Houston Journal of Health Law & Policy

ARTIFICIAL INTELLIGENCE AND THE HIPAA PRIVACY RULE: A PRIMER

Stacey A. Tovino, JD, PhD*

* John B. Turner LLM Program Chair in Law.

I. INTRODUCTION

Consider a medical chatbot that a hospital makes available to patients scheduled for colonoscopies.[1] The chatbot uses artificial intelligence (AI)[2] to conduct online conversations via text or text-to-speech in lieu of providing patients direct contact with a live person.[3] The chatbot, which was designed to improve patient compliance with unpleasant bowel preparation, has been shown to increase the number of people who have successful colonoscopies and decrease the number of people who fail to show for their procedures.[4] Given that patients do share sensitive, bowel-related information with the chatbot, one question is whether federal or state laws protect the privacy and security of their information.

Further consider an AI-driven symptom checker that a health system makes available on its website.[5] After users enter their age, biological sex, location, and symptoms, the checker offers possible diagnoses that match the users' symptoms.[6] Since users can disclose sensitive reproductive health information, including missed period, sexually transmitted infection, and sexual assault information,[7] the application

---

1 *See* Bertalan Mesko, *The Top 10 Health Chatbots*, THE MED. FUTURIST (Aug. 1, 2023), https://medicalfuturist.com/top-10-health-chatbots/ (referencing a medical chatbot that helps patients comply with bowel preparation instructions).

2 *See, e.g.*, E. Haavi Morreim, *Errors in the EMR: Under-recognized Hazard for AI in Healthcare*, 24 HOU. J. HEALTH L. & POL'Y 127, 130 (2024) (defining artificial intelligence (AI)); Amy B. Cyphert & Valarie K. Blake, *Code Blue: The Threat of Synthetic Data Use to Generative Medical AI*, 24 HOU. J. HEALTH L. & POL'Y 167, 168–70 (2024) (defining generative AI).

3 *See generally*, Scott Stiefel, *The Chatbot Will See You Now: Protecting Mental Health Confidentiality in Software Applications*, 20 SCI. & TECH. L. REV. 333, 333-37 (2019) (providing background information regarding the use of chatbots in health care).

4 *See* Mesko, *supra* note 1 (describing a colonoscopy-related chatbot offered by New York's Northwell Health system).

5 *See, e.g.*, *Symptom Checker*, UNIV. HOSP., https://www.uhhospitals.org/health-information/health-and-wellness-library/symptom-checker (last visited Dec. 23, 2023) (asking users to share their age, sex, and symptoms).

6 *See, e.g., Symptom Checker*, BANNER HEALTH, https://www.bannerhealth.com/patients/symptom-checker (last visited Dec. 23, 2023) (asking users to share their age, sex, location, and symptoms).

7 *See, e.g.*, *Symptom Checker*, UNIV. OF MICH. HEALTH, https://www.uofmhealth.org/health-library/sx (last visited Dec. 23, 2023) (allowing adult women users to click on the following symptoms: Abnormal Vaginal Bleeding, Female Genital Problems and Injuries, Groin Problems and Injuries, Menstrual Cramps, Missed or Irregular Periods, Pregnancy-Related

of privacy and security laws to the AI-powered symptom checker would seem to be important.

Consider, too, a physician who uses ChatGPT[8] to generate automated summaries of medical histories and patient interactions.[9] The physician enjoys using ChatGPT because it streamlines their[10] otherwise time-consuming medical record documentation obligations.[11] Assume, however, that a particular medical history summary generated by ChatGPT is incorrect and that the incorrect summary is not only placed in the patient's medical record but is also used and disclosed throughout the course of the patient's treatment and subsequent insurance billing.[12] Does the patient have the right under federal or state privacy law to restrict subsequent uses and disclosures of the incorrect, AI-generated summary? Does the patient have the right to amend the incorrect summary? And, do data privacy and security laws regulate ChatGPT—or maybe just the physician whose documentation is assisted by ChatGPT?

Problems, Problems After Delivery of Your Baby, Sexual Abuse or Assault (Rape), Sexually Transmitted Infections, and Urinary Problems and Injuries).

8 *See Introducing ChatGPT*, OPENAI, https://openai.com/blog/chatgpt (last visited Dec. 28, 2023) ("We've trained a model called ChatGPT which interacts in a conversational way. The dialogue format makes it possible for ChatGPT to answer follow-up questions, admit its mistakes, challenge incorrect premises, and reject inappropriate requests.").

9 *See, e.g.*, Bernard Marr, *Revolutionizing Healthcare: The Top 14 Uses Of ChatGPT In Medicine And Wellness*, FORBES (May 2, 2023), https://www.forbes.com/sites/bernardmarr/2023/03/02/revolutionizing-healthcare-the-top-14-uses-of-chatgpt-in-medicine-and-wellness/?sh=10c5cb806e54 (exploring different uses of ChatGPT in the healthcare industry, including medical record documentation).

10 To respect the full range of gender identities, this Article uses gender-inclusive words and phrases throughout. *See generally*, *Gender Diversity in Legal Writing: Pronouns, Honorifics, and Gender-Inclusive Techniques*, BRITISH COLUMBIA L. INST. 8 (2022) (arguing that gender-inclusive language focuses on important issues instead of relaying extraneous information about a person's gender; is simpler than attempting to balance writing with male and female pronouns; includes people who do not conform to binary genders; does not alienate people readers based on outdated masculinization or feminization language or gender stereotypes; and eliminates the risk of misgendering someone).

