

Georgia State University Law Review

Volume 37
Issue 1 Fall 2020

Article 14

12-1-2020

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996: Health & Public Welfare


Erin L. Hayes

Georgia State University College of Law, ehayes18@student.gsu.edu

Kathryn A. Vance

Georgia State University College of Law, kvance6@student.gsu.edu

Follow this and additional works at: <https://readingroom.law.gsu.edu/gsulr>

 Part of the [Health Law and Policy Commons](#), [Public Health Commons](#), and the [State and Local Government Law Commons](#)

Recommended Citation

Erin L. Hayes & Kathryn A. Vance, *HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996: Health & Public Welfare*, 37 GA. ST. U. L. REV. 153 (2020).

Available at: <https://readingroom.law.gsu.edu/gsulr/vol37/iss1/14>

This Peach Sheet is brought to you for free and open access by the Publications at Reading Room. It has been accepted for inclusion in Georgia State University Law Review by an authorized editor of Reading Room. For more information, please contact gfwke@gsu.edu.

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996

*Health: Discussing Title 31 of the Official Code of Georgia
Annotated, Relating to the Notification of Disease and the Control
of Hazardous Conditions, Preventable Diseases, and Metabolic
Disorders & Public Welfare: Discussing Title 45 of the Code of
Federal Regulations, Relating to the Department of Health and
Human Services, and Administrative Data Standards and Related
Requirements*

CODE SECTION:	O.C.G.A. § 31-12-2
C.F.R. SECTIONS:	45 C.F.R. §§ 160, 164
SUMMARY:	The Standards for Privacy of Individually Identifiable Health Information (“Privacy Rule”) establish a standard for the use and protection of individuals’ health information and apply to certain covered entities or their business associates. Covered entities may only disclose an individual’s protected health information in limited situations. Covered entities or individuals that fail to comply with the Privacy Rule standards may be subject to civil or criminal penalties.

Introduction

In late August of 1996, Congress enacted a law that has been likened to a Leo Tolstoy novel.¹ This reference is due in part to the epic, detailed, and comprehensive scheme that the Health Insurance Portability and Accountability Act lays out; but also, like the Russian tragedies Tolstoy is so famous for, the Act has evoked many

1. INST. OF MED., BEYOND THE HIPAA PRIVACY RULE: ENHANCING PRIVACY, IMPROVING HEALTH THROUGH RESEARCH 153 (Sharyl J. Nass et al. eds., 2009); Daniel Solove, *HIPAA Turns 10: Analyzing the Past, Present and Future Impact*, 84 J. AHIMA 22, 23 (2013).

emotions from the healthcare industry, ranging from confusion to angst.² The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was originally created to achieve two main goals: (1) to protect individuals and their families from losing their health insurance if they lost or changed their job; and (2) to reduce waste and fraud in the healthcare industry by creating a uniform electronic system for storing and sharing health data.³

Prior to HIPAA's enactment, most health data was managed and exchanged in paper format.⁴ To further complicate matters, many states had varying privacy laws, creating puzzling situations for those working or moving across state lines.⁵ The absence of uniform standards and requirements for protecting health information coupled with the advancement of technologies within the healthcare industry prompted the formulation of HIPAA.⁶ HIPAA served as the vehicle to modernize health data storage, tracking, and exchange.⁷ The Act was divided into five Titles that provided protection for health insurance coverage of workers, rules regarding privacy and administrability, and guidelines for ensuring compliance with the Act.⁸

While all Titles of the Act work together to create a scheme to efficiently and securely manage protected health information (PHI), Title II provides the majority of the provisions regarding the safe-keeping, sharing, and enforcement requirements for healthcare providers and others who handle PHI.⁹ This *Peach Sheet* focuses

2. Solove, *supra* note 1.

3. *Why Was HIPAA Created?*, HIPAA GUIDE: HEALTHCARE COMPLIANCE (Oct. 9, 2017), <https://www.hipaaguide.net/why-was-hipaa-created/> [<https://perma.cc/4DUC-XNFT>].

4. Solove, *supra* note 1.

5. *Why Is the HIPAA Privacy Rule Needed?*, U.S. DEP'T OF HEALTH & HUM. SERVS., <https://www.hhs.gov/hipaa/for-professionals/faq/188/why-is-the-privacy-rule-needed/index.html> [<https://perma.cc/SJY2-D5Q3>] (Nov. 9, 2006); Solove, *supra* note 1, at 23–24.

6. Solove, *supra* note 1, at 23–24.

7. *Id.*

8. *See generally* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104–191, 110 Stat. 1936. Title I addresses “Healthcare Access, Portability, and Renewability.” *Id.* §§ 101–195, 110 Stat. at 1939–91. Title II addresses “Preventing Health Care Fraud and Abuse; Administrative Simplification; [and] Medical Liability Reform.” *Id.* §§ 200–271, 110 Stat. at 1991–2037. Title III addresses “Tax-Related Health Provisions.” *Id.* §§ 300–371, 110 Stat. at 2037–73. Title IV addresses “Application and Enforcement of Group Health Plan Requirements.” *Id.* §§ 401–421, 110 Stat. at 2037–89. Title V addresses “Revenue Offsets.” *Id.* §§ 500–521, 110 Stat. at 2089–2103.

