasma that could help other COVID-19 patients.[60] HHS reasoned that such uses are population-based HCO activities because "facilitating the supply of donated plasma would be expected to improve the covered health care provider's or health plan's ability to conduct case management for patients or beneficiaries that have or may become infected with COVID-19."[61] HHS also clarified that such uses must occur without the exchange of remuneration between the provider and, for example, a blood and plasma center; otherwise, the PHI uses would constitute marketing activities requiring each patient's prior written authorization.[62]

Moreover, in the First Bulletin, HHS clarified that a covered health care provider could share PHI, including suspected and confirmed COVID-19 diagnostic information, with a public health authority, such as the federal Centers for Disease Control and Prevention (CDC) or a state or local health department, for purposes of mandatory disease reporting as part of the PBA provisions.[63] HHS provided the following example: "[A] covered entity may disclose to the CDC protected health information on an ongoing basis as needed to report all prior and prospective cases of patients exposed to or suspected or confirmed to have Novel Coronavirus (2019-nCoV)."[64] HHS further clarified that a covered entity is permitted to share PHI with persons at risk of contracting or spreading COVID-19 in accordance with the PBA provisions if state or other law authorizes the covered entity to notify such persons as necessary to prevent or control the spread of the disease or otherwise to carry out public health interventions or investigations.[65] Finally, HHS clarified that covered health care providers could share PHI in accordance with the PBA provisions with anyone (including family, friends, law enforcement, and first responders) who could prevent or lessen an imminent threat of COVID-19 exposure.[66]

59. *Id.*
60. Third Guidance, *supra* note 35, at 1–2.
61. *Id.* at 2.
62. *Id.*
63. First Bulletin, *supra* note 36, at 3.
64. *Id.*
65. 45 C.F.R. § 164.512(b)(1)(iv) (2019); First Bulletin, *supra* note 36, at 4.
66. First Bulletin, *supra* note 36, at 4.

Under the HIPAA Privacy Rule's second use and disclosure requirement, a covered entity or BA may use and disclose an individual's PHI for certain activities, but only if the individual is informed (orally or in writing) in advance of the use or disclosure and is given the (oral or written) opportunity to agree to, prohibit, or restrict some or all of the uses and disclosures.[67] The certain activities captured by this provision include, but are not limited to, disclosures of PHI: (1) from a health care provider's facility directory; (2) to a person who is involved in an individual's care or payment for care; (3) for certain notification purposes, such as when an attending physician or a hospital social worker notifies a partner or spouse of a patient's death; and (4) for disaster relief activities.[68] If the individual who is the subject of the PHI is incapacitated, not available, or deceased, the covered entity may share PHI for these purposes if, in the covered entity's professional judgment, doing so is in the patient's best interest.[69] Thus, for example, a covered entity could notify the partner or spouse of a COVID-19 patient who is on a ventilator of the patient's current status.[70] By further example, a covered entity could notify a partner or spouse of a patient who died from COVID-19 of the occurrence of the death.[71] By still further example, a covered entity could share PHI with the American Red Cross as needed to obtain the American Red Cross's assistance with COVID-19 disaster relief activities.[72]

The HIPAA Privacy Rule's third use and disclosure requirement—a default rule—requires covered entities and BAs to obtain the prior written authorization of the individual who is the subject of the PHI before using or disclosing the individual's PHI in any situation that does not fit within the first two rules.[73] The HIPAA Privacy Rule requires these authorizations to contain a number of core elements and required statements.[74] This default authorization requirement was the topic of HHS's Second Guidance. There, HHS explained that a covered hospital or other covered health care facility, such as a nursing home, may not "give the media, including film crews, access to any areas of [the facility where patients or their] PHI will be accessible in any form . . . without first

67. *See* 45 C.F.R. § 164.510 (2019) (titled "Uses and disclosures requiring an opportunity for the individual to agree or object").
68. *See id.* §§ 164.510(a), (b)(1)(i)–(ii).
69. First Bulletin, *supra* note 36, at 4.
70. *See id.*
71. *See id.*
72. *See id.*
73. *See* 45 C.F.R. § 164.508(a)(1).
74. *Id.* §§ 164.508(c)(1)–(2) (listing the core elements and required statements of a HIPAA-compliant authorization form).

