A Digital Checkup on HIPAA: Modernizing Healthcare Privacy Standards for Telehealth Services

Julia Wells*

TABLE OF CONTENTS

* J.D., May 2023, The George Washington University Law School; B.A., Religion & Philosophy, Colgate University. I would like to thank Sarah Morris, Journal Adjunct, and Andrew Seneviratne, Notes Editor, for their support and guidance. I would also like to thank my family for their support during the writing process.

I. INTRODUCTION

Imagine consulting with your doctor or medical team through videoconferencing platforms or over messaging apps, but those platforms and apps are not encrypted or otherwise secure. Further, imagine that the device your doctor used to communicate with you is stolen, allowing the thief to view your personal health information. This is not an imaginary problem. In 2013, four unencrypted laptops belonging to Advocate Health Care that contained personal health information were stolen, and another unencrypted laptop with the personal information of over 2,000 patients was stolen from an employee's car.[1] The theft of unencrypted devices is not the only risk to patient privacy, however. Risks to patient privacy include ransomware attacks, health care providers sending private health information to the wrong person, and sending and storing unencrypted health information, including videos.[2]

Prior to the coronavirus pandemic, the use of telehealth services was uncommon.[3] Due to the pandemic, the use of telehealth services has increased, allowing people to receive routine checkups and medical care without risking their health by entering a hospital or doctor's office.[4] Although these telehealth services have provided much needed medical care during the pandemic, they have raised numerous patient privacy concerns. Because the pandemic made telehealth services a necessity to prevent in-person contact, several health care providers had to implement telehealth services quickly. Many of these services have likely not undergone the normal security checks and may not comply with the Health Insurance Portability and Accountability Act ("HIPAA").

During the pandemic, the Department of Health and Human Services ("HHS") announced that it would not penalize covered health care providers using video chatting platforms that may not be HIPAA compliant for telehealth services "in connection with the good faith provision of telehealth during the [pandemic]."[5] This regulatory discretion in enforcement implicates patients' data privacy. Because telehealth services will likely remain popular

---

1. Lisa Schencker, *Advocate to Pay $5.5 Million over Data Breach: Record HIPAA Settlement*, CHI. TRIB. (Aug. 5, 2016, 7:20 AM), https://www.chicagotribune.com/business/ct-advocate-settlement-privacy-0805-biz-20160804-story.html [https://perma.cc/PXF6-WBUT].

2. *See What Are Some Common HIPAA Violations?*, COMPLIANCY GRP., https://compliancy-group.com/common-hipaa-violations/ [https://perma.cc/MY59-5D7C] (last visited Mar. 3, 2022).

3. *See* Gabriela Weigel et al., *Opportunities and Barriers for Telemedicine in the U.S. During the COVID-19 Emergency and Beyond*, KAISER FAM. FOUND. (May 11, 2020), https://www.kff.org/womens-health-policy/issue-brief/opportunities-and-barriers-for-telemedicine-in-the-u-s-during-the-covid-19-emergency-and-beyond/ [https://perma.cc/BV2H-VYH3].

4. *Id.*

5. *Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency*, U.S. DEP'T HEALTH & HUM. SERVS. [hereinafter *Notification of Enforcement Discretion*], https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html [https://perma.cc/NF45-S27B] (last updated Jan. 20, 2021).

after the pandemic, Congress should reform HIPAA so that it maintains flexibility regarding telehealth platforms while protecting patients' personal information. HIPAA should be reformed to include more detailed provisions concerning best practices for maintaining data privacy, such as two-factor authentication and firewalls, and include technical requirements for devices used to connect with patients, such as encryption.

Part A of the Background section of this Note provides an overview of telehealth services and the agencies involved in regulating and providing access to those services. Additionally, Part A describes the expansion of telehealth services in the United States. Part B of the Background presents a brief overview of HIPAA, its limitations, as well as an overview of HHS' Notification of Relaxed Enforcement. Moreover, Part B describes the roles agencies, particularly the FCC, play in overseeing and implementing telehealth services. Part A of the Analysis demonstrates the feasibility of Congress addressing matters relating to healthcare despite intense congressional polarization. Part B of the Analysis argues that the FCC should be given a larger role in regulating telehealth services, and Part C proposes reforms that should be made to HIPAA to increase flexibility while providing greater protection to patients' private information. Finally, Part D addresses potential limitations of the proposal and provides possible solutions to those limitations.

II. BACKGROUND

A. Overview of Telehealth Services

1. Definition and Expansion of "Telehealth Services"

Telehealth services is "the use of electronic information and telecommunications technologies to support and promote long-distance clinical health care, patient and professional health-related education, and public health and health administration."[6] These services can be provided through audio, text, and video.[7] They are designed to overcome geographic barriers in connecting with patients for clinical services through information and communication technologies (e.g., computers, cell phones, etc.).[8]

Prior to the coronavirus pandemic, the use of telehealth services was uncommon. Based on a sample of health benefit claims in 2018, only 2.4% of patients enrolled in large employer health plans that included outpatient

6. *What Is Telehealth?*, U.S. DEP'T HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/faq/3015/what-is-telehealth/index.html [https://perma.cc/BAP6-RXNN] (last updated Mar. 27, 2020).

7. *Id.*

8. NICOL TURNER LEE ET AL., BROOKINGS INST. & JOHN LOCKE FOUND., REMOVING REGULATORY BARRIERS TO TELEHEALTH BEFORE AND AFTER COVID-19 5 (2020), https://www.brookings.edu/wp-content/uploads/2020/05/Removing-barriers-to-telehealth-before-and-after-COVID-19_PDF.pdf [https://perma.cc/W6XY-FJ94].

services had used a telehealth service.[9] By May of 2020, a poll had found that at least 23% of adults had utilized telehealth services, and that number has exponentially grown.[10] A global study from July 2021 found that, out of 5,000 responses, almost half had engaged in telehealth services.[11] Over 80% of the group that had used telehealth services used those services during the pandemic in order to minimize in-person interactions.[12] Furthermore, 63% of respondents stated that they plan to continue using telehealth services post-pandemic, and 77% stated that they "enjoyed using telehealth."[13] In addition to the increasing usage of telehealth services, investments in those services have increased.[14] In August 2021, the Biden-Harris Administration declared "a $19 million investment to expand telehealth and improve access in rural communities."[15] Furthermore, a study found that 76% of employers expanded their telehealth services during the pandemic and that they plan to continue providing telehealth options post-pandemic.[16] Given its increased usage and investment, as well as the convenience telehealth services provide both patients and doctors, telehealth services will likely remain popular after the pandemic. The continued use of telehealth services makes agency regulation extremely important.

2. Agency Regulation and Oversight of Telehealth Services

A variety of government agencies, including HHS and the FCC, are involved in regulating and providing greater access to telehealth services. The FCC has long been involved in telecommunications, including telehealth and telemedicine. In the Telecommunications Act of 1996, Congress ordered the FCC to "encourage the deployment on a reasonable and timely basis of advanced telecommunications capability to all Americans."[17] In 2006, the

---

9. *See* Gabriela Weigel et al., *Opportunities and Barriers for Telemedicine in the U.S. During the COVID-19 Emergency and Beyond*, KAISER FAM. FOUND. (May 11, 2020), https://www.kff.org/womens-health-policy/issue-brief/opportunities-and-barriers-for-telemedicine-in-the-u-s-during-the-covid-19-emergency-and-beyond/ [https://perma.cc/BV2H-VYH3].