9. *Id.* §§ 200–271, 110 Stat. at 1991–2037.

specifically on Title II and its implications for PHI during the COVID-19 pandemic.

Overview of Title II

Title II can be broken down into five parts or “rules.”¹⁰ These five rules address privacy, transactions and code sets, security, unique identifiers, and enforcement, respectively.¹¹ The first section, the Privacy Rule, outlines the goal for the entire Title: to prevent fraud and abuse of PHI.¹² Zeroing in on the Privacy Rule alone seems like enough focusing of the lens within the vast landscape of HIPAA. However, it stands that the yarn of the narrative needs more unravelling to create a suitable background for this Peach Sheet’s discussion. More specifically, the Privacy Rule protects “individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or medium, whether electronic, on paper, or oral.”¹³ This includes information that relates to physical or mental health, the provision of health care, or any form of payment for health care of an individual that “identifies the individual or provides a reasonable basis to believe the information can be used to identify the individual.”¹⁴ Individually identifiable information includes names, addresses, social security numbers, or birth dates when this information is associated with health data.¹⁵

The need to protect this information stems not only from the fear of fraud but also from consideration of the implications an individual’s health data may have on their employment or health insurance status. For example, the Privacy Rule protects an individual’s psychiatric records and rehabilitation records, which

10. A Brief Background on the HIPAA Rules and the HITECH Act of *HIPAA Rules*, HIPAA SURVIVAL GUIDE, <http://www.hipaasurvivalguide.com/hipaa-rules.php> [<https://perma.cc/SY4N-4NL2>].

11. *Id.*

12. *What Does the HIPAA Privacy Rule Do?*, U.S. DEP’T OF HEALTH & HUM. SERVS., <https://www.hhs.gov/hipaa/for-individuals/faq/187/what-does-the-hipaa-privacy-rule-do/index.html> [<https://perma.cc/N38X-W2UW>] (July 26, 2013).

13. *Summary of the HIPAA Privacy Rule*, U.S. DEP’T OF HEALTH & HUM. SERVS. [hereinafter *HIPAA Summary*], <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html> [<https://perma.cc/SWP8-4WDE>] (July 26, 2013).

14. *Id.*

15. *Id.*

prevents potential employers from discriminating against applicants based on past medical history. Additionally, it is imperative to protect the privacy of individuals living with conditions and diseases that carry a negative stigma because the presence of these conditions could hinder employment opportunities and living or social situations.¹⁶ Under the Privacy Rule, individuals may authorize disclosure of their PHI.¹⁷ This authorization requires written consent from the individual that includes, among other things, a description of the information being disclosed, the individual making the disclosure, the party to whom the disclosure is being made, the expiration date for allowable disclosures, and occasionally, how the information will be used.¹⁸ The Privacy Rule also contains several other requirements pertaining to the notices and copies of authorization that are to be provided to the patient.¹⁹

In total, the Privacy Rule also enumerates six exceptions that allow for, but do not require, disclosure of a patient's PHI.²⁰ These six exceptions encompass: (1) disclosures to the individual; (2) disclosures for treatment or payment purposes; (3) authorized disclosures; (4) disclosures of incidental information; (5) disclosures for benefit of public interest; and (6) disclosures where personally identifiable information has been removed.²¹

To facilitate the last exception, HIPAA created a "De-identification Standard," which states that "health information is not individually identifiable if it does not identify an individual and if

16. Dealing with Stigma and Discrimination of HIV, CTRS. FOR DISEASE CONTROL & PREVENTION, <https://www.cdc.gov/hiv/basics/livingwithhiv/stigma-discrimination.html> [https://perma.cc/QU7N-4Q6U] (Aug. 6, 2019); *Mental Health: Overcoming the Stigma of Mental Illness*, MAYO CLINIC (May 24, 2017), <https://www.mayoclinic.org/diseases-conditions/mental-illness/in-depth/mental-health/art-20046477> [https://perma.cc/NK8N-4XDX].

17. *HIPAA Summary*, *supra* note 13.

18. *Disclosures for Emergency Preparedness – a Decision Tool: Authorization*, U.S. DEP'T OF HEALTH & HUMAN SERVS., <https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/authorization/index.html> [https://perma.cc/79JY-EQ3D] (July 26, 2013).

19. Kim Stanger, *Valid HIPAA Authorizations: A Checklist*, HOLLAND & HART LLP (Nov. 25, 2014), <https://www.hollandhart.com/valid-hipaa-authorizations-a-checklist> [https://perma.cc/DN27-G7KX].

20. Patrick Ouellette, *HIPAA Privacy Rule: Permitted PHI Uses and Disclosures*, HEALTHITSECURITY XTELLIGENT HEALTHCARE MEDIA (June 17, 2014), <https://healthitsecurity.com/news/hipaa-privacy-rule-permitted-phi-uses-and-disclosures> [https://perma.cc/V83Q-EWJS].