obtaining [the prior] written . . . authorization [of] each patient [who would be interviewed, photographed, or filmed, or] whose PHI would be accessible."[75] HHS also clarified that covered health care facilities are not permitted to condition a patient's admission to or treatment at the facility on the patient signing an authorization form giving the media access to the patient or the patient's PHI.[76]

2. The Individual Rights

In addition to the use and disclosure requirements, the HIPAA Privacy Rule also contains a second set of regulations establishing certain rights for individuals who are the subject of PHI vis-à-vis their covered entities, including the right to receive a notice of privacy practices (NOPP),[77] the right to request additional privacy protections and confidential communications,[78] the right to access PHI,[79] the right to request amendment of incorrect or incomplete PHI,[80] and the right to receive an accounting of PHI disclosures.[81] The NOPP requirement, in particular, was featured in HHS's HIPAA Rules Waiver.[82] There, HHS clarified that it would not impose sanctions and penalties against a covered hospital that does not distribute a NOPP for a period of up to seventy-two hours from the time the covered hospital implements its disaster protocol and before the termination of either Secretary Azar's PHE or President Trump's national emergency.[83] The NOPP requirement was also central in HHS's CBTS Enforcement Discretion.[84] There, HHS encouraged CBTSs to post a NOPP (or information about how to find the NOPP online) at the CBTS in a place that is readily viewable by individuals who approach the CBTS.[85] However, HHS clarified that it would not impose penalties for violations of the HIPAA Rules, including the NOPP requirement, that occur in connection with the good faith operation of a CBTS.[86] Additional rights, including the right to request additional privacy protections and confidential communications, were

75. Second Guidance, *supra* note 34, at 1.
76. *Id.*
77. 45 C.F.R. § 164.520.
78. *Id.* § 164.522.
79. *Id.* § 164.524.
80. *Id.* § 164.526.
81. *Id.* § 164.528.
82. *See* HIPAA Rules Waiver, *supra* note 14, at 1.
83. *Id.*
84. CBTS Enforcement Discretion, 85 Fed. Reg. 29,637, 29,637–38 (May 18, 2020).
85. *Id.* at 29,638.
86. *Id.*

central in HHS's HIPAA Rules Waiver as well.[87] As with the NOPP, HHS clarified in its Rules Waiver that it would not impose sanctions and penalties against a covered hospital that does effectuate these rights for a period of up to seventy-two hours from the time the covered hospital implements its disaster protocol and before the termination of either Secretary Azar's PHE or President Trump's national emergency.[88]

3. The Administrative Requirements

In addition to the use and disclosure requirements and the individual rights, the HIPAA Privacy Rule contains a third set of requirements known as the administrative requirements.[89] In particular, the HIPAA Privacy Rule requires covered entities to designate a privacy officer to oversee compliance with the HIPAA Privacy Rule, train workforce members regarding how to comply with the HIPAA Privacy Rule, sanction workforce members who violate the HIPAA Privacy Rule, establish a complaint process for individuals who believe their privacy rights have been violated, and develop privacy-related policies and procedures, among other similar requirements.[90]

B. The HIPAA Security Rule

The HIPAA Security Rule requires covered entities and BAs to implement administrative, physical, and technical safeguards designed to protect the confidentiality, integrity, and availability of electronic protected health information (ePHI).[91] In particular, the HIPAA Security Rule's administrative requirements obligate covered entities and BAs to designate a security official responsible for the development and implementation of the covered entity's or BA's security policies and procedures.[92] These policies and procedures shall: (1) "prevent, detect, contain, and correct security violations"; (2) ensure that workforce members have appropriate access to ePHI; (3) prevent workforce members who should not have access to ePHI from obtaining such access; (4) create a security awareness and training program for all workforce members; and (5) address and respond to security incidents,

87. *See* HIPAA Rules Waiver, *supra* note 14, at 1.
88. *Id.*
89. 45 C.F.R. § 164.530 (2019).
90. *Id.*
91. *Id.* § 160.103 (defining ePHI); *id.* §§ 164.302–.310 (establishing the security obligations of covered entities and BAs).
92. *Id.* § 164.308.

emergencies, environmental problems, and other occurrences such as fire, vandalism, system failure, and natural disaster that affect systems containing ePHI and the security of ePHI, among other requirements.[93]