11 *See, e.g.*, Geoff Brumfiel, *Doctors Are Drowning in Paperwork. Some Companies Claim AI Can Help*, NAT'L PUB. RADIO (Apr. 5, 2023) (referencing the AI-driven tools of Glass Health, a company that has the goal of dramatically reducing physicians' paperwork burdens and improving their daily lives).

12 *See, e.g.*, *ChatGPT: Friend or Foe?* 5 LANCET DIGITAL HEALTH e102, e102 (2023) (noting that ChatGPT incorrectly added extra information to a patient's discharge summary).

Further consider a health insurer that uses AI to review and, more frequently than not, deny Medicare Advantage claims for elderly beneficiaries notwithstanding their physicians' documentation showing that their health care services are medically necessary.[13] Assume that the claims denials, which impose significant medical and financial hardships on the beneficiaries, result from the insurer's use of a faulty AI model that the insurer knows has a 90% error rate.[14] Is the insurer permitted to use AI to deny its beneficiaries' claims even if those beneficiaries do not know or have not authorized the processing of their information by AI? Further, assume that hackers install malware and conduct reconnaissance activities that result in the impermissible disclosure of the protected information of more than one million of the elderly beneficiaries, including their names, addresses, dates of birth, Social Security numbers, bank account information, and clinical treatment information, as well as their incorrect, AI-generated, claim denials.[15] What security and breach notification responsibilities does the insurer have? Can penalties be imposed on the insurer for its failure to conduct an enterprise-wide risk analysis and its refusal to implement risk management, information system activity review, and access controls, all of which led to the security breach?

Finally, consider the number of large technology companies and startups that are working with health industry participants, including

---

13 *See, e.g.*, Complaint at 1, ¶ 1, Lokken v. UnitedHealth Grp, Inc., No. O:23-cv-03514 (D. Minn. Nov. 14, 2023) ("This putative class action arises from Defendants' [UnitedHealth's] illegal deployment of artificial intelligence (AI) in place of real medical professionals to wrongfully deny elderly patients care owed to them under Medicare Advantage Plans by overriding their treating physicians' determinations as to medically necessary care based on an AI model that Defendants know has a 90% error rate.").

14 *See id.*; Elizabeth Napolitano, *UnitedHealth Uses Faulty AI to Deny Elderly Patients Necessary Coverage, Lawsuit Claims*, CBS NEWS (Nov. 20, 2023), https://www.cbsnews.com/news/unitedhealth-lawsuit-ai-deny-claims-medicare-advantage-health-insurance-denials/ (reporting that, "The families of two now-deceased former beneficiaries of UnitedHealth have filed a lawsuit against the health care giant, alleging it knowingly used a faulty artificial intelligence algorithm to deny elderly patients coverage for extended care deemed necessary by their doctors.").

15 *See, e.g., Health Insurer Pays $5.1 Million to Settle Data Breach Affecting Over 9.3 Million People*, U.S. DEP'T HEALTH & HUM. SERVS. (Jan. 15, 2021), https://public3.pagefreezer.com/browse/HHS.gov/28-12-2022T07:11/https://www.hhs.gov/about/news/2021/01/15/health-insurer-pays-5-1-million-settle-data-breach.html (announcing that Excellus (a HIPAA covered health plan) experienced a data breach very similar to the one described in the text accompanying this note).

hospitals and health insurers, to research, create, and deploy machine learning healthcare solutions.[16] These solutions could revolutionize health care, enabling earlier and more precise diagnostics; targeted and more effective treatments; clear-cut and more accurate outcomes predictions; and incredible cost savings.[17] To realize these ends, however, the technology companies need access to vast health data sets of hospitals and other health care providers.[18] Assume that a hospital that partners with a technology company removes almost two dozen identifiers from its patient medical records (in accordance with a federal de-identification safe harbor) to protect the privacy of the medical records subjects before disclosing their allegedly de-identified data to the technology company.[19] Assume, however, that the technology company is accused of being able to re-identify the purportedly de-identified data by combining it with other data sets in the company's possession.[20] Based on these facts, has patient privacy been violated? If a patient complains to the federal government of a privacy violation, can the government impose civil and criminal penalties on the hospital if it: (1) adhered to a federal de-identification regulation when removing the patient identifiers; (2) entered into a business associate agreement with the technology company, obligating the company to maintain patient privacy; and (3) claims it did not know that the de-identified information that was disclosed could be re-identified by the technology company? Does the potential for re-identification, without actual evidence of re-identification, qualify as a breach of unsecured protected information and do patients need to be notified of this breach? Should

---

16 *See, e.g.*, Jayanth Kancherla, *Re-identification of Health Data Through Machine Learning* 1 (2020) (referencing partnerships between health industry participants and AI-involved technology companies).

17 *See* Ed Corbett, *Real-World Benefits of Machine Learning in Healthcare*, HEALTH CATALYST (May 18, 2022), https://www.healthcatalyst.com/insights/real-world-benefits-machine-learning-healthcare.

18 *See id.*

19 *See, e.g.*, Dinerstein v. Google, LLC, 73 F.4th 502, 509–10 (7th Cir. 2023) (class action lawsuit against Google and the University of Chicago Medical Center alleging that the medical center improperly sold patient health information to Google, which, in conjunction with Google's other data, could be used to reveal patient identities and other sensitive information).

20 *See* Stacey A. Tovino, *Not so Private*, 71 DUKE L. J. 985 (2022) (synthesizing federal and state de-identification laws that expressly or potentially apply to health data and identifying significant weaknesses in these laws in light of the developing reidentification literature).

the technology company have been required to use synthetic data, rather than human data? Would synthetic data better protect patient privacy?