10. *Id.*

11. *New Survey Reveals Appeal of Telehealth Services; 63% Plan to Increase Use Post-Pandemic*, BUS. WIRE (Oct. 13, 2021, 9:00 AM), https://www.businesswire.com/news/home/20211013005160/en/New-Survey-Reveals-Appeal-of-Telehealth-Services-63-Plan-to-Increase-Use-Post-Pandemic [https://perma.cc/T5LZ-AN8G].

12. *Id.*

13. *Id.*

14. David Jagielski, *Why It Isn't Too Late to Invest in Telehealth*, MOTLEY FOOL (Sept. 8, 2021, 6:13 AM), https://www.fool.com/investing/2021/09/08/why-it-isnt-too-late-to-invest-in-telehealth/ [https://perma.cc/DK6C-CTLE].

15. *Id.*

16. *Id.*

17. Telecommunications Act of 1996, Pub. L. No. 104-104, § 706, 110 Stat. 56, 152 (1996); *FCC Health IT Actions and Activities Timeline*, FCC, https://www.fcc.gov/general/fcc-health-it-actions-and-activities-timeline [https://perma.cc/X578-RSUQ] (last visited Jan. 28, 2022).

FCC created the Rural Health Care Pilot Program aimed at introducing telemedicine and telehealth services to rural areas.[18] Moreover, in 2014, the FCC formed the Connect2Health FCC Task Force, which is concerned with "the critical intersection of broadband, advanced technology, and health with the primary goal of ensuring that advanced health care solutions are readily accessible to all Americans."[19] Additionally, the FCC worked with the Food and Drug Administration and the Office of the National Coordinator for Health Information Technology to propose "recommendations on appropriate, risk-based regulatory framework pertaining to health information technology . . . that promotes innovation, protects patient safety, and avoids regulatory duplication."[20]

During the pandemic, Congress furthered the FCC's role in telehealth by passing the Coronavirus Aid, Relief, and Economic Security Act ("CARES Act").[21] The CARES Act allocated $200 million to the FCC for the expansion of telehealth services across the U.S.[22] The FCC was authorized to use these funds "to prevent, prepare for, and respond to coronavirus, domestically or internationally, including to support efforts of health care providers to address coronavirus by providing telecommunications services, information services, and devices necessary to enable the provision of telehealth services during an emergency period."[23] With this increased funding, the FCC has focused on providing telehealth services to people in remote areas.[24] It uses these funds to enable eligible nonprofit and public health care providers to buy telecommunications services and devices necessary to use those services.[25]

In addition to allocating funds to the FCC to expand telehealth services, the CARES Act encourages the expansion of telemedicine in general.[26] For example, Section 3212 adds $29 million in annual funding for 2021 through 2025 to develop "'evidence-based projects that utilize telehealth technologies through telehealth networks.'"[27] Moreover, Section 3707 instructs the Secretary of HHS to "encourage the use of telecommunications systems" in home health services during the emergency period.[28] Other provisions in the

18. *FCC Health IT Actions and Activities Timeline*, *supra* note 17.

19. *Id.*

20. *Id.*

21. Coronavirus Aid, Relief, and Economic Security Act, Pub. L. No. 116-136, 134 Stat. 281 (2020).

22. Coronavirus Aid, Relief, and Economic Security Act § 15002; *Connecting Americans to Healthcare*, FCC, https://www.fcc.gov/connecting-americans-health-care [https://perma.cc/D2XD-9DAS] (last visited Nov. 19, 2021).

23. Coronavirus Aid, Relief, and Economic Security Act § 15002.

24. *Connecting Americans to Healthcare*, *supra* note 22.

25. *CARES Act: AMA COVID-19 Pandemic Telehealth Fact Sheet*, AM. MED. ASS'N [hereinafter *Pandemic Telehealth Fact Sheet*], https://www.ama-assn.org/delivering-care/public-health/cares-act-ama-covid-19-pandemic-telehealth-fact-sheet [https://perma.cc/XT7Z-HGB4] (last updated Apr. 27, 2020).

26. Andrew D. Lipman & Tamar E. Finn, *CARES Act Includes Provisions Regarding Telecommunications, Telehealth*, MORGAN LEWIS (Apr. 1, 2020), https://www.morganlewis.com/pubs/2020/04/cares-act-includes-provisions-regarding-telecommunications-telehealth-cv19-lf [https://perma.cc/63BX-2VPJ].

27. Coronavirus Aid, Relief, and Economic Security Act § 3212.

28. Coronavirus Aid, Relief, and Economic Security Act § 3707.

CARES Act provide for reimbursement of particular telehealth services for seniors on Social Security and encourage the Secretary of Veterans Affairs to enter into contracts to expand telehealth services for veterans.[29] Although the expansion of the FCC's regulation of telehealth services has so far been limited to during the pandemic, the continued rise in telehealth services indicates that continued regulation will be necessary post-pandemic. Given the variety of provisions in the CARES Act that aim to expand telehealth services, it is likely that telehealth services will continue to be a priority for the foreseeable future. And, given the growing importance of telehealth services, it is important to understand the patient privacy regulations that were in place prior to COVID-19.

B. Health Insurance Portability and Accountability Act of 1996

Part 1 of this section describes the critical provisions of HIPAA impacting telehealth services and the rules, including the Privacy Rule and the Security Rule, that health care providers and business associates must follow. Additionally, Part 1, Subsection c explains how the Health Information Technology for Economic and Clinical Health (HITECH) Act amended HIPAA. Part 2 discusses the potential issues with HIPAA outside the public health emergency context. Part 3 explains the Department of Health and Human Services' notification of relaxed enforcement of HIPAA and describes the potential issues with such relaxed enforcement of HIPAA.

1. Overview of HIPAA

Under the HIPAA of 1996, health information is protected.[30] Protected health information ("PHI") includes information that can be used to identify an individual and is related to "the individual's past, present or future physical or mental health or condition," "the provision of health care to the individual," "or the past, present, or future payment for the provision of health care to the individual."[31] The protection of health information is governed by the HIPAA Privacy Rule, a primary objective of which is ensuring "that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well being."[32]

29. Coronavirus Aid, Relief, and Economic Security Act §§ 3704, 20004; *see* Lipman & Finn, *supra* note 26.

30. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

31. Health Insurance Portability and Accountability Act § 1171; U.S. DEP'T HEALTH & HUM. SERVS., SUMMARY OF THE HIPAA PRIVACY RULE 4 (2003) [hereinafter SUMMARY OF HIPAA PRIVACY RULE], https://www.hhs.gov/sites/default/files/privacysummary.pdf [https://perma.cc/5GQJ-WGFH].