In terms of physical safeguards, the HIPAA Security Rule requires covered entities and BAs to implement policies and procedures that: (1) limit physical access to electronic information systems and the facilities in which they are located; (2) address the safeguarding, functioning, and physical attributes of workstations through which ePHI is accessed; and (3) govern the receipt and removal of hardware and electronic media that contain ePHI.[94]

And, in terms of technical safeguards, the HIPAA Security Rule requires covered entities and BAs to implement: (1) "technical policies and procedures for electronic information systems that maintain [ePHI] to allow access only to those persons or software programs that have been granted access rights"; (2) "hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use [ePHI]"; (3) "policies and procedures to protect [ePHI] from improper alteration or destruction"; (4) "procedures to verify that a person or entity seeking access to [ePHI] is the one claimed"; and (5) "technical security measures to guard against unauthorized access to [ePHI] that is being transmitted over an electronic communications network."[95]

The HIPAA Security Rule was central to HHS's Telehealth Enforcement Discretion and to HHS's Telehealth FAQs. In the former, HHS stated that it would exercise enforcement discretion, including HIPAA Security Rule enforcement discretion, in the context of covered health care providers' good faith provision of nonpublic facing telehealth through products such as Skype, Zoom, FaceTime, Facebook Messenger, and Google Hangouts.[96] Although HHS encourages covered health care providers to notify patients that these third-party applications potentially introduce security risks and encourages health care providers to enable all available encryption and privacy modes when using these products, HHS stated in its Telehealth FAQs that it would not be imposing sanctions or penalties for security breaches, such as interceptions, that occur during a good faith telehealth session.[97]

93. *Id.*
94. *Id.* § 164.310.
95. *Id.* § 164.312.
96. *See* Telehealth Enforcement Discretion, 85 Fed. Reg. 22,024, 22,025 (Apr. 21, 2020).
97. *See* Telehealth FAQs, *supra* note 38, at 5–6 (specifically Question 11).

C. The HIPAA Breach Notification Rule

In addition to promulgating Privacy and Security Rules, HHS has also promulgated a Breach Notification Rule.[98] The HIPAA Breach Notification Rule requires covered entities, following the discovery of a breach[99] of unsecured protected health information (uPHI),[100] to "notify each individual whose [uPHI] has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach."[101] The notification, which shall be provided without undue delay and within sixty calendar days after the discovery of the breach, shall include: (1) a brief description of the nature of the breach, "including the date of the breach and the date of [its] discovery"; (2) a description of the types of uPHI involved in the breach; (3) "[a]ny steps [the] individual[ ]should take to protect [herself] from potential harm resulting from the breach"; (4) a brief description of the steps taken by the covered entity "to investigate the breach, to mitigate harm to individuals" whose uPHI was part of the breach, and to protect against future breaches; and (5) contact information sufficient to allow individuals to ask questions or learn additional information about the breach.[102]

When a breach involves the uPHI of more than 500 residents of a state or jurisdiction, the HIPAA Breach Notification Rule also requires the covered entity to "notify prominent media outlets serving the [s]tate or jurisdiction."[103] When a breach involves the uPHI of 500 or more individuals, regardless of their state of residency, the covered entity is also required to notify the Secretary of HHS within sixty calendar days after the discovery of the breach.[104] Finally, when the breach involves the uPHI of less than 500 individuals, the covered entity is required to notify the Secretary of HHS not later than sixty calendar days after the end of the calendar year.[105]

The HIPAA Breach Notification Rule was central to HHS's CBTS Enforcement Discretion.[106] There, HHS explained that its enforcement discretion does not protect "covered health care providers or their [BAs]

98. *See* 45 C.F.R. §§ 164.400–.414 (referencing the HIPAA Breach Notification Rule).
99. *Id.* § 164.402 (defining breach).
100. *Id.* (defining uPHI).
101. *Id.* § 164.404(a)(1).
102. *Id.* §§ 164.404(b)–(c).
103. *Id.* § 164.406(a).
104. *Id.* § 164.408(b).
105. *Id.* § 164.408(c).
106. *See* CBTS Enforcement Discretion, 85 Fed. Reg. 29,637, 29,638 (May 18, 2020).

when [they] are performing non-CBTS related activities, including the handling of PHI outside of the operation of a CBTS."[107] For example, HHS explained that

