Summer 2021

At a COVID Crossroads : Public Health, Patient Privacy, and Health Information Confidentiality

Stacey A. Tovino, *University of Oklahoma College of Law*

AT A COVID CROSSROADS: PUBLIC HEALTH, PATIENT PRIVACY, AND HEALTH INFORMATION CONFIDENTIALITY

STACEY A. TOVINO*

ABSTRACT

This essay summarizes and assesses the various bulletins, guidance documents, and notices of enforcement discretion released by the federal Department of Health and Human Services regarding the application of the HIPAA Privacy Rule to the COVID-19 pandemic. Among other topics and actions, these authorities address the application of the HIPAA Privacy Rule to the use and disclosure of protected health information for public health activities, waive the application of certain HIPAA Privacy Rule requirements during the COVID-19 pandemic, and announce enforcement discretion regarding certain covered entities' non-compliance with particular provisions within the HIPAA Privacy Rule. These authorities overwhelmingly, and appropriately, prioritize the health, safety, and welfare of the public over individual rights to patient privacy and health information confidentiality during the COVID-19 pandemic.

* J.D., Ph.D., Professor of Law, The University of Oklahoma College of Law, Norman, Oklahoma.

INTRODUCTION

On October 2, 2020, the *Saint Louis University Law Journal* hosted "Tradeoffs: Technology, Privacy, and the Law," its first-ever virtually-presented Childress Lecture.[1] Following a keynote address by Orin Kerr, Professor of Law at the University of California, Berkeley School of Law, and an opening panel titled "The Fourth Amendment, Privacy, and Technology,"[2] the second panel examined the promise and perils of using technology to fight the severe acute respiratory syndrome coronavirus 2 ("SARS-CoV-2"), the virus that causes coronavirus disease 2019 ("COVID-19").[3] As the second speaker on the second panel, I addressed two topics at the intersection of public health, patient privacy, and health information confidentiality in the context of the COVID-19 pandemic, including: (1) relevant government guidance and legislative activity; and (2) the potential for individually identifiable data breaches involving COVID-19-related data, the informational injuries associated with such breaches, and the likely disparate impact of such breaches on minority and vulnerable populations. My remarks on the first topic are set forth below.[4]

I. GOVERNMENT GUIDANCE

To date, the public has received significant guidance from the federal Department of Health and Human Services ("HHS") regarding the application of the health information confidentiality rule that implements the Administrative Simplification provisions within the Health Insurance Portability and Accountability Act of 1996[5] ("HIPAA Privacy Rule")[6] to the COVID-19

1. *See Richard J. Childress Memorial Lecture*, SAINT LOUIS UNIVERSITY SCHOOL OF LAW, https://www.slu.edu/law/law-journal/programs/childress-lecture.php [https://perma.cc/7CQV-BFAH] ("On Oct. 2, 2020, the Law Journal hosted a 'virtual' Childress Lecture via Zoom.").

2. *Id.* ("Panels included 'The Fourth Amendment, Privacy, and Technology,' 'The Promise and Perils of Using Technology in Fighting Against COVID-19,' and 'Lawyering in an Interconnected World.' Orin Kerr, professor of law at the University of California, Berkeley School of Law, gave the keynote lecture, 'Email Preservation and the Fourth Amendment.'").

3. *See supra* note 1; *see also How Did COVID-19 Get its Name?*, CTRS. DISEASE CONTROL & PREVENTION, U.S. DEP'T OF HEALTH AND HUMAN SERVS., https://www.cdc.gov/coronavirus/2019-ncov/cdcresponse/about-COVID-19.html [https://perma.cc/7BPG-9X6H] (providing a video explaining how the disease COVID-19 was named).

4. My remarks on the second topic are beyond the scope of this essay, which was limited by the Journal to 3,500 words.

5. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 2021-34 (codified as amended in scattered sections of 42 U.S.C.) [hereinafter HIPAA] (amended in part by Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226 (codified as amended in scattered sections of 42 U.S.C.) [hereinafter HITECH]).