21. *Id.*

the covered entity has no reasonable basis to believe it can be used to identify an individual.”²² HIPAA further details two separate methods to ensure de-identification of PHI.²³

The fifth exception, which allow disclosure for the benefit of public interest, details twelve national priority purposes that trigger the exception and permit disclosure without authorization or permission from an individual.²⁴ One of the twelve national priority purposes includes “public health activities.”²⁵ Public health activities allowed under this exception include: (1) situations in which “public health authorities [are] authorized by law to collect or receive such information for preventing or controlling disease, injury, or disability and to public health or other government authorities authorized to receive reports of child abuse and neglect”; (2) use for U.S. Food and Drug Administration (FDA) tracking for entities regulated by the FDA; (3) situations in which “individuals who may have contracted or been exposed to a communicable disease [and] notification is authorized by law”; and (4) situations in which employers are seeking information concerning a work-related illness or injury.²⁶

State and Federal Law Interaction

It is important to note that circumstances leading to preemption may be an issue because HIPAA is federal law. Generally, due to the comprehensive regulatory scheme HIPAA provides, federal law preempts state laws contrary to the Privacy Rule.²⁷ However, there

22. *Guidance Regarding Methods for De-Identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, U.S. DEP’T OF HEALTH & HUM. SERVS., <https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html> [<https://perma.cc/62YF-YX94>] (Nov. 6, 2015).

23. *Id.* There are two methods that can be used to determine if data has achieved de-identification: (1) the expert determination method; and (2) the safe harbor method. *Id.*

24. Ouellette, *supra* note 20. The twelve national priority purposes are as follows: (1) required by law; (2) public health activities; (3) victims of abuse, neglect, or domestic violence; (4) health oversight activities; (5) judicial and administrative proceedings; (6) law enforcement purposes; (7) decedents; (8) cadaveric organ, eye, or tissue donation; (9) research; (10) serious threat to health or safety; (11) essential government functions; and (12) workers compensation. *Id.*

25. *Id.*

26. *Id.*

27. *Does the HIPAA Privacy Rule Preempt State Laws?*, U.S. DEP’T OF HEALTH & HUMAN SERVS., <https://www.hhs.gov/hipaa/for-professionals/faq/399/does-hipaa-preempt-state-laws/index.html>

are several exceptions when state law may be involved. These exceptions include situations when state law provides greater privacy, the data is used for health surveillance and reporting, or when the data is used for health management or financial audits.²⁸ Additional factors may also be considered to determine which law controls.²⁹

Background

As COVID-19 emerged in the United States in early 2020, covered entities under the HIPAA Privacy Rule began to understand that protection of PHI in the midst of a global pandemic would be a challenge because covered entities must “juggle the protections [of HIPAA] but [also] meet the needs of policy makers.”³⁰ As new cases emerged daily, the transmission of critical, “real-time” data of patients infected with COVID-19 to local and state health departments was necessary to prevent further spread.³¹ However, the Centers for Disease Control and Prevention (CDC) used this data differently than data collected during other smaller outbreaks that they had fought in the past.³² State officials and medical professionals were using the data in “real[time]” as they responded to COVID-19, which was not what the Department of Public Health (DPH) surveillance system was originally designed to do.³³ According to Dr. Kathleen Toomey, Commissioner of the Georgia DPH, “never before had there been this type of demand for data at the granular level Public health surveillance was never meant to provide real-time data.”³⁴ Even so, there was an ever-present and

[<https://perma.cc/NMF2-UR69>] (July 26, 2013); RONALD D. ROTUNDA ET AL., TREATISE ON CONSTITUTIONAL LAW: SUBSTANCE & PROCEDURE § 12.1 (8th ed. 2009).

28. ROTUNDA ET AL., *supra* note 27.

29. *Id.*

30. Electronic Mail Interview with Dr. Kathleen Toomey, Comm’r, Ga. Dep’t of Pub. Health (June 12, 2020) (on file with the Georgia State University Law Review) [hereinafter Toomey Interview].

31. Eduardo Sanchez, *COVID-19 Science: Why Testing Is So Important*, AM. HEART ASS’N (Apr. 2, 2020), <https://www.heart.org/en/news/2020/04/02/covid-19-science-why-testing-is-so-important> [<https://perma.cc/K9Z4-536P>].

32. Toomey Interview, *supra* note 30.

33. *Id.* (“Public health surveillance was never meant to provide real-time data The data was not meant to be reactionary data[,] as it is not real and can even be post mortem sometimes.”).

34. *Id.*

urgent need from federal and state health agencies—and even the public in general—to have easy access to up-to-date numbers of COVID-19 cases.³⁵

Under normal circumstances, HIPAA “is always important and always in effect.”³⁶ In a global pandemic when every day counts, however, local and state health agencies (such as the DPH) saw a loosening of these restrictions as they related to the disclosure of PHI to protect the public.³⁷ Beginning in February of 2020, the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR), the agency responsible for enforcing compliance with HIPAA, released several bulletins and notifications of enforcement and discretion.³⁸ Each bulletin and notification related to a specific aspect of HIPAA and COVID-19 and demonstrated the OCR’s recognition that covered entities should be afforded a certain level of discretion with HIPAA compliance during the pandemic to protect the public and provide accurate, “real-time” data.³⁹

Due to the comprehensive nature of HIPAA, this *Peach Sheet* focuses on the Privacy Rule, how and to whom PHI relating to COVID-19 was disclosed, and how those disclosures affected individuals and their rights under the federal scheme and Georgia law.