32. SUMMARY OF HIPAA PRIVACY RULE, *supra* note 31, at 1.

a. The Privacy Rule

The Privacy Rule applies to health plans, health care providers who electronically convey health information regarding certain transactions, and health care clearinghouses, such as billing services.[33] The Privacy Rule requires covered entities to enter into a Business Associate Agreement ("BAA") with any business associates performing work on behalf of, or providing services to, covered entities.[34] Business associates are people or other organizations that perform a variety of services including claims processing, billing, and data analysis.[35] Services that business associates provide include legal, consulting, management, accreditation, and financial.[36] Covered entities are required to "impose specified written safeguards on the individually identifiable health information used or disclosed by its business associates" in the BAA.[37] BAAs cannot be used to authorize business associates to use or disclose PHI in violation of the Privacy Rule.[38] Additionally, BAAs must "[r]equire the business associate to use appropriate safeguards to prevent a use or disclosure of the protected health information other than as provided for by the contract."[39] Finally, if the covered entity discovers the business associate violated the agreement, the entity must "take reasonable steps to cure the breach or end the violation, and if such steps are unsuccessful, to terminate the . . . arrangement."[40] The requirement to enter into a BAA only applies if the relationship between the covered entity and the business associate involves creating or sharing PHI.[41]

b. The Security Rule

HIPAA also includes a Security Rule, the purpose of which is to "protect the privacy of individuals' health information while allowing covered entities to adopt new technologies to improve the quality and efficiency of patient care."[42] The Security Rule of HIPAA protects a subgroup of the information protected by the Privacy Rule.[43] This subgroup is "all individually identifiable health information a covered entity creates, receives,

---

33. *Id.* at 2.

34. U.S. DEP'T HEALTH & HUM. SERVS., BUSINESS ASSOCIATES 1 (2003), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.pdf [https://perma.cc/3AMX-NSLR].

35. *Id.* at 3.

36. *Id.*

37. *Id.*

38. *Id.*

39. BUSINESS ASSOCIATES, *supra* note 34, at 3.

40. *Id.*

41. 45 C.F.R. § 160.103(1)(i)-(ii) (2022); SUMMARY OF HIPAA PRIVACY RULE, *supra* note 31, at 3.

42. *Summary of the HIPAA Security Rule*, U.S. DEP'T HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html#:~:text=The%20Security%20Rule%20protects%20a,%E2%80%9D%20(e%2DPHI) [https://perma.cc/5HVQ-DV3Q] (last updated July 26, 2013).

43. *Id.*

maintains or transmits in electronic form," otherwise known as e-PHI.[44] In other words, the Security Rule protects PHI only when it is transmitted electronically.[45] The Security Rule applies to the same entities as the Privacy Rule, as well as business associates who transmit health information electronically.[46]

Under the Rule, covered entities must "maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI."[47] Covered entities are required to ensure that e-PHI is not disclosed or made available to those who are unauthorized.[48] Additionally, e-PHI must not be "altered or destroyed in an unauthorized manner" and must be "accessible and usable on demand by an authorized person."[49] Moreover, covered entities are required to "[i]dentify and protect against reasonably anticipated threats to the security or integrity of the information" and "[p]rotect against reasonably anticipated, impermissible uses or disclosures."[50] Finally, covered entities must ensure that all employees comply with the Security Rule.[51]

c. Key Technical Considerations

The Security Rule does not require that each covered entity must adopt a specific security measure; rather, covered entities have discretion in deciding which security measures to assume.[52] The Rule, however, does list factors that a covered entity must consider in its decision. Such factors include the entity's "size, complexity, and capabilities," the entity's "technical, hardware, and software infrastructure," the "costs of security measures, and" "the likelihood and possible impact of potential risks to e-PHI."[53] Covered entities must perform regular risk analyses to ensure that all e-PHI remain protected.[54] A risk analysis entails assessing "the likelihood and impact of potential risks to e-PHI," implementing security measures to address those potential risks, recording the security measures adopted and the rationale for that adoption, and maintaining "appropriate security protections."[55]

---

44. *Id.*
45. *Summary of the HIPAA Security Rule*, *supra* note 42; *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*, CDC, https://www.cdc.gov/phlp/publications/topic/hipaa.html [https://perma.cc/JD7A-S7LX] (last updated Sept. 14, 2018).
46. *See Summary of the HIPAA Security Rule*, *supra* note 42.
47. *Id.*
48. *Id.*
49. *Id.*
50. *Id.*
51. *Id.*
52. *Summary of the HIPAA Security Rule*, *supra* note 42.
53. *Summary of the HIPAA Security Rule*, *supra* note 42; *HIPAA Security Rule & Risk Analysis*, AM. MED. ASS'N, https://www.ama-assn.org/practice-management/hipaa/hipaa-security-rule-risk-analysis [https://perma.cc/QJ7M-M9DT] (last visited Apr. 11, 2022).
54. *Summary of the HIPAA Security Rule*, *supra* note 42.
55. *Id.*

Because covered entities are not required to adopt any specific security measures, the Security Rule does not require encryption of PHI.[56] Encryption converts "an original message of regular text into encoded text" using an algorithm.[57] Once the recipient receives the encrypted information, the recipient can restore the plain text of the information only by using a key, which is "a group of random characters in a particular order."[58] By encrypting information, a party can reduce the likelihood that someone other than the intended recipient would be able to translate the information into plain text.[59]

There are two main types of encryption: symmetric and asymmetric.[60] For symmetric encryption, "the sender uses the same secret key to decrypt the text as the recipient uses to decrypt the text."[61] Asymmetric encryption, on the other hand, requires two different keys.[62] The sender encrypts the message using a public key, and the recipient uses a private key to decrypt the message.[63] Although the public key can be made known to and identified by anyone, only the person decrypting the message can know the private key.[64] With end-to-end encryption, a form of asymmetric encryption, only those with the decryption keys can see the encrypted information.[65] End-to-end encryption thus "prevents unintended users, including third parties, from reading or modifying data when only the intended readers should have this access and ability."[66] When using any form of encryption, entities must ensure the security of encryption keys.[67] Entities may store keys on secure repositories, such as a local hard drive or a USB, but access to those keys should be limited and methods of verifying those who access the key, such as passwords, should be used.[68] Although encryption requires entities to ensure security of encryption keys regularly, which may be difficult for some entities, encryption is a useful tool in securing private information.[69]

---

56. *Is the Use of Encryption Mandatory in the Security Rule?*, U.S. DEP'T HEALTH & HUM. SERVS. [hereinafter *Is the Use of Encryption Mandatory?*], https://www.hhs.gov/hipaa/for-professionals/faq/2001/is-the-use-of-encryption-mandatory-in-the-security-rule/index.html [https://perma.cc/64YH-UJVL] (last updated July 26, 2013).

57. *What Is Encryption?*, U.S. DEP'T HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/faq/2021/what-is-encryption/index.html [https://perma.cc/LBD2-R469] (last updated July 26, 2013); *see* Nina Patel, Note, *Your Personal Health Information May Have Been Compromised: Using Encryption to Prevent Data Breaches on End-User Devices*, 48 HOFSTRA L. REV. 563, 578 (2019).

58. Patel, *supra* note 57, at 578; *What Is a Cryptographic Key? Keys and SSL Encryption*, CLOUDFLARE, https://www.cloudflare.com/learning/ssl/what-is-a-cryptographic-key/#:~:text=Combined%20with%20an%20encryption%20algorithm,KZ0KVey8l1c%3D%22%20as%20the%20ciphertext [https://perma.cc/V5QG-TN2N] (last visited Mar. 4, 2022).

59. *What Is Encryption?*, *supra* note 57.

60. Patel, *supra* note 57, at 580.

61. *Id.*

62. *Id.*

63. *Id.*

64. *Id.* at 580-81.

65. *What Is End-to-End Encryption?*, IBM, https://www.ibm.com/topics/end-to-end-encryption [https://perma.cc/UY58-TYTS] (last visited Mar. 3, 2022).

66. *Id.*

67. Patel, *supra* note 57, at 580-81.

68. *Id.* at 581.