6. The HIPAA Privacy Rule is codified at 45 C.F.R. Part 164, Subpart E (45 C.F.R. §§ 164.500-.534 (2019)). In a number of prior publications, the author has carefully reviewed the history, application, and requirements of the HIPAA Privacy Rule. *See, e.g.*, Stacey A. Tovino,

pandemic. In particular, HHS has issued a number of helpful bulletins, guidance documents, and formal notices of enforcement discretion (collectively, "Authorities") that: (1) explain the application of the HIPAA Privacy Rule to the use and disclosure of protected health information ("PHI")[7] for public health activities; (2) waive the application of certain HIPAA Privacy Rule requirements during the pandemic; and/or (3) exercise enforcement discretion regarding certain covered entities' non-compliance with certain provisions within the HIPAA Privacy Rule.[8] As explained in more detail below, these Authorities overwhelmingly, and appropriately, in my opinion, prioritize the health, safety, and welfare of the public over individual rights to patient privacy and health information confidentiality.

For example, HHS issued a bulletin early in the COVID-19 pandemic ("First Bulletin") reminding the public that although HIPAA covered entities[9] are generally required by the HIPAA Privacy Rule to obtain a patient's prior written authorization before using or disclosing the patient's PHI,[10] this requirement is waived during the conduct of certain public health activities.[11] In particular,

Assumed Compliance, 72 ALA. L. REV. 279, 286 (2020); Stacey A. Tovino, *Going Rogue: Mobile Research Applications and the Right to Privacy*, 95 NOTRE DAME L. REV. 155, 179–81 (2019) [hereinafter *Going Rogue*]; Stacey A. Tovino, *A Timely Right to Privacy*, 104 IOWA L. REV. 1361,1367–69 (2019); Stacey A. Tovino, *Patient Privacy: Problems, Perspectives, and Opportunities*, 27 ANNALS HEALTH L. 243, 244–47 (2018); Stacey A. Tovino, *The EU GDPR and the HIPAA Privacy Rule: Illustrative Comparisons*, 47 SETON HALL L. REV. 973, 974–78 (2017); Stacey A. Tovino, *Teaching the HIPAA Privacy Rule*, 61 ST. LOUIS U. L.J. 469, 470, 475 (2017) (collectively, "Prior Publications"). A discussion of the individuals and institutions that are regulated by the HIPAA Privacy Rule, the information that is protected by the HIPAA Privacy Rule, and the use and disclosure requirements set forth in the HIPAA Privacy Rule are beyond the scope of this essay, although this information is available in the author's Prior Publications. Any descriptions of particular HIPAA Privacy Rule requirements set forth in this essay are taken from these Prior Publications with the permission of the author.

7. 45 C.F.R. § 164.500(a) (explaining that the HIPAA Privacy Rule "appl[ies] to covered entities" with respect to "protected health information"); *id.* § 160.103 (2017) (defining PHI with reference to "individually identifiable health information" ("IIHI")); *id.* (defining IIHI as 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).

8. *See infra* notes 11, 19, 21, 29, 33, 34, and 35.

9. 45 C.F.R. § 160.103 (defining "covered entity" and "business associate"); *id.* §§ 164.500(a)–(c) (applying the HIPAA Privacy Rule to "covered entities" and "business associate[s]").

10. *Id.* § 164.508(a) (setting forth the prior written authorization requirement).

11. *See Bulletin: HIPAA Privacy and Novel Coronavirus*, U.S. DEP'T HEALTH & HUMAN SERVS. (Feb. 2020), https://www.hhs.gov/sites/default/files/february-2020-hipaa-and-novel-corona virus.pdf [https://perma.cc/YT8X-5C2J] [hereinafter First Bulletin]; *see also* 45 C.F.R. §

HHS explained that physicians, laboratories, and other mandated disease reporters are not required to obtain prior patient authorization before disclosing individually identifiable SARS-CoV-2 test results to a public health authority such as the federal Centers for Disease Control and Prevention and the Oklahoma State Department of Health.[12]

In its First Bulletin, HHS also reminded the public that public health investigations, including old-fashioned, person-to-person contact tracing as well as electronic contact tracing and exposure notification[13] can occur without the prior written authorization of the patient who is the source of the exposure.[14] As background, some contact tracers do not fall within the definition of a HIPAA covered entity,[15] and public health authorities normally instruct contact tracers not to disclose individually identifiable health information that is protected by the HIPAA Privacy Rule during their communications with contacts.[16] That said, to the extent a contact determines or guesses the identity of person who is the source of the contact's exposure after speaking with a HIPAA-covered

164.512(b) (setting forth a number of public health activities for which covered entities can use and disclose PHI without obtaining prior patient authorization, including disease reporting).