Bulletin and Notification Tracking of HIPAA

In February 2020, the OCR released its first bulletin issuing guidance on HIPAA and COVID-19.⁴⁰ The bulletin offered general HIPAA compliance guidelines, stating: “The HIPAA Privacy Rule protects the privacy of patients’ health information . . . but is

35. *Id.*

36. *Id.*

37. *Id.*

38. See OCR HIPAA Announcements Related to COVID-19 of *HIPAA and COVID-19*, U.S. DEP’T OF HEALTH & HUMAN SERVS. [hereinafter *HIPAA and COVID-19 Announcements*], <https://www.hhs.gov/hipaa/for-professionals/special-topics/hipaa-covid19/index.html> [https://perma.cc/ST5M-W6WN] (Sept. 28, 2020).

39. *Id.*

40. Bulletin, Off. for C.R., U.S. Dep’t of Health & Human Servs., HIPAA Privacy and Novel Coronavirus (Feb. 2020), <https://www.hhs.gov/sites/default/files/february-2020-hipaa-and-novel-coronavirus.pdf> [https://perma.cc/V7BX-MBBW].

balanced to ensure that appropriate uses and disclosures of the information still may be made when necessary to treat a patient, to protect the nation's public health, and for other critical purposes."⁴¹ Although covered entities can disclose PHI in certain situations without an individual's authorization (such as to a person at risk or to a public health authority for the purpose of preventing further spread of a disease), the OCR stressed the "minimum necessary" requirement of the Privacy Rule.⁴² The "minimum necessary" requirement ensures that a covered entity makes "reasonable efforts to limit the information disclosed to that which is the 'minimum necessary' to accomplish the purpose of the disclosure."⁴³

The OCR's March 2020 bulletin reiterated many of the same points about HIPAA compliance as the February 2020 bulletin.⁴⁴ One significant difference was that "while the HIPAA Privacy Rule is not suspended during a public health or other emergency, the Secretary of HHS may waive certain provisions of the Privacy Rule under the Project Bioshield Act of 2004 . . . and section 1135(b)(7) of the Social Security Act."⁴⁵ According to the March 2020 bulletin and "[i]n response to President Donald J. Trump's (R) declaration of a nationwide emergency concerning COVID-19," Alex M. Azar, Secretary of the HHS, "exercised the authority to waive sanctions and penalties against a covered hospital that does not comply with the following provisions of the HIPAA Privacy Rule."⁴⁶ The bulletin also listed the provisions that were not enforced if not followed by a covered entity, which included:

[T]he requirements to obtain a patient's agreement to speak with family members or friends involved in the patient's care[,] . . . the requirement to honor a request to opt out of

41. *Id.* at 1.

42. *Id.* at 5.

43. *Id.*

44. Bulletin, Off. for C.R., U.S. Dep't of Health & Human Servs., Limited Waiver of HIPAA Sanctions and Penalties During a Nationwide Public Health Emergency (Mar. 2020), <https://www.hhs.gov/sites/default/files/hipaa-and-covid-19-limited-hipaa-waiver-bulletin-508.pdf> [<https://perma.cc/34A5-DHKB>].

45. *Id.* at 1.

46. *Id.*

the facility directory[,] . . . the requirement to distribute a notice of privacy practices, the patient's right to request privacy restrictions[,] . . . [and] the patient's right to request confidential communications.⁴⁷

The waiver went into effect on March 15, 2020, and as of October 10, 2020, the OCR had not issued a subsequent bulletin or notification on when penalties for noncompliance would be reinstated.⁴⁸

On March 17, the OCR released an announcement regarding HIPAA and COVID-19 titled "Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency."⁴⁹ The notification allowed "covered health care providers subject to the HIPAA rules [to] seek to communicate with patients, and provide telehealth services, through remote communications technologies."⁵⁰ These remote communications technologies had to be non-public and included technologies such as Apple Facetime, Facebook Messenger video chat, Zoom, Skype, and others.⁵¹ Healthcare providers could utilize these technologies for telehealth, regardless of the medical condition presented.⁵² The OCR announced that it would "not impose penalties for noncompliance with the HIPAA [r]ules in connection with the good faith provision of telehealth using such non-public facing audio or video communication products during the COVID-19 nationwide public health emergency."⁵³

On March 24, the OCR issued "Guidance to Help Ensure First Responders and Others Receive Protected Health Information About Individuals Exposed to COVID-19."⁵⁴ The guidance listed various

47. *Id.*

48. *Id.*; see also *HIPAA and COVID-19 Announcements*, *supra* note 38.

49. Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency, 85 Fed. Reg. 22,024-01 (Mar. 17, 2020) (to be codified at 45 C.F.R. §§ 160, 164).

50. *Id.* at 22,025.