69. *See id.* at 564-65, 580-81.

Rather than requiring encryption, the Security Rule makes encryption an "addressable implementation specification."[70] The "addressable" designation "permits covered entities to determine whether the addressable implementation specification is reasonable and appropriate for that covered entity."[71] Thus, a covered entity is only required to implement encryption "if, after a risk assessment, the entity has determined that the specification is a reasonable and appropriate safeguard in its risk management of the confidentiality, integrity and availability of e-PHI."[72] If an entity determines that encryption is not reasonable and appropriate, the entity must note that decision and, if reasonable and appropriate, "implement an equivalent alternative measure."[73] An entity may not need to adopt either the implementation specification or the alternative if the Security Rule can be met otherwise, but the entity must record its rationale for doing so.[74]

Similar to encryption, other security measures are also addressable and, thus, are not required at the outset. One such security measure is a firewall. A firewall is a computer software or hardware that protects one's network "by filtering traffic and blocking outsiders from gaining unauthorized access to the private data" on the computer.[75] Firewalls can also prevent malicious software from infecting a computer.[76] Another such security measure is two-factor authentication. Two-factor authentication is a two-step log-in process that verifies the user's identity and prevents unauthorized individuals from accessing the user's information.[77] When HIPAA was first enacted, covered entities were required to consider and implement these technical considerations if it were "'reasonable and appropriate'" for the entity to do so, but compliance with HIPAA remained low until the passage of the HITECH Amendment.[78]

---

70. *Is the Use of Encryption Mandatory?*, *supra* note 56.

71. *Summary of the HIPAA Security Rule*, *supra* note 42.

72. *Is the Use of Encryption Mandatory?*, *supra* note 56; *see, e.g.*, Press Release, U.S. Dep't Health & Hum. Servs., Lifespan Pays $1,040,000 to OCR to Settle Unencrypted Stolen Laptop Breach (July 27, 2020), https://public3.pagefreezer.com/content/HHS.gov/31-12-2020T08:51/https://www.hhs.gov/about/news/2020/07/27/lifespan-pays-1040000-ocr-settle-unencrypted-stolen-laptop-breach.html [https://perma.cc/NR2U-5ES4] (stating that Lifespan Health System Affiliated Covered Entity settled with HHS after OCR "determined that there was systemic noncompliance with the HIPAA Rules including a failure to encrypt ePHI on laptops after Lifespan ACE determined it was reasonable and appropriate to do so").

73. *Is the Use of Encryption Mandatory?*, *supra* note 56.

74. *Id.*

75. Alison Grace Johansen, *What Is a Firewall? Firewalls Explained and Why You Need One*, NORTONLIFELOCK (June 17, 2021), https://us.norton.com/internetsecurity-emerging-threats-what-is-firewall.html [https://perma.cc/G9R7-Q8PJ].

76. *Id.*

77. Kyle Chivers, *What Is Two-Factor Authentication (2-FA) and How Does It Work?*, NORTONLIFELOCK (Oct. 15, 2020), https://us.norton.com/blog/how-to/importance-two-factor-authentication [https://perma.cc/7YYR-G922].

78. Patel, *supra* note 57, at 572-73, 575.

d. The HITECH Amendment to HIPAA

Prior to 2009, HIPAA included loopholes that allowed covered entities to avoid sanctions for violating HIPAA "by claiming their business associates were unaware that they were violating HIPAA."[79] Additionally, penalties for violations of HIPAA were too low to incentivize health care organizations and business associates to comply with HIPAA.[80] To remedy these issues, Congress passed the Health Information Technology for Economic and Clinical Act of 2009 ("HITECH Act" or "HITECH").[81] The HITECH Act expanded enforcement and penalties of HIPAA, business associate duties under HIPAA, and patient rights.[82] The HITECH Act increased monetary penalties and increased enforcement in a variety of ways, including increased public education of PHI and authorization of state attorneys general to bring civil suits.[83] Covered entities were now subject to increased civil penalties for violations of HIPAA.[84]

In addition to increasing enforcement and penalties of HIPAA, HITECH also expanded the duties of business associates under HIPAA. HITECH bound business associates to the HIPAA Security Rule requirements.[85] Additionally, business associates were now subject to civil and criminal penalties for violations of the Security Rule.[86] Thus, as with covered entities, business associates were required to implement, maintain, develop, and document security measures to safeguard PHI; however, business associates, like covered entities, had flexibility in what security measures they implement.[87]

The HITECH Act also expanded patient rights under HIPAA. Under HITECH, patients are allowed to access and obtain their electronic health information.[88] Additionally, HITECH prohibited business associates from marketing, without authorization, e-PHI.[89] Moreover, if patients had originally authorized business associates to use e-PHI, patients can now revoke that authorization.[90] Finally, HITECH requires that any disclosures of PHI be recorded, which includes noting who the information was given to and the purpose of the disclosure.[91] Although HITECH addressed some of the

79. *What Is the HITECH Act?*, HIPAA J., https://www.hipaajournal.com/what-is-the-hitech-act/ [https://perma.cc/UB6R-663S] (last visited Jan. 28, 2022).
80. *Id.*
81. Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226, 246 (2009) (codified in scattered sections of 42 U.S.C.).
82. *Id.*
83. Jason W. Davis, *HITECH HIPAA Amendments: New Rules on Breach Notification, Business Associate Compliance, and Enforcement*, 21 HEALTH L. 23, 26 (2009).
84. *Id.*
85. *Id.* at 25.
86. *Id.*
87. *Id.*
88. *What Is the HITECH Act?*, *supra* note 79.
89. *Id.*
90. *Id.*
91. *Id.*

limitations of HIPAA, potential privacy issues with HIPAA remain and must be addressed.

2. Potential Privacy Issues with HIPAA

As it stands, HIPAA is still susceptible to privacy issues. Because the Security Rule only requires entities to "determine whether the addressable implementation specification is reasonable and appropriate for that covered entity," covered entities have considerable discretion in determining what security measures to adopt, when to adopt those measures, and whether to adopt an alternative measure.[92] Moreover, the Security Rule lacks guidance for how covered entities should identify possible risks to e-PHI or how to address potential risks to the information.[93] Entities, particularly smaller covered entities, may not have the requisite knowledge or expertise to conduct regular assessments for identifying potential risks.

Additionally, the Security Rule allows covered entities to forgo adopting either the implementation specification or the alternative if the Security Rule can be met otherwise.[94] Of course, the entities must record their rationale for doing so, but this potential loophole could allow covered entities to make an excuse in order to forego implementing a security measure that they may see as a time-waster or a drain on resources.[95] These potential privacy issues became more salient in 2020 when the COVID-19 pandemic forced people to turn to telehealth services for routine medical care.

3. Department of Health and Human Services' Notification of Relaxed Enforcement

In response to the pandemic, HHS issued a notice in March of 2020 detailing limited waivers of select provisions in HIPAA for the duration of COVID-19.[96] The notice states that the Office for Civil Rights ("OCR") will "exercise its enforcement discretion and will not impose penalties for noncompliance with the regulatory requirements under HIPAA Rules against covered health care providers in connection with the good faith provision of telehealth during the COVID-19 nationwide public health emergency."[97] OCR is a division of HHS in charge of enforcing federal civil rights laws, including HIPAA.[98] If a provider uses telehealth services and there is a breach

92. *Summary of the HIPAA Security Rule*, *supra* note 42; *see* Sharona Hoffman & Andy Podgurski, *In Sickness, Health, and Cyberspace: Protecting the Security of Electronic Private Health Information*, 48 B.C. L. REV. 331, 337 (2007).