These five hypotheticals describe a variety of ways in which health information is collected, created, used, or disclosed in the context of AI. In the first four hypotheticals, traditional privacy, security, and breach notification issues are raised. The concern is that the use of AI in healthcare will increase the risk and magnitude of privacy and security breaches, leading to substantial informational injuries.[21] In the fifth hypothetical, the focus turns to the need for data sharing to realize AI's incredible potential to transform health care. The fifth hypothetical begs the question: What is the proper balance between supporting AI-powered health care tools on the one hand and protecting patient privacy and data security on the other? Using the HIPAA Privacy, Security, and Breach Notification Rules (HIPAA Rules) as an illustrative platform,[22] this Article provides a roadmap for analyzing the application of data privacy and security laws to health care scenarios involving AI. In so doing, this Article identifies: (1) significant gaps in privacy, security, and breach notification regulation in the context of AI-powered tools; (2) not insignificant hurdles that can interfere with data sharing and AI's goal of improving health care; and (3) major regulatory provisions that require clarification and/or amendment to respond to the rapid growth of AI in healthcare.

As background for this Article's focus on the HIPAA Rules, the privacy and security of health information collected, created, used, or disclosed in connection with AI is governed by a frustrating patchwork of federal and state laws.[23] Some privacy and security requirements are sourced in federal regulations (including the HIPAA Rules) that govern certain, but not all, health industry participants as well as certain persons who provide services to or on behalf of such

---

[21] *See* Jill McKeon, *Security, Privacy Risks of Artificial Intelligence in Healthcare*, HEALTH IT SEC. (Dec. 1, 2021), https://healthitsecurity.com/features/security-privacy-risks-of-artificial-intelligence-in-healthcare.

[22] *See* text accompanying *infra* notes 51, 56, and 64 (providing background information regarding the HIPAA Privacy, Security, and Breach Notification Rules, respectively).

[23] *See* Stacey A. Tovino, *Privacy for Student-Patients: A Call to Action*, 73 EMORY L.J. 83, 96–128 (2023) (summarizing and analyzing a large patchwork of federal and state data privacy and security laws).

participants.[24] Other privacy and security requirements are sourced in state professional practice acts that apply to licensed health professionals who practice in the state.[25] Still other privacy and security rules are sourced in state facility licensing laws that apply to certain, but not all, health care facilities that are located in the state.[26] Additional privacy rules are sourced in state medical record privacy laws, which are designed to extend federal-like protections to information not protected by federal law.[27] As of this writing, twenty states have new data protection laws that protect the privacy and security of certain, but not all, health information.[28] That said, the United States does not have one federal law that protects the privacy and security of all health information, including health information collected, created, used, or disclosed in connection with AI.[29] Although the application of all data protection laws to the use of AI in healthcare is beyond the scope of this Article, this Article does carefully apply the HIPAA Rules to health information collected, created, used, or disclosed in connection with a range of AI-powered tools. The regulatory gaps and information sharing hurdles identified by this Article under the HIPAA Rules can be used to guide similar analyses under other federal and state data privacy and security laws.[30]

This Article proceeds as follows: Part II briefly reviews the regulatory history of the HIPAA Rules and quickly summarizes limitations inherent in the Rules that restrict their application in the context of AI.[31] Part III examines a variety of health care hypotheticals that

---

24 *Infra* Part II.

25 Tovino, *supra* note 23, at 117–120 (analyzing state professional practice acts).

26 *Id.* at 120 (analyzing state facility licensure laws).

27 *Id.* at 120–21 (analyzing state medical record privacy laws).

28 *Id.* at 124–27 (analyzing new consumer data protection laws); F. Paul Pittman, *US Data Privacy Guide*, WHITE AND CASE (Dec. 26, 2023), https://www.whitecase.com/insight-our-thinking/us-data-privacy-guide (last visited Oct. 20, 2024) (Currently, [as of Oct. 20, 2024], a total of twenty states have passed comprehensive data privacy laws in the United States: California, Virginia, Colorado, Connecticut, Utah, Iowa, Indiana, Tennessee, Texas, Florida, Montana, Oregon, Delaware, New Hampshire, New Jersey, Kentucky, Nebraska, and Rhode Island. Of those twenty, California, Colorado, Connecticut, Virginia, Utah, Florida, Texas, and Oregon's laws are currently effective.).

29 McKeon, *supra* note 21.

30 *See* Tovino, *supra* note 23, at 110–28 (carefully examining these other federal and state laws).

31 *Infra* Part II.

involve the use of AI, identifying those persons and organizations who meet the definition of a HIPAA covered entity or business associate and those who do not.[32] Part III shows that not all health industry participants who use AI are regulated by the HIPAA Rules.[33] Part IV focuses on the information that is actually protected by the HIPAA Rules.[34] Some pieces of health information created, used, or disclosed as part of generative or predictive AI do fall within the definition of protected information but other pieces do not.[35]

Part V of this Article examines the HIPAA Privacy Rule's use and disclosure requirements, identifying the purposes for which PHI may be used or disclosed without the prior written authorization of the individual who is the subject of the information.[36] Even when a covered entity or business associate is involved in an AI scenario and is creating, using, or disclosing PHI, the individual who is the subject of that PHI is not always required to authorize the creation, use, or disclosure of their PHI.[37] Illustrative examples include the use of AI to summarize patient encounters, the use of AI to create discharge summaries, the use of AI to accept or reject health insurance claims, the use of AI to support quality assurance, outcomes evaluation, utilization review, and the disclosure of allegedly de-identified information to technology companies to support their AI initiatives.[38]

Part VI of this Article focuses on the five individual rights set forth in the HIPAA Privacy Rule.[39] The use of AI in healthcare raises novel and interesting issues regarding these rights. For example, must patients be notified through a covered entity's notice of privacy practices

---

32 *Infra* Part III.