51. *Id.*

52. *Id.*

53. *Id.*

54. Guidance, Off. for C.R., U.S. Dep't of Health & Human Servs., Disclosures to Law Enforcement, Paramedics, Other First Responders and Public Health Authorities (Mar. 24, 2020),

situations when a covered entity could disclose the PHI of a patient infected with or exposed to COVID-19 to “law enforcement, paramedics, other first responders, and public health authorities without the individual’s HIPAA authorization.”⁵⁵ The OCR gave examples in each situation of when it was appropriate to disclose PHI, such as the following: “HIPAA permits a covered skilled nursing facility to disclose PHI about an individual who has COVID-19 to emergency medical transport personnel who will provide treatment while transporting the individual to a hospital’s emergency department.”⁵⁶ Again, the OCR stressed that all covered entities should make reasonable efforts to disclose the “minimum necessary to accomplish the purpose of the disclosure.”⁵⁷

On April 7, the OCR released another notification titled the “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.”⁵⁸ The purpose of this notification was to inform healthcare providers and their business associates that the OCR would “exercise its enforcement discretion and [would] not impose potential penalties for violations of certain provisions of the HIPAA Privacy Rule against health care providers or their business associates for uses and disclosures of protected health information by business associates for public health and health oversight activities during the COVID-19” pandemic.⁵⁹

On May 5, the OCR issued “Guidance on Covered Health Care Providers and Restrictions on Media Access to Protected Health Information About Individuals in Their Facilities.”⁶⁰ The purpose of

<https://www.hhs.gov/sites/default/files/covid-19-hipaa-and-first-responders-508.pdf>
[<https://perma.cc/89GJ-U5XK>].

55. *Id.* at 1.

56. *Id.*

57. *Id.* at 3.

58. 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. 19,392-02 (Apr. 7, 2020) (to be codified at 45 C.F.R. §§ 160, 164).

59. *Id.* at 19,392.

60. Guidance, Off. for C.R., U.S. Dep’t of Health & Human Servs., Guidance on Covered Health Care Providers and Restrictions on Media Access to Protected Health Information About Individuals in Their Facilities (May 5, 2020), <https://www.hhs.gov/sites/default/files/guidance-on-media-and-film-crews-access-to-phi.pdf> [<https://perma.cc/NPB3-6MSZ>].

this guidance was to remind covered entities that the HIPAA Privacy Rule “does not permit covered health care providers to give the media, including film crews, access to . . . patients’ PHI . . . without . . . a written HIPAA authorization.”⁶¹ It offered guidance on when an individual’s HIPAA authorization was required before granting media access and the practices that covered health care providers must use when the media and reporters were given access to a healthcare facility.⁶²

Finally, on June 12, the OCR issued “Guidance on HIPAA and Contacting Former COVID-19 Patients About Blood and Plasma Donation.”⁶³ The guidance allowed covered entities or their associates to use PHI to identify and contact their own former COVID-19 patients about blood and plasma donation.⁶⁴ However, the OCR emphasized that although HIPAA allowed for this use of PHI, covered entities could not use it as a marketing tool.⁶⁵

Analysis

The Georgia Department of Public Health’s Daily Status Report

During the COVID-19 pandemic, the DPH maintained a “Daily Status” report available to the public on its webpage.⁶⁶ The status report provided information “reported to [the] DPH on the total number of COVID-19 tests, confirmed COVID-19 cases (PCR positive), ICU admissions, hospitalizations, and deaths attributed to COVID-19.”⁶⁷ The DPH updated the page daily.⁶⁸ The page

61. *Id.* at 1.

62. *Id.* at 1–2.

63. Guidance, Off. for C.R., U.S. Dep’t of Health & Human Servs., Guidance on HIPAA and Contacting Former COVID-19 Patients About Blood and Plasma Donation (June 12, 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/BPC5-A6LW>].

64. *Id.* at 1.

65. *Id.* at 2.

66. *Georgia Department of Public Health Daily Status Report*, GA. DEP’T OF PUB. HEALTH [hereinafter *Daily Status Report*], <https://dph.georgia.gov/covid-19-daily-status-report> [<https://perma.cc/8PGE-XN83>].

67. *Id.* A PCR test is a polymerase chain reaction (PCR) test that detects whether there is genetic material of a virus present in a sample. *How COVID-19 Testing in Georgia Works*, GA. DEP’T OF PUB. HEALTH, <https://dph.georgia.gov/how-covid-19-testing-georgia-works> [<https://perma.cc/M2FZ-89TJ>].

contained a disclaimer that the data displayed “[were] based on available information at the time of the report and may not reflect all cases or tests performed in Georgia.”⁶⁹

The data were further broken down and organized in various ways in an attempt to provide a more granular view of the state’s situation.⁷⁰ The breakdown included cases, deaths, and hospitalizations by county; cases, deaths, and hospitalizations by age group; and cases by race and sex.⁷¹ During the earlier stages of the pandemic, the DPH published data broken down even further to display each individual death listed.⁷² The prior data displayed the individual’s age, race, county, and whether they had any underlying conditions.⁷³ Once the deaths in Georgia reached a level where this granular data displayed over a thousand names, the data were condensed.⁷⁴

Though helpful for maintaining awareness of COVID-19’s spread and for informing officials implementing public health interventions, data broken down to such a granular level could potentially violate an individual’s HIPAA rights.⁷⁵ In smaller, less populated counties, listing information such as someone’s age, race, and whether they suffered from underlying conditions could reasonably lead others within the community to deduce the identification of the individual, especially when coupled with an individual’s possible absence from work. Such disclosure of reasonably identifiable information typically violates HIPAA’s de-identification requirements. During the COVID-19 pandemic, however, HIPAA’s requirements were relaxed to allow for entities such as the DPH’s Division of Epidemiology to make public health decisions and interventions with

(June 23, 2020).