93. *See* Hoffman & Podgurski, *supra* note 92, at 351.

94. *Is the Use of Encryption Mandatory?*, *supra* note 56.

95. *Id.*

96. *Notification of Enforcement Discretion*, *supra* note 5; Anna Clark & Joel Thayer, *What Privacy Compliance Looks Like During COVID-19*, LAW360 (Apr. 8, 2020, 1:15 PM), https://www.law360.com/articles/1261184 [https://perma.cc/5PDW-UD7K].

97. *Notification of Enforcement Discretion*, *supra* note 5.

98. *About Us*, U.S. DEP'T HEALTH & HUM. SERVS., https://www.hhs.gov/ocr/about-us/index.html [https://perma.cc/AP95-SYXY] (last visited Jan. 24, 2022).

in which e-PHI is intercepted, OCR will not automatically impose a penalty for violating the HIPAA Security Rule during the pandemic.[99] Instead, OCR will use its enforcement discretion and determine if the breach resulted from good faith efforts to provide telehealth services.[100] In determining whether there has been good faith, OCR will consider the facts and circumstances surrounding the breach.[101] Thus, even if a health care provider does not analyze possible privacy risks of a telehealth service or otherwise take steps to ensure patient privacy, they may still use telehealth services to connect with patients without violating HIPAA.[102] This notice does not apply to all entities covered by HIPAA (e.g., health insurance companies who pay for telehealth services), only covered health care providers utilizing telehealth services.[103] Additionally, covered health care providers who want to use audio or video technology in order to provide telehealth services to patients may use any non-public facing platform, including Facebook Messenger, Google Hangouts, and FaceTime, even if those platforms are not HIPAA compliant.[104]

a. Non-Public Facing vs. Public-Facing Platforms

Non-public facing communication platforms only allow authorized parties to communicate.[105] Generally, these non-public facing platforms use end-to-end encryption, enabling only authorized individuals to see the communication that is transmitted.[106] Additionally, non-public facing platforms permit separate user accounts and passwords, allowing those platforms to verify participants.[107] Finally, non-public facing platforms provide users with the ability to control the platform to an extent by allowing users to choose whether to record the communication or to switch off the audio or video.[108] Public-facing platforms, such as Facebook Live and TikTok, are "designed to be open to the public or allow wide or indiscriminate

99. *If a Covered Health Care Provider Uses Telehealth Services During the COVID-19 Outbreak and Electronic Protected Health Information is Intercepted During Transmission, Will OCR Impose a Penalty on the Provider for Violating the HIPAA Security Rule?*, U.S. DEP'T HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/faq/3025/if-a-covered-health-care-provider-uses-telehealth-services-during-the-covid-19-outbreak-and-electronic-protected-health-information-is-intercepted-during-transmission-will-ocr-impose-a-penalty-on-the-provider/index.html [https://perma.cc/HL9S-NPKS] (last updated Mar. 27, 2020).

100. *Id.*

101. *Id.*

102. *Pandemic Telehealth Fact Sheet*, *supra* note 25.

103. *Notification of Enforcement Discretion*, *supra* note 5.

104. *Id.*

105. *What Is a "Non-Public Facing" Remote Communication Product?*, U.S. DEP'T HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/faq/3024/what-is-a-non-public-facing-remote-communication-product/index.html [https://perma.cc/95AJ-GGYH] (last visited Jan. 24, 2022).

106. *Id.*

107. *Id.*

108. *Id.*

access to the communication" and are thus not allowed for telehealth services.[109]

Although HHS provides specific qualifications for what applications and video platforms covered entities are allowed to use when connecting with patients, there are still serious implications for patients' privacy.[110] HHS explicitly prohibits the use of public facing platforms for telehealth services, but the Notification does not require that the non-public facing platforms be HIPAA compliant.[111] Thus, the use of even non-public facing platforms may not be secure.[112] Such platforms may not currently use encryption or other security measures to protect patient information.

b. BAAs Under the Notification of Relaxed Enforcement

OCR has not required covered entities to enter into a business associate agreement with vendors of video communication platforms during the pandemic.[113] Relaxing the requirement of BAAs could have negative consequences for patient privacy. Some of the video platforms that had entered into BAAs and complied with HIPAA before the pandemic may be secure and may utilize enhanced security provisions. However, other platforms that had not already offered telehealth services may not be compliant.[114] The Notification mentions vendors, such as Skype and Zoom, that have marketed products claimed to be HIPAA compliant, but OCR has not reviewed the BAAs of these platforms, nor has OCR endorsed these platforms.[115] Because telehealth services were in high demand due to the pandemic, many providers likely were not able to ensure that the chosen platform was HIPAA-compliant.[116]

Business associates are also allowed to share data related to COVID-19, including PHI.[117] The Privacy Rule already allows covered entities to share this data.[118] The justification for this is that federal, state, and local agencies "need quick access to COVID-19 related health data to fight this

109. *Id.*; *Notification of Enforcement Discretion*, *supra* note 5.

110. *Notification of Enforcement Discretion*, *supra* note 5.

111. *Id.*

112. *Notification of Enforcement Discretion*, *supra* note 5; *see* Sharon Bassan, *Data Privacy Considerations for Telehealth Consumers amid COVID-19*, 7 J.L. & BIOSCIENCES 1, 5-6 (2020).

113. *Notification of Enforcement Discretion*, *supra* note 5.

114. *See* Bassan, *supra* note 112, at 5.

115. *Notification of Enforcement Discretion*, *supra* note 5; *see* Bassan, *supra* note 112, at 5.

116. *See* Bassan, *supra* note 112, at 5-6.

117. ROBERT GELLMAN & PAM DIXON, WORLD PRIV. F., COVID-19 AND HIPAA: HHS'S TROUBLED APPROACH TO WAIVING PRIVACY AND SECURITY RULES FOR THE PANDEMIC 13 (2020), https://www.worldprivacyforum.org/2020/09/covid-19-and-hipaa/ [https://perma.cc/29VV-H97G].

118. *Id.* at 3.

pandemic."[119] This justification may not be entirely persuasive because business associates who have already entered into BAAs with health care providers must adhere to those agreements with regards to sharing data.[120] Business associates, thus, must be specifically authorized by the covered entity to release the data to those agencies.[121] Although some business associates may be prevented from disclosing PHI, some health care providers may be using video communications platforms that they have not entered into BAAs with. Additionally, business associates are not limited to disclosing this information to public health agencies; rather, a business associate can disclose PHI to "anyone it believed 'in good faith' could make a contribution to the emergency."[122] Thus, a business associate could potentially release private patient information in good faith to a company that may in turn use the information for a different purpose.[123] Because business associates are not held to the same medical ethical standards as covered entities, business associates may not act with the same level of restraint in disclosing patient information.[124]

c. Waiver of Privacy Notifications to Patients and of Sanctions

OCR encourages doctors and health care providers to notify their patients of the security risks posed by using telehealth services; however, OCR does not require patients to be notified of those risks before doctors engage with their patients over telehealth services.[125] HHS has also waived sanctions and penalties for noncompliance with requirements relating to privacy notices and patient agreement to disclosures of PHI as long as the noncompliance is in good faith.[126] For the duration of the COVID-19 pandemic, covered entities need not acquire a patient's consent to speak with family or friends about the patient's care, nor do covered entities need to "distribute a notice of privacy practices."[127] Additionally, covered entities are

119. GELLMAN & DIXON, *supra* note 117 at 13; *see* Nancy L. Perkins, *Personal Health Information Privacy and COVID-19: HIPAA and California Law Enforcement Forbearance*, ARNOLD & PORTER (Apr. 8, 2020), https://www.arnoldporter.com/en/perspectives/publications/2020/04/personal-health-information-privacy-and-covid-19 [https://perma.cc/3JBA-MR29].