33 *Infra* Part III.

34 *Infra* Part IV.

35 *Infra* Part IV.

36 *Infra* Part V.

37 *Infra* Part V.

38 *See, e.g.*, Jean Feng et al., *Clinical artificial intelligence quality improvement: towards continual monitoring and updating of AI algorithms in healthcare*, 5 DIGITAL MED. 66 (2022) (explaining how machine learning and artificial intelligence have the potential to derive insights from clinical data and improve patient outcomes, thus supporting quality assurance activities); Michelle S. Lee et al., *The Impact of Artificial Intelligence on Quality and Safety*, 10 GLOBAL SPINE J. 99S (2020) (same).

39 *Infra* Part VI.

that AI is used in connection with the collection, creation, use, or disclosure of their PHI?[40] Do patients have the right to request their covered entities not to share their information with AI-powered tools?[41] If so, are covered entities required to comply with these requests?[42] Do patients have the right to access their AI-created clinical notes and discharge summaries? Do patients have the right to amend subtle inaccuracies in AI-generated medical record documentation?[43] Finally, Part VII reviews the HIPAA Breach Notification Rule, with a focus on words and phrases therein that will be implicated by AI-involved hypotheticals.[44] A conclusion re-emphasizes the existence of other federal and state data protection laws and the need to evaluate these laws in the context of health information that is collected, created, used, or disclosed in connection with AI.

II. REGULATORY HISTORY OF THE HIPAA RULES

The HIPAA Rules are widely known as providing a national floor of data privacy, security, and breach notification protections for all individually identifiable health information.[45] Some brief background information is necessary to show why this is not always true in the context of health information collected, created, used, or disclosed in the context of predictive or generative AI.[46]

---

40 *Infra* Part VI.

41 *Infra* Part VI.

42 *Infra* Part VI.

43 *Infra* Part VI.

44 *Infra* Part VII.

45 *See, e.g.*, *Frequently-Asked Question No. 399, Does the HIPAA Privacy Rule Preempt State Laws?*, U.S. DEP'T HEALTH & HUMAN SERVS., https://www.hhs.gov/hipaa/for-professionals/faq/399/does-hipaa-preempt-state-laws/index.html (last visited Feb. 5, 2023) ("The HIPAA Privacy Rule provides a Federal floor of privacy protections for individuals' individually identifiable health information where that information is held by a covered entity or by a business associate of the covered entity.").

46 *See* Yana Khare, *Generative AI vs. Predictive AI: What is the Difference?* ANALYTICS VIDHYA (Sept. 26, 2023), https://www.analyticsvidhya.com/blog/2023/09/generative-ai-vs-predictive-ai/ ("While predictive AI uses previous data to make predictions, generative AI generates new data.").

President Clinton signed the Health Insurance Portability and Accountability Act (HIPAA) into law on August 21, 1996.[47] Section 264 of HIPAA directed the Secretary of the Department of Health and Human Services (HHS) to promulgate data privacy regulations if Congress failed to enact privacy legislation within three years of HIPAA's date of enactment.[48] When Congress missed its three-year legislative deadline, HHS incurred the obligation to promulgate privacy regulations.[49] These regulations, known as the HIPAA Privacy Rule, require covered entities and business associates to: (1) adhere to certain use and disclosure requirements with respect to protected health information (PHI);[50] (2) provide individuals with certain rights relating to their PHI; and (3) comply with certain administrative requirements.[51] As discussed in more detail in Part III below, the HIPAA Privacy only applies to covered entities and business associates, leaving many health information collectors, creators, users, and disclosers (including those involved in predictive and generative AI) unregulated.[52] In addition, the Privacy Rule only protects the confidentiality of

---

47 *See* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191 (Aug. 21, 1996) [hereinafter HIPAA].

48 *Id.* at § 264(c)(1).

49 *Id.*

50 *See infra* Part IV (defining protected health information (PHI)).

51 The HIPAA Privacy Rule, codified at 45 C.F.R. §§ 164.501-.534., was created through a series of proposed and final rules promulgated by HHS between 1999 and the present. *See, e.g.,* Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59918 (proposed Nov. 3, 1999) (to be codified at 45 C.F.R. pts. 160–64); Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82462 (Dec. 28, 2000) (to be codified at 45 C.F.R. pts. 160, 164); Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 14776 (proposed Mar. 27, 2002) (to be codified at 45 C.F.R. pts. 160, 164); Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53182 (Aug. 14, 2002) (codified at 45 C.F.R. pts. 160, 164); Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act, 75 Fed. Reg. 40868 (proposed July 14, 2010) (to be codified at 45 C.F.R. pts. 160, 164); Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5566, 5688 (Jan. 25, 2013) (codified at 45 C.F.R. pgs. 160, 164) [hereinafter Final HITECH Rules].

52 *Infra* Part III.

information falling within the definition of PHI, leaving some information collected, created, used, or disclosed in the context of AI unprotected.[53]

In addition to Section 264 of HIPAA, which directed HHS to adopt privacy regulations, Section 262 of HIPAA directed HHS to promulgate information security regulations.[54] These regulations, known as the HIPAA Security Rule, require covered entities and business associates to: (1) ensure the confidentiality, integrity, and availability of all electronic protected health information (ePHI)[55] the covered entity or business associate creates, receives, maintains, or transmits; (2) protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI; (3) protect against any reasonably anticipated uses or disclosures of ePHI that are not permitted or required under the HIPAA Privacy Rule; and (4) ensure compliance with the HIPAA Security Rule by their workforce members.[56] As with the HIPAA Privacy Rule, the HIPAA Security Rule only applies to covered entities and business associates, leaving many health information collectors, creators, users, and disclosers (including those involved in predictive and generative AI) unregulated.[57] In addition, the Rule only protects the confidentiality, integrity, and availability of ePHI—but not information falling outside that definition—leaving many pieces of individually identifiable health information unprotected.[58]

---

53 *Infra* Part IV.