68. See *Daily Status Report*, *supra* note 66.

69. *Id.*

70. *Id.*

71. *Id.*

72. *Id.*; see also, e.g., Andy Miller, *Average Age of Georgia COVID-19 Deaths Is Lower than Global Figure, Data Shows*, WABE (Mar. 30, 2020), <https://www.wabe.org/average-age-of-georgia-covid-19-deaths-is-lower-than-global-figure-data-shows/> [<https://perma.cc/2TS9-86QF>].

73. See, e.g., Miller, *supra* note 72.

74. See *Daily Status Report*, *supra* note 66.

75. *Id.*

ease.⁷⁶ Regardless of the need for this granular data, it must still be weighed against the negative consequences it may have on an individual's day-to-day life and mental health. Because this kind of particularized data, no matter how sensitive it may be, helps public health agencies and other entities to determine what measures to take to protect the public, the need to publically publish such data may outweigh any individualized negative consequences, especially in the midst of a pandemic.⁷⁷

Having these data readily available helps facilitate faster and more efficient decision-making at the public health management level. Additionally, making these data public helps business owners or other service providers make decisions about their day-to-day operations. For example, businesses servicing the elderly or those with underlying conditions in areas that had experienced a recent spike in reported COVID-19 cases could have used the data to take additional precautions to promote the safety of all. Some stores even implemented a set time where fragile individuals could shop separately from the general public.⁷⁸ Moreover, these data could be useful for businesses and facilities to make decisions on constricting or expanding operations based on their county and the general demographic they serve.⁷⁹

76. Toomey Interview, *supra* note 30. The DPH is a "hybrid entity" for the purposes of HIPAA. Colleen Healy Boufides et al., *FAQ: COVID-19 and Health Data Privacy*, NETWORK FOR PUB. HEALTH L. (June 22, 2020), <https://www.networkforphl.org/resources/faqs-covid-19-and-health-data-privacy/> [<https://perma.cc/6U86-AG84>]. In accordance with HIPAA regulations, 45 C.F.R. § 164.105(a), the DPH elected to declare itself a "hybrid entity" divided into "covered components," which must follow HIPAA, and "non-covered components," which do not. *Id.* The DPH Division of Epidemiology has been formally designated by the Commissioner as a "non-covered component." Toomey Interview, *supra* note 30. The DPH's Division of Epidemiology is thus not subject to the restrictions of HIPAA's "safe harbor" de-identification protocol, allowing it to publish information with a level of specificity that a HIPAA-covered entity might not be allowed to do. Boufides et al., *supra*.

77. *Daily Status Report*, *supra* note 66; *COVID-19: Businesses and Employers*, GA. DEP'T OF PUB. HEALTH [hereinafter *Businesses & Employers*], <https://dph.georgia.gov/covid-19-businesses-and-employers> [<https://perma.cc/RSU2-USNE>].

78. See, e.g., *Coronavirus Update: How Trader Joe's Is Caring for Crew Members and Customers*, TRADER JOE'S, <https://www.traderjoes.com/announcement/coronavirus-update-how-trader-joes-is-caring-for-crew-members-and-customers> [<https://perma.cc/AK4C-BWJF>] (July 15, 2020); *Dollar General Announces First Hour of Operations to Be Dedicated to Senior Customers*, DOLLAR GEN.: NEWSROOM (Mar. 16, 2020), <https://newscenter.dollargeneral.com/covid-19/dollar-general-announces-first-hour-of-operations-to-be-dedicated-to-senior-customers.htm> [<https://perma.cc/T7W7-98MV>].

79. See, e.g., *Daily Status Report*, *supra* note 66; *Businesses & Employers*, *supra* note 77.

The reasons for making such granular data public are valid and important, but at what costs would such public data come? What is the risk in allowing other nefarious actors in the United States and abroad to easily access these data? As discussed *supra*, these data can be reasonably used to identify individuals in smaller counties. Because of certain negative stigma that may attach to certain sensitive medical information, this identification could lead to extreme outcomes such as ostracization of individuals from their community, loss of employment, receiving improper medical care, or even refusal of medical care entirely. This “outing” of sorts violates an individual’s privacy rights under HIPAA.⁸⁰ Making these specific data so readily available also allows for abuse of the data through manipulation.⁸¹ These data could be manipulated in a way that misrepresents the reported facts to arrive at varying conclusions that negatively affects the community where the data is ultimately distributed.⁸² Balancing these two competing interests behind releasing data to the public and protecting individual privacy detracts from the underling goal, however, where the focus should lie on preserving the general health of the community.

Nursing Homes and Long-term Care Facilities

As COVID-19 spread throughout the United States, a common worry among the medical community revolved around the possibility of the disease infiltrating nursing homes and long-term care facilities.⁸³ Patients and residents in such facilities were more susceptible to the negative effects of COVID-19.⁸⁴ The Centers for

80. Ouellette, *supra* note 20.

81. Samuel Volkin, *Recognizing Disinformation During the COVID-19 Pandemic*, JOHNS HOPKINS U. (May 8, 2020), <https://hub.jhu.edu/2020/05/08/thomas-rid-disinformation-in-covid-19-pandemic/> [<https://perma.cc/2NRJ-8DFB>].