120. Caroline D. Kessler, *HHS OCR to Exercise Enforcement Discretion to Allow Business Associates to Share PHI for Public Health and Health Oversight Activities*, AKIN GUMP (Apr. 9, 2020), https://www.akingump.com/en/experience/practices/cybersecurity-privacy-and-data-protection/ag-data-dive/hhs-ocr-to-exercise-enforcement-discretion-to-allow-business-associates-to-share-phi-for-public-health-and-health-oversight-activities.html [https://perma.cc/43DY-XDAJ].

121. GELLMAN & DIXON, *supra* note 117, at 13-14.

122. GELLMAN & DIXON, *supra* note 117, at 15; *see* Kessler, *supra* note 120.

123. GELLMAN & DIXON, *supra* note 117, at 15 (providing an example of a business associate who releases PHI to a commercial data broker for public health analysis, but intermediary turns out to be a Medicare fraudster).

124. *Id.*

125. *Pandemic Telehealth Fact Sheet*, *supra* note 25.

126. GELLMAN & DIXON, *supra* note 117, at 4-5.

127. *Id.* at 9.

not required to acquiesce to a patient's request for privacy restrictions or for confidential communications.[128]

This relaxation of privacy notifications to patients and the waiver of sanctions has serious implications for patient privacy. Patients may not know that health care providers do not need their permission to speak with family and friends about the patient for the duration of the pandemic.[129] Additionally, patients are unlikely to know what privacy policies are in place or the possible risks to their privacy without receiving the privacy notices from the provider.[130] The Notification of Relaxed Enforcement highlights potential issues for patient privacy during the pandemic, but the Notification also highlights issues with HIPAA that will continue even after the pandemic, thus necessitating reform.

III. ANALYSIS

The potential privacy issues for patients' health information should be addressed by reforming HIPAA. Congress should reform HIPAA so that it maintains flexibility regarding telehealth platforms while protecting patients' personal information by including specific security measures and detailing best practices for health care providers, business associates, and patients. Such security measures and best practices include implementing encryption, firewalls, and two-factor authentication.

Part A of the analysis addresses the feasibility of congressional action on this issue and argues that, although Congress appears unwilling to compromise on many issues, Congress is willing to address healthcare. Part B of this section explores why the FCC should have an expanded role in regulating telehealth services. Part C describes how HIPAA should be reformed to include greater flexibility while also including heightened privacy protections, such as encryption and two-factor authentication. Finally, Part D examines some of the limits of the proposal and addresses possible ways of mitigating those limitations.

A. Although Congress Appears Unwilling to Compromise on any Issues, Congress is Willing to Address and Act on Issues Involving Healthcare

Over the years, Congress has become increasingly polarized, as evidenced by the Pew Research Center's finding that "Democrats and Republicans are farther apart ideologically today than at any time in the past 50 years."[131] Because of this increasing polarization and congressmembers'

128. *Id.*

129. *See* Bassan, *supra* note 112, at 6-7; GELLMAN & DIXON, *supra* note 117, at 9.

130. *See* Bassan, *supra* note 112, at 6-7; GELLMAN & DIXON, *supra* note 117, at 9.

131. Drew DeSilver, *The Polarization in Today's Congress Has Roots That Go Back Decades*, PEW RSCH. CTR. (Mar. 10, 2022), https://www.pewresearch.org/fact-tank/2022/03/10/the-polarization-in-todays-congress-has-roots-that-go-back-decades/ [https://perma.cc/8XMB-BS8R].

fear of losing reelections, Congress has been unwilling to compromise and act on a variety of issues.[132] Polarization and the resulting unwillingness to compromise has led to greater congressional inaction characterized by a "my way or the highway" mentality.[133]

Despite Congress' polarization and apparent unwillingness to compromise, Congress could feasibly address and act on issues involving healthcare in a bipartisan manner. Recent congressional action demonstrates that Congress is willing to address important healthcare issues in general, as well as telehealth in particular. For example, Congress worked quickly to pass the CARES Act in order to expand access to healthcare generally, and telehealth services in particular, during the pandemic.[134]

Furthermore, Senators Tammy Baldwin (D-WI) and Bill Cassidy, M.D. (R-LA) recently introduced the Health Data Use and Privacy Commission Act.[135] This Act would form a commission "to research and give official recommendation[s] to Congress on how to modernize the use of health data and privacy laws to ensure patient privacy and trust while balancing the need of doctors to have information at their fingertips to provide care."[136] The commission would be responsible for reviewing existing state and federal protections for PHI, as well as how health care and other industries use health data.[137] Finally, the commission would be charged with providing recommendations and conclusions on, among other things, "potential threats posed to individual health privacy and legitimate business and policy interests," "[t]he effectiveness of existing statutes [and] regulations . . . in protecting individual health privacy," and "whether federal legislation is necessary, and if so, specific suggestions on proposals to reform, streamline, harmonize, unify, or augment current laws and regulations relating to individual health privacy . . . ."[138] Recent congressional actions and the

---

132. *See* David Davenport, *Congress and the Lost Art of Compromise*, FORBES (Jan. 24, 2018, 1:00 PM), https://www.forbes.com/sites/daviddavenport/2018/01/24/congress-and-the-lost-art-of-compromise/?sh=637b5743d597 [https://perma.cc/8DBL-WMJ3]; Sarah E. Anderson et al., *Biden Wants to Bring Democrats and Republicans Together. Here's Why That's So Challenging.*, WASH. POST (Dec. 21, 2020), https://www.washingtonpost.com/politics/2020/12/21/biden-wants-bring-democrats-republicans-together-heres-why-thats-so-challenging/ [https://perma.cc/F68U-2MGE].

133. Frank Newport, *The Impact of Increased Political Polarization*, GALLUP (Dec. 5, 2019), https://news.gallup.com/opinion/polling-matters/268982/impact-increased-political-polarization.aspx [https://perma.cc/KP24-D98D].

134. Coronavirus Aid, Relief, and Economic Security Act, Pub. L. No. 116-136, 134 Stat. 281 (2020); Amber Phillips, *'Totally Unprecedented in Living Memory': Congress's Bipartisanship on Coronavirus Underscores What a Crisis This Is*, WASH. POST (Mar. 26, 2020, 12:35 PM) https://www.washingtonpost.com/politics/2020/03/26/totally-unprecedented-living-memory-congresss-bipartisanship-coronavirus-underscores-what-crisis-this-is/ [https://perma.cc/WB2Q-EHRH].

135. Press Release, Bill Cassidy, Senator, *Cassidy,* Baldwin Introduce Legislation to Begin Modernization of Health Privacy Laws (Feb. 9, 2022), https://www.cassidy.senate.gov/newsroom/press-releases/cassidy-baldwin-introduce-legislation-to-begin-modernization-of-health-privacy-laws [https://perma.cc/8JVD-6LYM].