12. 45 C.F.R. § 164.512(b)(1)(i) (permitting covered entities to disclose PHI to a public health authority for purposes of disease reporting); *id.* § 164.512(a) (permitting covered entities to disclose PHI as required by other law); OKLA. ADMIN. CODE §§ 310:515-1-3(9)–(11) (2019) (an "other" law that requires health care practitioners and laboratories to disclose the "novel coronavirus" and other "apparent outbreaks of infectious disease" (both of which would include SARS-CoV-2) to the Oklahoma State Department of Health).

13. *See Contact Tracing for COVID-19*, CTRS. FOR DISEASE CONTROL & PREVENTION, U.S. DEP'T OF HEALTH AND HUMAN SERVS., https://www.cdc.gov/coronavirus/2019-ncov/php/contact-tracing/contact-tracing-plan/contact-tracing.html [https://perma.cc/F3CQ-86BN] [hereinafter CDC on Contact Tracing] (explaining that "[a] close contact to a patient with confirmed or probable COVID-19 should be notified of their exposure as soon as possible . . . Contacts can be notified through different channels such as phone, text, email, or in-person (if appropriate) in the primary language of the individual."; further providing a helpful contact tracing diagram).

14. *See* First Bulletin*, supra* note 11, at 4 (explaining that covered entities are permitted by the HIPAA Privacy Rule to disclose PHI to "persons at risk of contracting or spreading a disease or condition if other law, such as state 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."); 45 C.F.R. § 164.512(b)(1)(iv) (setting forth a number of public health activities for which covered entities can use and disclose PHI without obtaining prior patient authorization, including disclosures to "[a] person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if the covered entity or public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation").

15. *See* Stacey A. Tovino, *COVID-19 and the HIPAA Privacy Rule: Asked and Answered*, 50 STETSON L. REV. 365, 379–82 (2021) (analyzing the question of who is regulated by the HIPAA Privacy Rule in the context of the COVID-19 pandemic).

16. *See, e.g.*, CDC on Contact Tracing, *supra* note 13 (explaining that, in appropriately conducted contact tracing, "The identity of the patient or other identifying information will not be revealed, alluded to, or confirmed by the contact tracer, even if explicitly asked by a contact.").

contact tracer, the HIPAA Privacy Rule has not been violated even if the contact tracer did not obtain the written authorization of the person who is the source of exposure.[17] Again, HHS has prioritized the health, safety, and welfare of the public, including individuals who have been exposed to COVID-19, over the confidentiality and privacy rights of the individual with COVID-19.

HHS also reminded the public of several other situations in which a covered entity may disclose PHI for a public health activity without the prior written authorization of the individual who has COVID-19. For example, HHS reminded the public that HIPAA covered entities are permitted 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, correctional officers, paramedics, and other first responders without the individual's prior written authorization.[18] HHS further reminded covered entities that the HIPAA Privacy Rule permits covered entities to contact patients "who have recovered from COVID-19 to provide them with information about donating blood and plasma that could help other patients with COVID-19."[19] HHS clarified that this contact can occur without the prior written authorization of the recovered patients so long as the blood or plasma donation center does not exchange remuneration with the covered entity providing the information to the recovered patient.[20] The permissions described in this paragraph and the two preceding paragraphs evidence HHS's intent to prioritize the health, safety, and welfare of the public over the confidentiality and privacy rights of individuals with COVID-19 and individuals who have recovered from COVID-19.

HHS's decision to prioritize public health and safety over patient privacy is further illustrated by the agency's waiver ("Waiver") of sanctions and penalties that arise from a covered hospital's noncompliance with certain requirements within the HIPAA Privacy Rule.[21] These requirements relate to honoring a patient's request to opt out of a health care provider's facility directory,[22]

17. *See* First Bulletin*, supra* note 11; 45 C.F.R. § 164.512 (b)(1)(iv).

18. First Bulletin, *supra* note 11, at 4.

19. *Guidance on HIPAA and Contacting Former COVID-19 Patients about Blood and Plasma Donation*, U.S. DEP'T HEALTH & HUMAN SERVS. (Aug. 2020), https://www.hhs.gov/sites/default/files/guidance-on-hipaa-and-contacting-former-covid-19-patients-about-blood-and-plasma-donation.pdf [https://perma.cc/82LK-HLXN].