54 HIPAA, *supra* note 47, at § 262.

55 *See infra* Part IV (defining electronic protected health information (ePHI)).

56 The HIPAA Security Rule, codified at 45 C.F.R. §§ 164.302–.318, was created through a series of proposed and final rules promulgated by HHS between 1998 and the present. *See, e.g.*, Security and Electronic Signature Standards; Proposed Rule, 63 Fed. Reg. 43242 (proposed Aug. 12, 1998) (to be codified at 45 C.F.R. pt. 142); Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334 (Feb. 20, 2003) (to be codified at 45 C.F.R. pts. 160, 162, and 164); Office for Civil Rights: Delegation of Authority, 74 Fed. Reg. 38630 (Aug. 4, 2009); Modifications to the HIPAA Privacy, Security, and Enforcement Rules under the Health Information Technology for Economic and Clinical Health Act, 75 Fed. Reg. 40868 (July 14, 2010) (to be codified at 45 C.F.R. pts. 160 and 164); Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5566 (Jan. 25, 2013) (to be codified at 45 C.F.R. pts 160 and 164).

57 *Infra* Part III.

58 *Infra* Part IV.

President Obama signed the American Recovery and Reinvestment Act (ARRA) into law on February 17, 2009.[59] Section 13402 of the Health Information Technology for Economic and Clinical Health Act (HITECH), codified at Division A, Title XIII of ARRA,[60] required covered entities and business associates, following the discovery of a breach of unsecured PHI (uPHI),[61] to notify certain parties.[62] Section 13402 of HITECH also directed the Secretary to promulgate regulations implementing these breach notification requirements.[63] These regulations, known as the HIPAA Breach Notification Rule,[64] require covered entities to notify individuals and certain media outlets, as well as the Secretary of HHS, in the event of certain breaches of uPHI.[65] Following the discovery of a breach of uPHI, business associates also have the obligation to notify the covered entities with whom they work of a breach.[66] Like the HIPAA Privacy and Security Rules, however, the HIPAA Breach Notification Rule only imposes notification obligations on covered entities and business associates, leaving many health information collectors, creators, users, and disclosers (including those who employ AI-powered tools) without notification obligations in the event of a breach.[67] Moreover, the HIPAA Breach Notification Rule

---

59 American Recovery and Reinvestment Act, Pub. L. 111-5 (Feb. 17, 2009) [hereinafter ARRA].

60 Health Information Technology for Economic and Clinical Health Act, codified at ARRA, §§ 13001–13424 [hereinafter HITECH].

61 *See infra* Part IV (defining unsecured protected health information (uPHI)).

62 HITECH, *supra* note 60, at § 13402(a), (b).

63 *Id.* § 13402(j).

64 The HIPAA Breach Notification Rule, codified at 45 C.F.R. §§ 164.400–.414, was created through a series of requests for information, interim final rules, and final rules promulgated by HHS between 2009 and present. *See, e.g.*, Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements Under Section 13402 of Title XIII (Health Information Technology for Economic and Clinical Health Act) of the American Recovery and Reinvestment Act of 2009; Request for Information, 74 Fed. Reg. 19006 (Apr. 17, 2009); Breach Notification for Unsecured Protected Health Information, 74 Fed. Reg. 42740 (Aug. 24, 2009); Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5566 (Jan. 25, 2013).

65 45 C.F.R. §164.404.

66 *Id.* at § 164.410.

67 *Infra* Part III.

only applies to breaches involving uPHI, further limiting the number of situations in which notification obligations apply.[68] Taken together, these limitations in the HIPAA Rules described in this Part II create relatively large gaps in protection for information collected, created, used, or disclosed in connection with AI. Each of these gaps is explored in more detail below.

III. COVERED ENTITIES AND BUSINESS ASSOCIATES

As currently written, the HIPAA Rules only regulate covered entities[69] and business associates.[70] Covered entities include health plans,[71] health care clearinghouses,[72] and certain health care providers[73] (i.e., those health care providers that transmit health information in electronic form in connection with certain standard transactions).[74] Health care providers, the most common type of covered entity, are defined to include persons and organizations that furnish, bill, or get paid for "health care" in the normal course of business.[75] "Health care" is defined to include "care, services, or supplies related to the health of an individual" (including "[p]reventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care") as well as the "[s]ale or dispensing of a drug, device, equipment, or other item in accordance with a prescription."[76] Examples of health care providers include, but certainly are not limited to, physicians, psychologists, pharmacists, physician assistants, nurse practitioners, social workers, marriage and family therapists, licensed independent counselors, hospitals, clinics,

---

68 45 C.F.R. § 164.404 (individual notification); 45 C.F.R. §164.406 (media outlet notification); 45 C.F.R. §164.408 (Secretary of HHS notification).

69 45 C.F.R. § 160.103 (defining covered entity); 45 C.F.R. § 160.102(a) (applying the HIPAA Rules to covered entities).

70 45 C.F.R. § 160.103 (defining business associate); 45 C.F.R. § 160.102(b) (applying the HIPAA Rules to business associates).

71 45 C.F.R. § 160.103 (defining health plan).

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

73 *Id.* (defining health care provider).

74 *Id.* (defining covered entity).

75 *Id.* (defining health care provider).