82. *Id.*

83. Taylor Cooper, *COVID-19 Spreads to Nearly All Residents at Brunswick Nursing Home*, BRUNSWICK NEWS (July 3, 2020), https://thebrunswicknews.com/news/coronavirus/covid-19-spreads-to-nearly-all-residents-at-brunswick-nursing-home/article_820af356-310f-554c-abb0-b2c3389c292a.html [<https://perma.cc/8JUN-TC4A>].

84. Memorandum from the Dir. of Quality, Safety & Oversight Grp. of the Dep’t Health & Human Servs., Ctrs. for Medicare & Medicaid Servs. on Nursing Home Reopening Recommendations to State Officials (May 18, 2020) (on file with the Georgia State University Law Review) [hereinafter Memorandum from CMS]; *see also* Older Adults of Coronavirus Disease 2019, CTRS. FOR DISEASE

Medicare and Medicaid Services (CMS) issued guidance on how to prevent COVID-19 in these facilities and what caretakers and staff should do in the event of infection, including immediately reporting patients with symptoms of COVID-19 to local health departments.⁸⁵

As part of Georgia's response to the COVID-19 health crisis, the Healthcare Facility Regulation Division (HFRD) of Georgia's Department of Community Health (DCH) compiled and released daily reports of COVID-19 numbers in nursing homes and long-term care facilities to "aid[] transparency" to the public.⁸⁶ The data collected by the HFRD was "[used] by the Georgia National Guard and state agencies to assist in planning, strategy[,] and intervention measures."⁸⁷ Because nursing homes and long-term care facilities are required under Georgia law to report "to the [DCH] and the county board of health all known or presumptively diagnosed cases of persons harboring any illness or health condition that may be caused by . . . [a] pandemic disease," the HFRD gathered information concerning COVID-19 from "all licensed nursing homes, all licensed assisted living communities, and licensed personal care homes [PCH] of [twenty-five] beds or more."⁸⁸ Each daily report included only the facility type (nursing home or PCH), the facility's name and location, the number of residents at the facility, the cumulative number of COVID-19 numbers within the facility, the cumulative number of COVID-19 deaths in the facility, and the cumulative number of staff working at the facility that had tested positive for COVID-19.⁸⁹ No information regarding patients' PHI, such as name or address, was included in the report.⁹⁰ Thus, each daily report was HIPAA-compliant because the reports fell under exception number

CONTROL & PREVENTION, <https://www.cdc.gov/coronavirus/2019-ncov/need-extra-precautions/older-adults.html> [<https://perma.cc/R6DQ-FFFM>] (Sept. 11, 2020) (recognizing that individuals living in a nursing home may be at greater risk of contracting COVID-19 due to factors such as old age and underlying health conditions).

85. Memorandum from CMS, *supra* note 84.

86. GA. DEP'T OF CMTY. HEALTH, HEALTHCARE FACILITY REGULATION (HFR) LONG-TERM CARE FACILITY COVID-19 REPORT FREQUENTLY ASKED QUESTIONS 1 (2020).

87. *Id.*

88. *Id.*; O.C.G.A. § 31-12-2(b) (2019).

89. GA. DEP'T OF CMTY. HEALTH, *supra* note 86.

90. *Id.*

six to HIPAA and because no personally identifiable information was included.⁹¹

Emergency Medical Services (EMS) Workers

During the COVID-19 pandemic, the DPH prioritized the protection of EMS and first responders from exposure to the virus: “The health and safety of our first responders is extremely important and notifying them in a timely manner of any potential exposure to COVID-19 allows them to keep themselves . . . safe.”⁹² Oftentimes, EMS and first responders were the first points of contact for COVID-19-positive patients being transported to hospitals. In an effort to reduce the spread of COVID-19 and to protect these workers, the DPH issued guidance on how to alert EMS and other first responders of potential exposure to COVID-19 while also maintaining compliance with HIPAA.⁹³ In its guidance, the DPH adopted a two-pronged approach for alerting EMS personnel of potential exposure.⁹⁴

The first approach was to alert EMS and other first responders of COVID-19 positive patients *before* the workers come into contact with the patient.⁹⁵ The DPH’s guidance contained several steps within this process geared to maintain the patient’s privacy in compliance with HIPAA.⁹⁶ First, the Georgia Emergency Management and Homeland Security Agency (GEMA/HS) would “pull the daily COVID-19 case list from the State Electronic Notifiable Disease Surveillance System (SENDSS).”⁹⁷ Next, the GEMA/HS would “separate the list into each of the eight GEMA/HS

91. *Id.*; Ouellette, *supra* note 20.

92. Guidance, Ga. Dep’t of Pub. Health, COVID-19 Notifications to 911 PSAPs and First Responder Agencies 2 (Apr. 11, 2020) [hereinafter First Responder Notification Guidance], <https://dph.georgia.gov/document/document/process-notify-psaps-and-first-responders/download> [https://perma.cc/KL4U-MKXA].

93. *Id.* at 1.

94. *Id.*; see also COVID-19 Notifications to 911 PSAPs and First Responder Agencies of Georgia *OEMS COVID-19 Guidance for First Responders (EMS, Fire, Law Enforcement)*, GA. DEPT. OF PUB. HEALTH, <https://dph.georgia.gov/EMS/oems-covid-19> [https://perma.cc/4GHC-9UZB] (Apr. 14, 2020).