> [a] covered health care provider that experiences a breach of PHI in its existing electronic health record system, which includes PHI gathered from the operation of a CBTS, could be subject to a civil money penalty for violations of the HIPAA Breach Notification Rule if it fails to notify all individuals affected by the breach (including individuals whose PHI was created or received from the operation of a CBTS).[108]

III. COVID-19: ASKED AND ANSWERED

Although the HHS Guidance answers many basic questions about the application of the HIPAA Privacy Rule to the COVID-19 pandemic, the Author has been contacted by a number of journalists, lawyers, law students, and community members with additional HIPAA-related questions not addressed by the HHS Guidance. This Part II answers these questions and, in so doing, hopefully provides a guide for the proper use and disclosure of PHI under the HIPAA Rules during future public health emergencies.

A. Who Is a Covered Entity?

Many of the questions received by the Author may be categorized as "Who is a covered entity?" questions. For example, several community members have referenced media stories in which celebrities are reported as having tested positive or negative for SARS-CoV-2 or having died of COVID-19. These community members have then asked the Author whether the reports are evidence of HIPAA Privacy Rule violations by the reporters. As an illustration, *Vanity Fair* reported on April 3, 2020, that Joseph Maldonado-Passage (also known as Joe Exotic or the Tiger King) was quarantined in a federal prison medical center due to concerns that he had contracted SARS-CoV-2.[109] *Page Six* reported on April 9, 2020, that Real Housewife of New Jersey Jennifer Aydin tested

107. *Id.*
108. *Id.*
109. Yohana Desta, *Yes, Tiger King's Joe Exotic Is Under Quarantine Amid Coronavirus Concerns*, VANITY FAIR, Apr. 3, 2020, https://www.vanityfair.com/hollywood/2020/04/joe-exotic-coronavirus-tiger-king.

positive for SARS-CoV-2.[110] The *Reno Gazette Journal* reported on May 8, 2020, that Las Vegas entertainer Roy Horn (of Siegfried and Roy fame) died of COVID-19.[111] And, on June 15, 2020, *Sports Illustrated* reported that Dallas Cowboy Ezekiel Elliot believed that the HIPAA Privacy Rule had been violated when someone reported his positive SARS-CoV-2 test results without his prior written authorization.[112]

In response, it must be explained that the HIPAA Privacy Rule only regulates covered entities and BAs.[113] Newspaper reporters and other members of the media do not fall within the definition of a covered entity or a BA. As such, members of the media cannot violate the HIPAA Privacy Rule when they report the health conditions of celebrities and other persons of interest.

At this point, the Author usually receives a follow-up question asking whether the person who provided the information to the news reporter violated the HIPAA Privacy Rule. Many times, the source of the information is the patient herself. For example, Real Housewife of New Jersey Jennifer Aydin voluntarily shared her own bout of COVID-19 with the media.[114] As with news reporters, patients are not covered entities and are free to share their own PHI without regulation by the HIPAA Privacy Rule. Sometimes, however, the source of the information is the patient's family member or friend. For example, Dillon Passage (Joe Exotic's current husband) told *Vanity Fair* that Joe Exotic was in quarantine due to a possible COVID-19 exposure.[115] Siegfried Fischbacher told the *Reno Gazette Journal* that his partner Roy Horn died of COVID-19.[116] Again, however, family members and friends do not fall within the definition of a covered entity or BA under the HIPAA Privacy

110. Jaclyn Hendricks, *Jennifer Aydin of 'RHONJ' Reveals Coronavirus Diagnosis*, PAGE SIX, Apr. 9, 2020, https://pagesix.com/2020/04/09/rhonj-star-jennifer-aydin-tests-positive-for-coronavirus.

111. Brett McGinness & Ed Komenda, *Roy Horn of 'Siegfried and Roy' Dies of COVID-19 Complications*, RENO GAZETTE J., May 8, 2020, https://www.rgj.com/story/news/2020/05/08/roy-horn-siegfried-and-roy-dies-covid-19/3101571001/.

112. Bri Amaranthus, *Zeke Suggests HIPAA Violation Regarding Positive COVID-19 Test*, SPORTS ILLUSTRATED, June 15, 2020, https://www.si.com/nfl/cowboys/news/dallas-cowboys-star-ezekiel-elliiott-suggests-hipaa-violation-regarding-positive-covid-19-test.