76 *Id.* (defining health care).

nursing homes, rehabilitation facilities, home health agencies, hospices, pharmacies, and durable medical equipment suppliers.[77]

Health care providers are regulated by the HIPAA Privacy Rule if they transmit health information in electronic form in connection with a standard transaction.[78] The most common standard transaction is the health insurance claim transaction.[79] A health care provider who takes any form of insurance (public or private) and who bills insurance electronically on behalf of even one patient (and not necessarily a patient who might later claim a privacy violation) will be a covered entity for all of its patients.[80] Because most health care providers accept insurance and bill insurance electronically, most providers are covered entities who must comply with the HIPAA Rules.[81] That said, not all health care providers are covered entities.[82] For example, providers who have cash or credit-only practices and who do not accept or bill insurance for any of their patients can escape regulation.[83]

Health plans, the second most common type of covered entity, include individual and group health plans.[84] Illustrative examples of health plans include health insurance issuers; health maintenance organizations (HMOs); Medicare Parts A, B, C, and D; State Medicaid Programs; the Children's Health Insurance Program; the Indian Health Service; the Federal Employees Health Benefits Program; a high risk pool established under state law to provide health insurance

---

77 Sections 1861(u) & 1861(s) of the Social Security Act, 42 U.S.C. 1395; 45 C.F.R. § 160.103.

78 45 C.F.R. § 160.103 (defining covered entity to include only those health care providers who "transmit[] any health information in electronic form in connection with a [standard] transaction").

79 *Id.* (defining transaction to include health care claims).

80 *See id.*

81 *See infra* Part IV. (HIPAA covered entities also must comply with the HIPAA Security Rule with respect to their electronic protected health information (ePHI) and the HIPAA Breach Notification Rule with respect to their unprotected health information (uPHI).)

82 45 C.F.R. § 160.103.

83 Steve Adler, *The HIPPA Definition of Covered Entities Explained*, THE HIPPA J. (Jan. 1, 2023), https://www.hipaajournal.com/hipaa-definition-covered-entities/.

84 45 C.F.R. § 160.103 (defining group health plan). A group health plan is defined as an employee welfare benefit plan, including insured and self-insured plans, to the extent that the plan provides medical care to employees or their dependents directly or through insurance, reimbursement, or otherwise, that: (1) has 50 or more participants; or (2) is administered by an entity other than the employer that established and maintains the plan.

coverage to eligible individuals; and any other individual or group plan, or combination of individual or group plans that provides or pays for the cost of medical care.[85] Health care clearinghouses, the least common type of covered entity, are public or private entities, including billing services, repricing companies, community health management information systems, and value-added networks and switches, that do either of the following: (1) process or facilitate the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction; or (2) receive a standard transaction from another entity and process or facilitate the processing of health information into nonstandard format or nonstandard data content for the receiving entity.[86]

Post-HITECH, the HIPAA Rules also apply directly to business associates.[87] Business associates are defined as persons who: (1) on behalf of a covered entity but other than in the capacity of a member of the workforce of a covered entity, create, receive, maintain, or transmit PHI for a function or activity regulated by the HIPAA Rules, including claims processing or administration; data analysis, processing, or administration; utilization review; quality assurance; patient safety activities; billing; benefit management; practice management; repricing; or (2) provide, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for the covered entity if the provision of the service involves the disclosure of PHI from the covered entity to the person.[88]

The use of predictive and generative AI in the health care industry raises new questions regarding the application of the HIPAA Rules. For example, many individuals enjoy using AI-driven symptom checkers, which are tools that allow users to select or manually enter symptoms and receive a list of possible causes of those symptoms.[89]

---

85 *Id.* (defining health plan).

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

87 *See* HITECH, *supra* note 60, at §§ 13401, 13404 (applying the HIPAA Security Rule and the HIPAA Privacy Rule to business associates).

88 45 C.F.R. § 160.103 (defining business associate).

89 *See Symptom Checker*, *supra* note 5; *see Symptom Checker*, *supra* note 6; *see Symptom Checker*, *supra* note 7.

Whether a symptom checker is regulated by the HIPAA Rules depends on whether the operator of the symptom checker is a covered entity or business associate. For example, Sutter Health, the Mayo Clinic, and Cedars-Sinai all operate symptom checkers, some of which are fueled by AI.[90] Because Sutter Health, Mayo Clinic, and Cedars Sinai take insurance and bill insurance electronically, any protected information entered into their symptom checkers would be protected by the HIPAA Rules.[91]

Ubie Health (Ubie) also offers an AI-fueled symptom checker that is available to the general public. After users enter their biological sex, age, and symptoms, Ubie offers possible "causes" of those symptoms.[92] Regardless of whether one could argue that these "causes" are "diagnoses" (and, thus, regardless of whether one could argue that Ubie is providing diagnostic care for purposes of HIPAA's definition of a health care provider[93]), Ubie offers these "causes" for free and does not accept and bill insurance electronically. As a result, Ubie is not a covered health care provider for purposes of the HIPAA Rules.[94] Because Ubie is also not a health plan, health care clearinghouse, or business associate,[95] Ubie is not regulated by the HIPAA Rules at all.[96] This means that any information entered into Ubie by a user would not be protected by the HIPAA Rules[97]—even if that information is identical

---

90 *Symptom Checker*, MAYO CLINIC, https://www.mayoclinic.org/symptom-checker/select-symptom/itt-20009075 (last visited Dec. 26, 2023); *Medical Symptom Checker*, SUTTER HEALTH, https://www.sutterhealth.org/health/symptom-checker (last visited Dec. 26, 2023); *Symptom Checker*, CEDARS-SINAI, https://www.cedars-sinai.org/health-library/symptom-checker.html#!/start (last visited Feb. 22, 2023).