95. First Responder Notification Guidance, *supra* note 92, at 1 (emphasis added).

96. *Id.*

97. *Id.*

Regions.”⁹⁸ The regional staff would “break the list down into the cities and counties that [were] served by each of the 911 Public Safety Answering Points (PSAPs),” and then send the list to each PSAP.⁹⁹ To comply with HIPAA, “[t]he list [would] only include the address, Date of Onset and the List Removal Date ([twenty-one] days after the [d]ate of [o]nset).”¹⁰⁰ These guidelines complied with HIPAA because the GEMA/HS and regional staff distributed each list in the public interest—that is, to protect EMS and other first responders before they came into contact with a potential COVID-19 patient.¹⁰¹ The PSAP then flagged each address with a known COVID-19 case “that [was] only visible to dispatchers.”¹⁰² If a 911 call was placed from a flagged address, “the dispatchers [would] inform the responding personnel of [its existence].”¹⁰³ The DPH emphasized in its guidance that “case information must not be broadcast on an open channel and must only be made available to individuals responding to the call.”¹⁰⁴

The second approach was to alert EMS and other first responders *after* potential exposure to a person with COVID-19.¹⁰⁵ To do this, the DPH split the guidance into two categories: (1) hospitalized COVID-19 patients, and (2) non-hospitalized COVID-19 patients.¹⁰⁶ The DPH requested that “[h]ospitals or acute facilities that have a patient who tests positive for COVID-19 . . . [n]otify . . . the DPH Regional EMS Director of the name, [date of birth,] and test date for any COVID-19 positive patient.”¹⁰⁷ These facilities were also requested to “[n]otify . . . [the] DPH through the State Electronic Notifiable Disease Surveillance System (SENDSS).”¹⁰⁸ Non-hospitalized patients with COVID-19 were reported to SENDSS by the testing facility and then sent to regional EMS directors for

98. *Id.*

99. *Id.*

100. *Id.*

101. First Responder Notification Guidance, *supra* note 92, at 1; Ouellette, *supra* note 20.

102. First Responder Notification Guidance, *supra* note 92.

103. *Id.* at 1.

104. *Id.*

105. *Id.* at 2–3 (emphasis added).

106. *Id.*

107. *Id.* at 3.

108. First Responder Notification Guidance, *supra* note 92, at 3.

appropriate follow-up with EMS and other first responders.¹⁰⁹ Once the regional EMS director was aware of any first responder agency with potential COVID-19 contact, the director was required to notify the agency.¹¹⁰ These guidelines also complied with HPAA and the OCR's bulletins on HIPAA compliance during the COVID-19 pandemic because no PHI was presented to the public.¹¹¹ The DPH ensured that any PHI, such as the name or address of anyone with COVID-19, was kept under strict control, limiting access to the information to only necessary personnel.¹¹²

The Future and Telehealth

As businesses, services, and other public venues closed their doors during the shelter-in-place Order, several essential services stayed open, and some limited their services or capacity.¹¹³ The complications resulting from these limited services produced a surprising outcome in the form of increased use of telehealth services.¹¹⁴ Though telehealth had been a useful tool for several years when providing health services to rural communities, its versatility provided fundamental to providing a safe alternative to healthcare during the pandemic.¹¹⁵ Many individuals turned to virtual appointments rather than venturing to doctors' offices where they faced the risks of not only being exposed to COVID-19 but also exposing others if they were carriers. This expanding area of health services became one to watch in terms of maintaining individual privacy rights under HIPAA and the requirements to ensure secure and private appointments. As telehealth continues to develop into a more prominent staple for healthcare providers, regulators must prioritize addressing issues concerning the privacy of virtual

109. *Id.*

110. *Id.*

111. *Id.* at 1.

112. *Id.*

113. Phil Galewitz, *Telemedicine Surges, Fueled by Coronavirus Fears and Shift in Payment Rules*, KAISER HEALTH NEWS (Mar. 27, 2020), <https://khn.org/news/telemedicine-surges-fueled-by-coronavirus-fears-and-shift-in-payment-rules/> [<https://perma.cc/VKN7-GMZL>].

114. *Id.*

115. *Id.*

appointments (both calls and videos), the platforms used to host the virtual appointments, and the data management systems used to store the information gathered from the appointments.

Conclusion

The DPH and other healthcare providers and agencies, both nationally and in Georgia, continued to navigate the challenges associated with COVID-19 and protecting the privacy of individuals throughout 2020. Accordingly, determining how to mesh protecting the public health of Americans and protecting the privacy of individuals evolved as well. Under HIPAA's directives, the DPH must constantly balance the consequences of releasing individuals' PHI, "all the while balancing the limitations and needs for public information and protections."¹¹⁶ Furthermore, due to the emergence of and increased reliance on telehealth systems during the COVID-19 pandemic, healthcare providers were forced to take proactive steps toward ensuring that patients were afforded privacy. Because of the constant balancing act required by HIPAA, regulators and healthcare providers are required to continuously analyze data and adjust privacy guards and practices to best suit the needs of their patients and protect the health of the community, especially in the midst of a pandemic.

Erin L. Hayes & Kathryn A. Vance

116. Toomey Interview, *supra* note 30.