113. *See supra* text accompanying notes 41–46 (defining covered entity, including a reference to the entities that fall within this definition, and business associate).

114. Hendricks, *supra* note 110.

115. Desta, *supra* note 109 (noting that Joe Exotic's husband, Dillon Passage, shared his husband's quarantined status with the media: "Husband Dillon Passage said that Exotic is being quarantined in a prison medical center, and that he hasn't been able to speak to Exotic since he was moved.").

116. McGinness & Komenda, *supra* note 111 (noting that Roy Horn's partner Siegfried Fischbacher shared Roy's death from COVID-19 with the media: "'Today, the world has lost one of the greats of magic, but I have lost my best friend . . . From the moment we met, I knew Roy and I, together, would change the world. There could be no Siegfried without Roy, and no Roy without Siegfried.'").

Rule. Although it is possible that a family member or friend could violate the partner's confidence in sharing the patient's information with the media, thus implicating state tort law or similar, the information sharing does not implicate the HIPAA Privacy Rule.[117]

Additional questions received by the Author (usually from colleagues in the legal academy and from her own law students) also may be categorized as "Who is a covered entity?" questions. As background, law faculty members and law students affiliated with law schools across the country are being asked to provide individually identifiable health information to their employers and universities in order to justify Americans with Disabilities Act (ADA) and other accommodations, such as teaching or attending class online versus in person. Faculty members and students also are being asked to provide individually identifiable health information to university administrators through online and mobile application-mediated screening portals and forms.[118] Faculty members and students who are concerned about the confidentiality and security of their data have asked the Author whether the federal government could impose civil or criminal penalties on their

117. The HHS Guidance does not specify with particularity that patients (or family members or friends of patients) are not regulated by the HIPAA Privacy Rule. In one piece of guidance, HHS does generically explain that

> [t]he HIPAA Privacy Rule applies to disclosures made by employees, volunteers, and other members of a covered entity's or business associate's workforce. Covered entities are health plans, health care clearinghouses, and those health care providers that conduct one or more covered health care transactions electronically, such as transmitting health care claims to a health plan. Business associates generally are persons or entities (other than members of the workforce of a covered entity) that perform functions or activities on behalf of, or provide certain services to, a covered entity that involve creating, receiving, maintaining, or transmitting protected health information. . . . The Privacy Rule does not apply to disclosures made by entities or other persons who are not covered entities or business associates (although such persons or entities are free to follow the standards on a voluntary basis if desired). There may be other state or federal rules that apply.

First Bulletin, *supra* note 36, at 5. Lay persons who are not skilled with reading and applying regulatory definitions cannot quickly determine from this paragraph that patients (and their friends and family members) are not covered entities or BAs.

118. *See, e.g.*, Letter from the University of Oklahoma, to all Employees, Students, Residents, and Mission-Critical Campus Visitors/Vendors, UNIV. OF OKLA. (Mar. 21, 2020), https://www.ou.edu/web/news_events/articles/news_2020/updated-travel-guidelines-and-online-screening-form (requiring University of Oklahoma faculty members and students to provide identifiable health information to the university via an online screening form in certain situations); *#CampusClear Daily Screening*, TEX. LUTHERAN UNIV., https://www.tlu.edu/covid-updates/staying-healthy-on-campus/campusclear-daily-screening (last visited Mar. 1, 2021) (requiring faculty and students at Texas Lutheran University (TLU) to complete daily self-screening and temperature attestations through the #CampusClear mobile application before entering TLU classrooms, buildings, and offices).

universities under the HIPAA Privacy Rule if an intentional or unintentional data breach or a cybersecurity incident occurs.

Whether and how the HIPAA Privacy Rule applies to a university depends on the different functions performed by the university and whether the university has designated itself as a "hybrid entity." As background, the HIPAA Privacy Rule defines a hybrid entity as "a single legal entity: (1) [t]hat is a covered entity; (2) [w]hose business activities include both covered and non-covered functions; and (3) [t]hat designates [its] health care components. . . ."[119] To the extent a university has a medical school, teaching hospital, student health center, or other health care provider that electronically bills health insurers, or to the extent a university has a group health plan that provides health insurance to its employees, the university most certainly performs covered functions.[120] Because most universities perform other, non-covered functions, such as operating a law school, running a music department, supporting a golf team, and running a book store, most universities have both covered and non-covered components. To the extent a university with both types of components designates its covered (versus non-covered) components, the university will meet the definition of a hybrid entity and the HIPAA Privacy Rule will only apply to the university's covered (but not non-covered) components.[121] As a result, the HIPAA Privacy Rule would apply to the university-operated health care provider and group health plan but would not apply to a law school (or other non-covered unit) that fails to protect its faculty members' and students' individually identifiable COVID-19 data.