91 *See Billing and Insurance*, SUTTER HEALTH, https://www.sutterhealth.org/for-patients/billing-insurance (last visited Jan. 17, 2024); *Insurance and Billing*, MAYO CLINIC, https://www.mayoclinic.org/patient-visitor-guide/billing-insurance (last visited Jan. 17, 2024); *Billing*, CEDARS SINAI, https://www.cedars-sinai.org/billing-insurance/billing.html (last visited Jan. 17, 2024).

92 *Symptom Checker*, UBIE HEALTH, https://ubiehealth.com (last visited Dec. 26, 2023).

93 *See supra* notes 73, at 77, 75–76 and accompanying text (explaining that "health care providers" are defined as persons and organizations that furnish, bill, or get paid for "health care" in the normal course of business; further explaining that "health care" is defined to include "diagnostic" care).

94 *See* 45 C.F.R § 160.103.

95 *See id.*

96 *See* Adler, *supra* note 83.

97 *See* Adler, *supra* note 83.

to the information users enter into the symptom checkers operated by Sutter Health, Mayo Clinic, or Cedars-Sinai.

The same is true of Everyday Health, which offers a symptom checker that is described as a "preliminary diagnosis and triage tool . . . that leverages artificial intelligence . . . to assess more than 1,500 symptoms and 800 conditions."[98] Regardless of whether one could argue that these "preliminary diagnosis and triage" services are true "diagnostic" services (and, thus, regardless of whether one could argue that Everyday Health is providing diagnostic care for purposes of HIPAA's definition of a health care provider[99]), Everyday Health offers its AI-leveraged tool for free and does not accept and bill insurance electronically. As a result, Everyday Health is not a covered health care provider for purposes of the HIPAA Rules.[100] Because Everyday Health also is not a health plan, health care clearinghouse, or business associate, Everyday Health is not regulated by the HIPAA Rules.[101] Again, this is so even though users enter information into Everyday Health's symptom checker that is identical to the information users enter into the symptom checkers of Sutter Health, Mayo Clinic, or Cedars Sinai, which are regulated by the HIPAA Rules.

Many individuals also take advantage of medical chatbots, which are software applications that use AI to conduct online chat conversations via text or text-to-speech in lieu of providing direct contact with a live person.[102] Whether a medical chatbot's collection, creation, use, or disclosure of protected information is regulated by the HIPAA Rules depends, again, on whether the chatbot operator is a covered entity or business associate. For example, New York's Northwell Health System recently rolled out an AI-driven medical chatbot called

---

98 *How Does Symptom Checker Work*, EVERYDAY HEALTH, https://www.everydayhealth.com/symptom-checker/#:~:text=How%20Does%20Symptom%20Checker%20Work,1%2C500%20symptoms%20and%20800%20conditions (last visited Dec. 26, 2023).

99 *See supra* notes 73, 77, 93.

100 *See* 45 C.F.R. § 160.103.

101 *See* Adler, *supra* note 83, at 71–76 (explaining that covered entities include health plans, health care clearinghouses, and only certain health care providers; that is, those that transmit health information in electronic form in connection with a standard transaction).

102 *See* Sara Reardon, *AI Chatbots Can Diagnose Medical Conditions at Home. How Good are They?*, SCI. AM. (Mar. 31, 2023), https://www.scientificamerican.com/article/ai-chatbots-can-diagnose-medical-conditions-at-home-how-good-are-they/.

Northwell Health Pregnancy Chats to obstetrics practices throughout its system.[103] Because Northwell Health's obstetrics practices accept and electronically bill health insurance,[104] the HIPAA Rules would protect any individually identifiable health information collected, created, used, or disclosed by the chatbot. For example, if protected information collected by Northwell's chatbot somehow ended up on social media, including Facebook, Instagram, or Twitter without the patient's authorization, the HIPAA Privacy Rule (and likely the HIPAA Security Rule) will have been violated and Northwell Health could be subject to government-imposed civil and criminal penalties. Along the same lines, if Northwell Health experienced a breach of uPHI that included information collected or created by the chatbot, Northwell Health would be obligated to notify the individuals whose uPHI was breached as required by the HIPAA Breach Notification Rule.[105]

AI also has been used to help interpret static, machine-generated, medical images, such as radiographs and electrocardiograms, as well as pathology specimens.[106] Whether health information collected, created, used, or disclosed in connection with AI-assisted diagnostics is regulated by the HIPAA Rules depends, yet again, on whether the individual or entity that is receiving the diagnostic assistance from AI is a HIPAA covered entity. For example, if a radiologist who accepts and electronically bills health insurance uses an AI-assisted tool to help diagnose pneumonia from a radiograph,[107] then the use or disclosure of

---

103 *Northwell Releases AI-Driven Pregnancy Chatbot*, NORTHWELL HEALTH, https://www.northwell.edu/news/the-latest/northwell-releases-ai-driven-pregnancy-chatbot (last visited Jan. 1, 2024).

104 *Protecting Patient Privacy*, NORTHWELL HEALTH, https://www.northwell.edu/about-northwell/commitment-to-excellence/protecting-patient-privacy (last visited Jan. 1, 2024) ("Q: Is Northwell Health required to comply with HIPAA? A: Yes.").

105 *See* 45 C.F.R. § 164.404 (individual notification).

106 *See, e.g.*, Pranav Rajpurkar & Matthew P. Lungren, *The Current and Future State of AI Interpretation of Medical Images*, 388 NEW ENG. J. MED. 1981 (2023) (examining the advantages and limitations of current clinical radiologic AI systems); Charlotte J. Haug & Jeffrey M. Drazen, *Artificial Intelligence and Machine Learning in Clinical Medicine*, 388 NEW ENG. J. MED. 1201 (2023) (describing the history of AI in medicine, including the use of AI for clinical diagnostics).