20. *Id.*

21. *COVID-19 & HIPAA Bulletin: Limited Waiver of HIPAA Sanctions and Penalties During a Nationwide Public Health Emergency*, U.S. DEP'T HEALTH & HUMAN SERVS. (Mar. 2020), https://www.hhs.gov/sites/default/files/hipaa-and-covid-19-limited-hipaa-waiver-bulletin-508.pdf [https://perma.cc/UPA4-JP7E] [hereinafter HIPAA Rules Waiver].

22. *See* 45 C.F.R. § 164.510(a)(2) ("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 . . .").

obtaining a patient's agreement before speaking with family members or friends,[23] giving patients a notice of privacy practices describing how and when the covered entity will use and disclose the patients' PHI,[24] giving patients the right to request additional privacy restrictions relating to their PHI,[25] and giving patients the right to request confidential communications of their PHI.[26] Effective March 15, 2020, HHS formally issued the Waiver, clarifying that it applies to: (1) HIPAA-covered hospitals that have instituted a disaster protocol; (2) for a period of up to seventy-two hours from the time a covered hospital has implemented its disaster protocol; and (3) until the termination of the public health emergency ("PHE") declared by HHS Secretary Alex Azar[27] or the national emergency proclaimed by former President Donald Trump.[28] With the Waiver, HHS is signaling its desire for hospitals to focus on patient care, not privacy paperwork and patient requests for additional privacy restrictions, during the COVID-19 pandemic.

HHS's intent to prioritize public health and safety over patient privacy and health information confidentiality is further evidenced by the three HIPAA-related Notices of Enforcement Discretion the agency has issued since the start of the PHE. On April 7, 2020, for example, HHS published in the *Federal*

23. *Id.* § 164.510(b)(1)(i) ("A covered entity may . . . 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 . . .").

24. *Id.* § 164.520(c)(2)(j) ("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.").

25. *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).").

26. 45 C.F.R. § 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.").

27. *See* Alex M. Azar II, Secretary, U.S. DEP'T HEALTH & HUMAN SERVS., *Determination that a Public Health Emergency Exists*, https://www.phe.gov/emergency/news/healthactions/phe/Pages/2019-nCoV.aspx [https://perma.cc/3RTH-9X3S]. Secretary Azar made his PHE determination made retroactive to January 27, 2020.

28. *See* Proclamation No. 9994, 85 Fed. Reg. 15,337 (Mar. 13, 2020); HIPAA Rules Waiver, *supra* note 21 (clarifying the application of the HIPAA Rules Waiver).

Register a Notice of Enforcement Discretion for business associates ("Business Associate Enforcement Discretion").[29] In its Business Associate Enforcement Discretion, HHS encouraged business associates ("BAs") of HIPAA-covered entities to perform public health data analytics even if the BAs were not authorized to perform such analytics by the health information confidentiality contracts (known as business associate agreements ("BAAs")) the BAs signed before commencing work on behalf of their covered entity clients.[30] Moreover, on April 21, 2020, HHS published a second Notice of Enforcement Discretion ("Telehealth Enforcement Discretion") regarding the HIPAA Privacy, Security,[31] and Breach Notification Rules,[32] (collectively "HIPAA Rules") in the context of covered health care providers' good faith provision of non-public facing telehealth.[33] In the Telehealth Enforcement Discretion, HHS took the position that social distancing (and increased access to telehealth, which would support such social distancing) should be prioritized over any privacy and

29. 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] (codified at 45 C.F.R. pt. 160, 164). As background, the HIPAA Privacy Rule traditionally allows a business associate ("BA") of a covered entity to use and disclose PHI 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. However, 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. *Id.* Apparently, some BAs did not respond to these requests because their BAAs did not expressly permit them to make the requested uses and disclosures. *Id.* 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 public health data and health oversight activities. *Id.*

30. *See id.* at 19, 393.

31. 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. Part 164, Subpart C (45 C.F.R. §§ 164.302-.318) [hereinafter HIPAA Security Rule].