B. What Is Protected Health Information?

Some of the questions received by the Author may be categorized as "What is protected health information?" questions. For example, sometimes a faculty member's or student's individually identifiable health information will be held by a HIPAA covered entity or a health care component of a hybrid entity. In this case, the HIPAA Privacy Rule technically applies to the covered entity or health care component of the hybrid entity in accordance with the rules discussed above. However, recall that the HIPAA Privacy Rule only applies to the use and disclosure

119. 45 C.F.R. § 164.103 (2019).

120. *See supra* text accompanying notes 41–45 (defining covered entity and referencing the entities that fall within the definition of covered entity).

121. 45 C.F.R. § 164.103 (defining hybrid entity); *id.* § 164.105(a)(1) (explaining that the HIPAA Privacy Rule only applies to a hybrid entity's covered health care components).

of "protected health information."[122] Further recall that, with four exceptions,[123] the HIPAA Privacy Rule defines PHI as individually identifiable health information. At least two of these exceptions are implicated by common COVID-19 scenarios presented to the Author.

The first exception excludes from the definition of PHI "employment records held by a covered entity in its role as [an] employer."[124] To the extent a university that is a covered entity or hybrid entity employs a law faculty member and the university requires that faculty member to disclose individually identifiable health information to the university (through a screening form, online portal, mobile application, or otherwise)[125] to determine whether the faculty member can present to work during the pandemic, that information is an employment record held by the university in its role as an employer of the employed law faculty member (not in its role as covered health care provider, health plan, or health care clearinghouse vis-à-vis the faculty member). Stated another way, the information that is collected is not PHI protected by the HIPAA Privacy Rule. Instead, the information is an employment record protected under employment law, which includes disability law.

The second exception excludes from the definition of PHI education records that are protected by the Family Education Rights and Privacy Act of 1974 (FERPA).[126] The regulations implementing FERPA define education records as "records that are: (1) [d]irectly related to a student; and (2) [m]aintained by an educational agency or institution or by a party acting for the agency or institution."[127] To the extent a university (or school or department on behalf of the university) collects or holds information relating to an identifiable student's COVID-19 status for purposes of determining whether the student can attend in-person classes or must stay at home for quarantine or isolation purposes, that information falls within the definition of an education record. FERPA, not HIPAA, protects that information.

---

122. *See id.* § 164.500(a) (stating that the HIPAA Privacy rule applies to "covered entities with respect to *protected health information*" (emphasis added)).

123. *See id.* § 160.103 (excluding from the definition of PHI individually identifiable health information that is: (1) in education records protected by FERPA; (2) in student treatment records; (3) "[i]n employment records held by a covered entity in its role as employer; and ([4]) [r]egarding a person who has been deceased for more than [fifty] years").

124. *Id.*

125. *See supra* note 118 (referencing online screening forms and mobile applications that collect individually identifiable temperature, symptom, and COVID-19-related information from employees of universities).

126. *See* 45 C.F.R. § 164.103.

127. *See* 34 C.F.R. § 99.3 (2019).

C. Can Covered Entities Disclose COVID Data to Funeral Homes?

One of the questions the Author has received repeatedly from news reporters relates to whether funeral homes that are collecting the bodies of hospital patients who have died from COVID-19 can obtain the decedents' COVID-19 status from the hospitals. Funeral homes want this information to protect themselves, their funeral workers, and the people who attend their funerals. However, some hospitals claim they cannot disclose patients' COVID-19 data to funeral homes without violating the HIPAA Privacy Rule.[128] Throughout the pandemic, journalists have asked the Author who is right: the funeral homes or the hospitals?