136. *Id.*

137. *Id.*

138. *Id.*

proposed bill demonstrate the feasibility of Congress addressing and acting on matters concerning healthcare, despite the intense polarization.

B. The FCC Should Have a Larger Role in Regulating Telehealth Due to its Expertise in Communications and History with Telemedicine

The FCC's long history of ensuring that all Americans have access to telehealth services indicates that the FCC's role in regulating telehealth is critical.[139] Since 1996, the FCC has encouraged and implemented the use of telehealth services, particularly in rural areas.[140] Moreover, the FCC has worked with other agencies to provide telehealth services in a safe and effective manner, indicating that the FCC is capable of further regulating telehealth.[141]

In addition to the FCC's historical involvement in telehealth, the recent statements of FCC Commissioner Geoffrey Starks and Chairwoman Jessica Rosenworcel highlight the FCC's prioritization of improving telehealth. In February 2022, Commissioner Starks made a statement regarding the proposal for further reforms to the Rural Health Care Program.[142] Commissioner Starks highlighted the crucial role that telehealth plays, noting that telehealth "is critically important to communities across the country, and especially in rural America."[143] Similarly, Chairwoman Rosenworcel highlighted the effectiveness and importance of telehealth during the pandemic and noted that the COVID-19 Telehealth Program has allowed the FCC to "expand the reach of communications and the possibilities of telehealth."[144]

The FCC currently has an enforcement process for protecting consumers from harmful uses of telecommunications, and this process could be applied to telehealth.[145] The Telecommunications Consumers Division investigates "the practices of companies engaged in various telecommunications-related activities," resolves "formal complaints brought by consumers," and consults "with internal and external organizations to ensure the FCC rules provide the maximum protection."[146] Applying this type

---

139. *See* Telecommunications Act of 1996, Pub. L. No. 104-104, § 706, 110 Stat. 56, 152 (1996); *FCC Health IT Actions and Activities Timeline*, *supra* note 17.

140. *See* Telecommunications Act § 254; *FCC Health IT Actions and Activities Timeline*, *supra* note 17.

141. *See FCC Health IT Actions and Activities Timeline*, *supra* note 17.

142. FCC Seeks Comment on Further Reforms to Rural Health Care Program, *Further Notice of Proposed Rulemaking*, FCC 22-15 (2022), https://docs.fcc.gov/public/attachments/DOC-380472A4.pdf [https://perma.cc/8UL2-8UNM].

143. *Id.* at para. 1.

144. COVID-19 Telehealth Program, *Report and Order and Order on Reconsideration*, FCC 21-39, para. 6 (2021), https://docs.fcc.gov/public/attachments/FCC-21-39A2.pdf [https://perma.cc/UR3A-MU5R].

145. *See* ENFORCEMENT BUREAU, FCC, ENFORCEMENT OVERVIEW 5 (2020), https://www.fcc.gov/sites/default/files/public_enforcement_overview.pdf [https://perma.cc/M63G-MMKX].

146. *Id.*

of process to telehealth, the FCC would investigate the practices of health care providers and their business associates. Additionally, the FCC would resolve complaints brought by patients and consult with organizations both within and outside of the FCC. Given the FCC's investment in telehealth and its extensive expertise in communications platforms and law, the FCC would play a vital role in ensuring that telehealth services protect patient safety.

C. HIPAA Should Retain Flexibility but Should Include Best Practices for Ensuring Data Privacy, and Agencies Should Coordinate on Implementation of Privacy Standards

1. Maintaining Flexibility

HIPAA should be reformed to maintain the flexibility it has during the pandemic, while still protecting patient privacy. Prior to HHS' Notification of Relaxed Enforcement, it was challenging to use everyday video platforms, such as FaceTime and Facebook Messenger, for telehealth. These everyday platforms typically were not HIPAA-compliant or did not have a BAA.[147] The Notification allows patients to connect with healthcare providers through these common video platforms, even if those platforms were not HIPAA-compliant.[148] This allows patients with limited access to technology and other software to receive healthcare without risking their health through in-person visits.[149]

Although this new flexibility in the type of platforms health care providers may utilize should remain after the pandemic, the privacy of patient information must be addressed.[150] These platforms must be updated to ensure that they will be HIPAA-compliant post-pandemic. Additionally, health care providers must enter into BAAs with these platforms to ensure that there are provisions in place to adequately protect patient information. Although maintaining flexibility with respect to the allowed video platforms is important, more reforms are needed to protect patient privacy.

2. Covered Entities Should Implement Privacy Safeguards

HIPAA should be reformed to include express requirements for security measures that must be implemented before providing telehealth services. Although covered entities vary in ways that may affect the ability of a covered entity to adopt a specific security measure, one such measure that all covered entities should adopt is PHI encryption.[151] There are a variety of

147. Clark & Thayer, *supra* note 96.

148. *Notification of Enforcement Discretion*, *supra* note 5.

149. *See* Steve North, Opinion, *These Four Telehealth Changes Should Stay, Even After the Pandemic*, FAM. PRAC. MGMT., May-June 2021, at 9, 9-10 (2021), https://www.aafp.org/fpm/2021/0500/fpm20210500p9.pdf [https://perma.cc/LXN5-3HK8].

150. *See id.*

151. *See* Patel, *supra* note 57, at 588-91.

encryption methods that allow covered entities to choose the best fit.[152] According to an IBM Security report, the average cost of a data breach has risen to $9.42 million.[153] The report further found that the cost of a data breach decreased at companies that utilized encryption and other security measures.[154] Those companies saved between $1.25 million and $1.40 million for each data breach that occurred.[155] Thus, the cost of a data breach far outweighs the cost of implementing and maintaining encryption.[156]

The requirement to implement and maintain encryption should apply to both covered entities and business associates. All PHI should be encrypted, including when transferred onto a flash drive, CD, or other portable electronic device.[157] Additionally, when sending e-PHI over email, covered entities and business associates should ensure that the email server is secure and that the email is encrypted.[158] Finally, health care providers that record and store video telehealth visits should adopt encryption.[159] In expressly requiring the implementation and maintenance of encryption, HIPAA should direct the FCC to provide guidance on current standards and techniques for encryption to covered entities and business associates in order to mitigate any user error.[160] Such guidance should include methods of conducting regular risk assessments, as well as guidance on which type of encryption to adopt.[161] The FCC has far-reaching expertise in providing guidance on cybersecurity. For example, the FCC has provided a cybersecurity tip sheet for small businesses.[162] Thus, it is qualified to provide similar guidance to covered entities and business associates.

---

152. *See id.* at 588-91.

153. *The Average Cost of a Healthcare Data Breach is Now $9.42 Million*, HIPAA J. (July 29, 2021), https://www.hipaajournal.com/average-cost-of-a-healthcare-data-breach-9-42-million-2021/ [https://perma.cc/V43R-CKRE].

154. *Id.*

155. *Id.*

156. *See id.*; Patel, *supra* note 57, at 590.

157. *See* Roger Hsieh, *Improving HIPAA Enforcement and Protecting Patient Privacy in a Digital Healthcare Environment*, 46 LOY. U. CHI. L.J. 175, 184 n.51 (2014) (noting that "PHI can be stored in a wide variety of mediums . . . which can lead to breaches of patient privacy").

158. *See id.*; Patel, *supra* note 57, at 590.