32. HHS's breach notification regulations, which implement section 13402 of HITECH [42 U.S.C. § 17932], are codified at 45 C.F.R. Part 164, Subpart D (45 C.F.R. §§ 164.400-.414) [hereinafter HIPAA Breach Notification Rule].

33. Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency, 85 Fed. Reg. 22,024 (Apr. 21, 2020) [hereinafter Telehealth Enforcement Discretion]. According to HHS, non-public facing telehealth products include Skype, Zoom, FaceTime, Facebook Messenger, and Google Hangouts. *Id.* Although HHS did not define the "good faith" provision of non-public facing telehealth in its Enforcement Discretion, HHS did state that enforcement discretion would not be applied to situations involving "bad faith." *Id.* 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 non-public facing) remote communication products, such as Facebook Live, Twitch, and TikTok. *Id.*

confidentiality concerns or risks associated with intercepted telecommunications, such as Zoom bombing. Finally, on May 18, 2020, HHS published a third Notice of Enforcement Discretion ("CBTS Enforcement Discretion"), this time for community-based testing sites ("CBTSs").[34] In the CBTS Enforcement Discretion, HHS prioritized the public's access to SARS-CoV-2 specimen collection and COVID-19 testing over patient privacy and health information confidentiality.

Notwithstanding these illustrations of public health priority, HHS issued one guidance document reminding covered hospitals and other health care facilities that prior written authorization from a patient or the patient's legal representative must be obtained before a journalist, news reporter, camera person, or film crew would be permitted to enter an intensive care unit or other treatment area and see patients with COVID-19 or access their PHI.[35] Even during the COVID-19 pandemic, HHS continues to subordinate general news reporting and other marketing and communications activities to patient privacy and health information confidentiality.[36]

II. LEGISLATIVE ACTIVITY

In summary—and with the exception of access to health care facilities by news reporters, journalists, camera persons, and video crews—the federal government has prioritized a wide range of communicable disease testing, health care delivery, public health surveillance, public health investigation, and public health intervention activities over patient privacy and health information confidentiality. That said, the federal government's focus on the application of the HIPAA Privacy Rule to the COVID-19 pandemic must be viewed in light of the HIPAA Privacy Rule's limited application; that is, the HIPAA Privacy Rule only applies to covered entities, namely certain (but not even all) health care

34. 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]. In the CBTS Enforcement Discretion, HHS announced that it would not impose penalties for noncompliance with the HIPAA Rules by covered health care providers and their business associates who participate in good faith in the operation of a community-based testing site during the PHE. As explained in the Enforcement Discretion, CBTSs include "mobile, drive-through, or walk-up sites that only provide COVID-19 specimen collection or testing services to the public." *Id.* Although the Office for Civil Rights ("OCR") within HHS encourages covered health care providers and business associates operating CBTSs to implement a number of reasonable safeguards to protect the privacy and security of individuals' PHI, OCR also 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. *Id.*

35. *Guidance on Covered Health Care Providers and Restrictions on Media Access to Protected Health Information about Individuals in Their Facilities*, U.S. DEP'T HEALTH & HUMAN SERVS., https://www.hhs.gov/sites/default/files/guidance-on-media-and-film-crews-access-to-phi.pdf [https://perma.cc/9LDU-GGFD].

36. *See id.*

providers, health plans, and health care clearinghouses, as well as the business associates thereof.[37] The HIPAA Privacy Rule does not apply to many of the technology companies, mobile application developers, newspaper reporters, and other data harvesters, gatherers, and researchers that collect, analyze, use, and disclose COVID-19-related data for a wide variety of purposes and activities.[38]

In an attempt to respond to the limited reach of the HIPAA Privacy Rule (both before and after the start of the COVID-19 pandemic), lawmakers have introduced a number of new patient privacy and health information confidentiality bills. In December 2018, for example, Senator Brian Schatz (D-HI) introduced the Data Care Act, which would establish duties of care, loyalty, and confidentiality for online service providers that handle individually identifiable health information.[39] In June 2019, Senator Amy Klobuchar (D-MN) introduced the Protecting Personal Health Data Act, which would direct the Secretary of HHS to promulgate regulations that would strengthen privacy and security protections for "personal health data" collected, processed, analyzed, or used by consumer devices, services, applications, or software.[40] A few months later, in October 2019, Senator Ron Wyden (D-OR) introduced the Mind Your Own Business Act, which would require the FTC to promulgate regulations obligating certain entities to implement reasonable cybersecurity and privacy policies, practices, and procedures to protect "personal information."[41]