Although the HIPAA Privacy Rule vaguely addresses this question in the funeral homes' favor, the preamble to the HIPAA Privacy Rule clarifies that it would not violate the HIPAA Privacy Rule for a hospital to disclose a patient's infectious-disease status to a home that is directing a funeral. As background, the HIPAA Privacy Rule expressly provides that a covered entity may disclose PHI to funeral directors "as necessary to carry out their duties with respect to the decedent."[129] The HIPAA Privacy Rule does not clarify, however, what it means to "carry out their duties with respect to the decedent."[130] However, the preamble to the HIPAA Privacy Rule, which contains comments from the public as well as HHS's response to those comments, provides:

> *Comment*: . . . In addition, it was noted that funeral directors need to be aware of the presence of a contagious or infectious disease in order to properly advise family members of funeral and disposition options and how they may be affected by state law. For example, certain states may prohibit cremation of remains for a certain period unless the death was caused by a contagious or infectious disease, or prohibit family members from assisting in preparing the body for disposition if there is a risk of transmitting a communicable disease from the corpse.
>
> *Response:* We agree that disclosures to funeral directors for the above purposes should be allowed. Accordingly, the final rule at [45 C.F.R.] § 164.512(g)(2) permits covered entities to disclose protected health

128. *See, e.g.*, Antoinette DelBel, *Coronavirus Pandemic Forces Funeral Directors on the Front Line*, WTKR (Apr. 27, 2020), https://www.wtkr.com/news/coronavirus-pandemic-forces-funeral-directors-on-the-frontline (reporting that a funeral director who transports decedents from hospitals to his funeral home will not always be told by the hospital whether the decedent died of COVID-19).

129. 45 C.F.R. § 164.512(g)(2) (2016).

130. *Id.*

> information to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to the decedent. Such disclosures are also permitted prior to, and in reasonable anticipation of, the individual's death.[131]

D. Can Covered Entities Disclose PHI to Coroners and Medical Examiners?

A second question the Author has received repeatedly from news reporters relates to whether a physician, hospital, or other covered entity can disclose PHI to a coroner or medical examiner to help the coroner or medical examiner determine whether the patient's cause of death was COVID-19 or something else. The HIPAA Privacy Rule itself answers this question affirmatively. In particular, the HIPAA Privacy Rule provides: "A covered entity may disclose protected health information to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law."[132]

E. Can Covered Entities Disclose PHI about Inmates to Correctional Institutions?

A third question the Author has received repeatedly relates to whether a health care provider or laboratory can disclose an inmate's laboratory test result showing that the inmate tested positive for SARS-CoV-2 to the correctional institution in which the inmate is housed or the employees thereof of the correctional institution. The Author received this question numerous times early in the pandemic when Joe Exotic was quarantined in a federal medical center prison due to a concern that he had been exposed to COVID-19.[133] The HIPAA Privacy Rule answers this question in the affirmative. In particular, the HIPAA Privacy Rule states that

> [a] covered entity may disclose to a correctional institution . . . protected health information about such inmate . . . if the . . . [disclosure] is necessary for: (A) The provision of health care to such individuals; (B) The health and safety of such individual or other inmates; (C) The health and safety of the officers or employees of or others at the correctional institution; (D) The health and safety of

131. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,633 (Dec. 28, 2000).

132. 45 C.F.R. § 164.512(g)(1).

133. *See* Desta, *supra* note 109.

> such individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another; . . . or (F) The administration and maintenance of the safety, security, and good order of the correctional institution.[134]

F. Does the HIPAA Privacy Rule Require Covered Entities to Disclose COVID Data to Public Health Authorities?

A final question the Author has received repeatedly is whether the HIPAA Privacy Rule *requires* covered entities, such as physicians and laboratories, to disclose positive SARS-CoV-2 test results to public health authorities, including the CDC and state and local departments of health. As background, and as discussed above in Part I of this Article, the HIPAA Privacy Rule *permits* covered entities to disclose PHI to public health authorities as part of state mandatory disease reporting laws[135]: "For example, a covered entity *may* disclose to the CDC protected health information on an ongoing basis as needed to report all prior and prospective cases of patients exposed to or suspected or confirmed to have Novel Coronavirus (2019-nCoV)."[136] With two exceptions relating to disclosures to patients and disclosures to the Secretary of HHS, however, the HIPAA Privacy Rule does not *require* covered entities to disclose PHI to particular individuals or in particular situations. That said, news reporters, students, colleagues, and members of the community persist in their belief that health care providers and laboratories that do not disclose positive SARS-CoV-2 tests to public health authorities can have civil or criminal penalties imposed on them under the HIPAA Privacy Rule. The Author usually responds by explaining that health care providers that have mandatory disease reporting obligations under state law and that fail to satisfy those obligations risk civil, criminal, or administrative sanctions under state law but not civil or criminal penalties under the HIPAA Privacy Rule. In Oklahoma, where the Author currently works, the failure or refusal to report diseases in accordance with Oklahoma's mandatory disease reporting statute constitutes a misdemeanor.[137]

---

134. 45 C.F.R. § 164.512(k)(5).