159. Geoffrey Lottenberg, *COVID-19 Telehealth Boom Demands Better Privacy Practices*, LAW360 (July 2, 2020, 4:11 PM), https://www.law360.com/cybersecurity-privacy/articles/1287404/covid-19-telehealth-boom-demands-better-privacy-practices- [https://perma.cc/ZJD2-87TB].

160. *See* Patel, *supra* note 57, at 582.

161. *See, e.g.*, *id.* at 589-90 (arguing that hospitals and insurance companies should be required to implement asymmetric encryption, that smaller covered entities and business associates should at least utilize symmetric encryption keys, that all entities should "conduct independent audits to determine if they have adequate protection because symmetric encryption may not be enough," and that "risk assessments and other factors, such as financial feasibility, size, and complexity of the entity," should inform the determination of whether to use asymmetric encryption).

162. *Ten Cybersecurity Tips for Small Businesses*, FCC (May 16, 2011), https://apps.fcc.gov/edocs_public/attachmatch/DOC-306595A1.pdf [https://perma.cc/6WBE-RQW5].

3. Best Practices for Maintaining Data Privacy

In addition to requiring certain security measures, HIPAA should include specific best practices that health care providers, business associates, and patients should undertake. HIPAA, while including a list of best practices, could also include the organization that should be responsible for generating more best practices. Given the FCC's extensive background with a variety of technologies and HHS' involvement in telehealth, these two agencies seem best positioned for this task.

Two such best practices that could be listed are firewalls and two-factor authentication.[163] Health care providers that record and store video telehealth visits should have a firewall to ensure that unsanctioned individuals do not gain access to private health information and to prevent threats from malicious software.[164] Health care providers can also implement two-factor authentication as an extra step to ensure patients' private information is protected.[165] By implementing two-factor authentication, health care providers can verify the identity of individuals accessing the private health information.[166]

In addition to implementing security measures such as firewalls and two-factor authentication, health care providers should carefully review BAAs to ensure that the agreement provides the best possible protection. Similarly, covered entities should notify their patients of the potential risks of engaging in telehealth services, including the risks of using video platforms. Additionally, covered entities should notify patients of privacy notices even when not required to do so.

Patients can also take steps before engaging in telehealth services to understand the possible risks and assess whether the risks outweigh the benefits of using the service. One best practice for patients is reading the privacy policy of whichever technology they will be using.[167] In doing so, patients can decide beforehand whether to use that particular technology. When reading the privacy policy, patients should focus on parts of the notice that specify what information can be used or disclosed, "persons authorized to use or disclosure [sic] the information, those to whom disclosure may be made, and each purpose for disclosure."[168]

Because privacy policies are not typically user-friendly, the FCC should direct the Consumer Advisory Committee ("CAC") to provide guidance on how providers can offer streamlined, user-friendly versions of privacy policies. In 2016, the CAC provided broadband labels "to provide consumers of mobile and fixed broadband Internet service with easy-to-

163. Lottenberg, *supra* note 159.
164. *Id.*
165. *See id.*
166. *See* Chivers, *supra* note 77.
167. Bassan, *supra* note 112, at 8.
168. *Id.* at 8-9.

understand information about price and performance."[169] These labels provided consumers with information about the price, speed, and reliability of broadband services, and they served as a "'safe harbor'" for meeting the Open Internet transparency rules.[170] These rules "require broadband Internet service providers to disclose this information to consumers in an accurate, understandable and easy-to-find manner."[171] The FCC should direct the CAC to provide similar guidance on how health care providers can provide easy-to-understand information regarding the possible security risks to patient privacy when using telehealth services. Such guidance should also inform patients of ways they can limit possible security risks.

4. Agency Coordination

Finally, HIPAA should be reformed to include agency coordination. The FCC and HHS should work together to effectively enforce and implement HIPAA. Given HHS' mission to "enhance the health and well-being of all Americans"[172] and the FCC's expertise in regulating and implementing communications law, these two agencies are best positioned to protect patient privacy and ensure telehealth services are safe and effective.

D. The Proposal to Reform HIPAA is Limited by Security Risks Posed by Patients Using Telehealth Services, but Health Care Providers Can Mitigate These Risks

Although covered entities and business associates are legally bound to provide secure and safe platforms for telehealth services, patients can also pose security risks to themselves. Thus, HIPAA does not completely mitigate security risks. Patients pose security risks by using public Wi-Fi, sending information on unsecure websites, and accessing telehealth services outside of a private location.[173] Public Wi-Fi typically uses unsecure networks, which could allow unauthorized people to read data sent from a computer.[174] Using public Wi-Fi also risks that someone could put malware onto a computer.[175] Additionally, sending information on unsecure websites and using telehealth

169. Press Release, FCC, FCC Unveils Consumer Broadband Labels to Provide Greater Transparency to Consumers 1 (Apr. 4, 2016), https://docs.fcc.gov/public/attachments/DOC-338708A1.pdf [https://perma.cc/J3PN-666L].

170. *Id.*

171. *Id.*

172. *About HHS*, U.S. DEP'T HEALTH & HUM. SERVS., https://www.hhs.gov/about/index.html [https://perma.cc/QNB8-9JDW] (last visited Jan. 30, 2022).

173. *See Telehealth Privacy for Patients*, HEALTH RES. & SERVS. ADMIN., https://telehealth.hhs.gov/patients/telehealth-privacy-for-patients/ [https://perma.cc/43FC-CY5W] (last updated Dec. 15, 2021).

174. *The Risks of Public Wi-Fi*, NORTONLIFELOCK (May 26, 2018), https://us.norton.com/internetsecurity-privacy-risks-of-public-wi-fi.html [https://perma.cc/U5DG-TF3E].

175. *Id.*

services outside of a private location heightens the risk that someone could read a patient's PHI.

Although health care providers are unlikely to completely reduce the security risks patients may pose, there are ways that health care providers can help patients mitigate those risks. Prior to the telehealth visit, health care providers can expressly inform patients to avoid using public Wi-Fi and to attend telehealth appointments from a private location. Additionally, health care providers can advise patients what to look for to ensure that the website or platform is secure. Moreover, health care providers should present patients with a list of possible risks from using public Wi-Fi or unsecure websites. Finally, health care providers should provide patients with the best practices list, including firewalls and two-factor authentication. By explicitly notifying patients of practices that could pose security risks to PHI, health care providers can mitigate security risks and limit exposure to liability.

IV. CONCLUSION

The onset of the COVID-19 pandemic has highlighted ways in which HIPAA should be reformed to address issues with using telehealth services. HHS' Notification of Relaxed Enforcement allows health care providers to offer telehealth services through common platforms such as Facebook Messenger and FaceTime, and thus patients with limited access to more advanced video platforms can connect with their health care team without in-person contact. Although this increased flexibility allows patients and health care providers to easily connect, it also raises privacy concerns. The Notification of Relaxed Enforcement states that OCR will use its enforcement discretion to determine whether to penalize health care providers who utilize non-HIPAA compliant platforms. Allowing providers to use non-HIPAA compliant platforms for telehealth services invites possible security risks to patients' private health information.

The risks highlighted from the use of non-HIPAA compliant platforms also highlights inadequacies in HIPAA as it stands outside of a public health emergency. HIPAA does not mandate covered entities to adopt specific security measures; rather, covered entities only need to adopt security measures after a risk to PHI has been identified. Thus, HIPAA should be reformed to maintain the flexibility of video platforms while mandating specific security measures and providing guidance for best practices in offering telehealth services.