In November of 2019—closer to the beginning of the COVID-19 pandemic—Senator Bill Cassidy (R-LA) introduced the Smartwatch Data Act, which would prohibit certain entities that collect consumer health information ("CHI") from transferring or selling CHI to information brokers who collect or analyze CHI for profit.[42] On May 7, 2020,—during the heart of the COVID-19 pandemic—Senator Roger Wicker (R-MS) introduced the COVID-19 Consumer Data Protection Act, designed protect the privacy of consumers' personal health information, proximity data, device data, and geolocation data during the pandemic.[43] One week later, on May 14, 2020, Senator Richard Blumenthal (D-CT) introduced the Public Health Emergency Privacy Act, which would establish rights to privacy and security in the context of COVID-19 emergency health data.[44] The legislative initiatives referenced in this

37. *See* Tovino, *supra* note 15, at 379–82 (discussing the limited application of the HIPAA Privacy Rule in the context of the COVID-19 pandemic).

38. *See* Tovino, *Going Rogue*, *supra* note 6 (discussing the limited application of the HIPAA Privacy Rule in the context of mobile health and mobile health research applications).

39. Data Care Act of 2018, S. 3744, 115th Cong., § 3, (2018).

40. Protecting Personal Health Data Act, S. 1842, 116th Cong., (2019).

41. Mind Your Own Business Act of 2019, S. 2637, 116th Cong., (2019).

42. Stop Marketing and Revealing the Wearables and Trackers Consumer Health (Smartwatch) Data Act, S. 2885, 116th Cong., (2019).

43. COVID-19 Consumer Data Protection Act, S. 3663, 116th Cong., (2020).

44. Public Health Emergency Privacy Act, S. 3749, 116th Cong., (2020).

paragraph and the preceding paragraph evidence lawmaker and constituent desire for additional privacy and security regulation of non-HIPAA covered entities as well as concerns regarding the collection, analysis, use, and disclosure of COVID-19-related data.

CONCLUSION

This essay has shown that HHS has issued a number of Authorities during the COVID-19 pandemic that: (1) explain the application of the HIPAA Privacy Rule to uses and disclosures of PHI for public health activities; (2) waive the application of certain HIPAA Privacy Rule requirements during the pandemic; and/or (3) exercise enforcement discretion regarding certain covered entities' non-compliance with certain provisions within the HIPAA Privacy Rule. This essay has also shown that these Authorities overwhelmingly, and appropriately, in my opinion, prioritize the health, safety, and welfare of the public over individual rights to patient privacy and health information confidentiality. Although many people recover from COVID-19, the disease is fatal in a small percentage of cases.[45] Individual rights to confidentiality and privacy must give way to efforts to save the lives of law enforcement, correctional officers, paramedics, and other first responders, as well as the general public.

As the third speaker on the second panel noted, individually identifiable and re-identifiable data breaches may have a disparate impact on minorities and other vulnerable populations.[46] One way to protect these vulnerable individuals would be to extend the HIPAA Privacy Rule (and the civil and criminal penalties that come with it) to non-covered entities and to promulgate new regulations that would better protect the collection, use, disclosure, and re-disclosure of COVID-19-specific data for non-public health activities. To date, not one of the new legislative initiatives described in this essay has been signed into law. It is my hope that new and/or strengthened privacy and confidentiality protections will be promulgated before informational injuries associated with the secondary use, disclosure, and re-disclosure of COVID-19 data occurs in vulnerable and other populations.

45. *See, e.g.*, *Coronavirus Resource Center-Mortality Analyses*, JOHNS HOPKINS UNIVERSITY, https://coronavirus.jhu.edu/data/mortality [https://perma.cc/6JMS-S5EW] (listing the case-fatality rate (*i.e.*, the number of deaths divided by the number of confirmed cases) by country; reporting, for example, that the United States has a 2.0% case-fatality rate).

46. Nicol Turner Lee, Director of the Center for Technology Innovation at Brookings Institution, Governance Studies, Address at the Saint Louis University School of Law Journal Childress Lecture (Oct. 2, 2020).