135. *See, e.g.*, *id.* § 164.512(b)(1)(i).

136. First Bulletin, *supra* note 36, at 3 (emphasis added).

137. OKLA. STAT. ANN. tit. 36, § 1-503(a) (2019) ("The State Board of Health shall promulgate rules and regulations establishing a system of reporting of cases of diseases diagnosed or detected by practicing physicians and/or clinical laboratories which come within the purview of this article. A reporting system established by the Board shall be applicable to penal and eleemosynary

IV. CONCLUSION AND PROPOSALS

SARS-CoV-2, the virus that causes COVID-19, raises a number of important yet vexing privacy and security issues. Public health officials, law and policy makers, and members of the general public disagree, for example, regarding the amount and type of individually identifiable health data that should be collected, used, and disclosed for public health surveillance, public health investigation, and public health intervention. Stakeholders also diverge in their opinions regarding the sufficiency of federal and state data privacy and security laws. Some stakeholders believe that current statutes and regulations are sufficient to protect individually identifiable COVID-19 data whereas others contend that new privacy and security laws are needed. At a more basic level, stakeholders also vary in their understanding of the application of the HIPAA Rules to particular uses and disclosures of COVID-19 data.

This Article has responded to the varying levels of public understanding of HIPAA by: (1) summarizing the HIPAA Rules and assessing the many waivers, notices of enforcement discretion, guidance documents, bulletins, frequently asked questions, and webinars released by HHS during the COVID-19 pandemic; and (2) identifying and answering additional HIPAA Rules questions not addressed, or not sufficiently addressed, by the HHS Guidance. In addition, this Article proposes that HHS amend the process by which it issues pandemic-related guidance. As discussed in the Introduction, HHS issued a string of formal and informal guidance documents telling the public how the HIPAA Privacy Rule applies to the use and disclosure of PHI during the COVID-19 pandemic. These guidance documents, which were released at different times and were made available in different places (*e.g.*, some were published in the *Federal Register* while others were simply posted to HHS's website) included the HIPAA Rules Waiver, the Business Associate Enforcement Discretion, the Telehealth Enforcement Discretion, the CBTS Enforcement Discretion, the First Guidance, the Second Guidance, the Third Guidance, the First Bulletin, the Second Bulletin, the Telehealth FAQs and the Webinar.

Given that the Author teaches a HIPAA Privacy Law class every year, it is the Author's job to stay current on the HIPAA Privacy Rule. As such, she was able to follow the release of these varied guidance documents throughout the PHE. That said, the Author is certain that a member of

institutions. Failure or refusal to report diseases as required by the Board *shall constitute a misdemeanor*.") (emphasis added).

the lay public would not subscribe to all of the listservs, blogs, and *Federal Register* notices that would enable that person to follow the release of these guidance documents. In addition, many of the guidance documents repeat themselves. For example, the First Bulletin, the Second Bulletin, and the HIPAA Rules Waiver contain nearly identical language in several paragraphs, making it difficult for anyone but a lawyer or law professor to identify any new waivers or flexibilities announced by HHS.

In addition, many of the guidance documents contain technical advice that a lawyer or law professor would understand but that a community member would not. For example, simply providing a community member with the technical definition of a covered entity or a BA is not the same thing as explaining to the community member that a patient, or a family member or friend of a patient does not fall within the definition of a covered entity or BA and therefore is not regulated by the HIPAA Privacy Rule.[138] The Author finds HHS's less formal frequently asked questions (FAQs), such as the Telehealth FAQs, to be more helpful to community members in understanding how the HIPAA Rules apply to very specific questions. To this end, the Author recommends that HHS perhaps release fewer guidance documents and focus on one running guidance document that does not repeat itself—perhaps in the format of FAQs—that is posted in a place where community members can find it.

138. *See supra* note 117.