107 *See, e.g.*, John R. Zech et al., *Variable Generalization Performance of a Deep Learning Model to Detect Pneumonia in Chest Radiographs: A Cross-Sectional Study*, 15 PLOS MEDICINE e1002683 (2018) (finding that pneumonia-screening convolutional neural networks achieved better internal than external performance in 3 out of 5 natural comparisons).

any protected information evaluated by (or any results that include protected information that are generated by) the AI tool would be regulated by the HIPAA Rules. On the other hand, if a physician does not accept and bill insurance electronically and obtains diagnostic assistance from an AI-powered tool, then the information evaluated by (or the results generated by) the tool would not be protected by the HIPAA Rules.

Digital phenotyping, which is the moment-by-moment quantification of individual-level human phenotype *in situ*, using data from personal digital devices,[108] also raises interesting HIPAA Rules application questions. One illustrative, AI-powered, phenotyping platform (PhenOM) uses its affiliated company's (OM1's) repository of linked electronic medical records, claims records, and other data covering more than 300 million patients to identify unique digital phenotypes associated with conditions and outcomes.[109] PhenOM's goals include finding patients with rare, undiagnosed, or misdiagnosed conditions; personalizing treatment recommendations; and predicting the risk of specific outcomes.[110] As with the examples discussed above, whether PhenOM must comply with the HIPAA Rules depends on whether OM1 is a covered entity or a business associate. A brief review of OM1's website reveals that OM1 is not a covered entity.[111] OM1 is simply the builder of a real-world cloud that claims to enable healthcare stakeholders to cost-effectively access, analyze, and use outcomes data in a more robust, clinically meaningful, and precise way.[112] Although these stakeholders may meet the definition of a covered provider, plan, or clearinghouse, OM1 does not. That said, OM1 could be a business associate if OM1, on behalf of a covered entity, creates, receives, maintains, or transmits PHI for a function or activity regulated by the HIPAA Rules. OM1 could also be a business associate if it

---

108 *See* Jyoti Prakash et al., *Digital Phenotyping in Psychiatry: When Mental Health Goes Binary*, 30 IND. PSYCHIATRY J. 191 (2021) (defining digital phenotyping).

109 *See Harness AI-Powered Digital Phenotyping for Actionable Insights with PhenOM™*, OM1, https://www.om1.com/solutions/phenom/ (last visited Dec. 26, 2023).

110 *See Creating Digital Phenotypical Fingerprints*, OM1, https://www.om1.com/solutions/phenom/ (last visited Dec. 26, 2023).

111 *See* OM1, https://www.om1.com/ (last visited Jan. 17, 2024).

112 *See Outcomes Management*, OM1 https://www.om1.com/solutions-2/healthcare-providers/clinical-outcomes-measurement/ (last visited Mar.19, 2024).

provides data aggregation or certain other enumerated services to or for a covered entity and the provision of such services involves the disclosure of PHI from the covered entity to OM1.[113] Remember that, post-HITECH, business associates are directly regulated by the HIPAA Rules and can be subject to government-imposed civil and criminal penalties for violations of the HIPAA Rules.[114]

In addition to AI-powered symptom checkers, medical chatbots, and diagnostic tools, AI also has the ability to function as a health care scribe, including by "listening" to clinician-patient encounters and "writing" notes summarizing those encounters.[115] An illustrative example involves Epic, an electronic medical record (EMR) software company, which recently partnered with Nuance Communications (Nuance), Microsoft's speech recognition subsidiary. Through their partnership, Epic and Nuance offer the Dragon Ambient eXperience Express (DAX Express) tool, which uses OpenAI's GPT-4 to listen to patient encounters and write EMR notes automatically from those encounters, regardless of whether those encounters take place in an in-person or virtual examination room.[116] To the extent a health care provider (including one who uses DAX Express) accepts and bills insurance electronically, the health care provider will meet the definition of a covered entity and must comply with the HIPAA Rules.[117] DAX

---

113 *See Privacy Policy*, OM1 (2017), https://www.om1.com/privacy/. It appears from OM1's website that OM1 provides data to stakeholders that could include covered entities, not the other way around as is required by the definition of a business associate, although this point is unclear.

114 *See* HITECH, *supra* notes 60, 87.

115 *See Nuance and Epic Expand Ambient Documentation Integration Across the Clinical Experience with DAX Express for Epic*, NUANCE (June 27, 2023), https://news.nuance.com/2023-06-27-Nuance-and-Epic-Expand-Ambient-Documentation-Integration-Across-the-Clinical-Experience-with-DAX-Express-for-Epic (reporting that providers who use DAX Express "will be able to create draft clinical notes automatically and securely from the exam room or via a telehealth encounter for immediate clinical review and completion after each patient visit" and that, "DAX Express is the next milestone in Nuance's long-standing mission to reduce administrative burden and empower clinicians to spend more time taking care of patients and less time on paperwork.").

116 *See* Hannah Nelson, *Epic Announces Ambient Clinical Documentation EHR Integration*, TECHTARGET (June 27, 2023), https://ehrintelligence.com/features/epic-taps-ambient-intelligence-to-streamline-clinical-documentation (stating that clinicians who use DAX Express report saving seven minutes per patient encounter, improving work-life balance and reducing clinical burnout).

117 45 C.F.R. § 160.103 (defining covered entity).

Express does not meet the definition of a covered entity because it is neither a health care provider, health plan, nor health care clearinghouse.[118] That said, any covered health care provider that shares PHI with DAX Express, or that allows DAX Express to create PHI on its behalf for a purpose listed in the definition of a business associate,[119] must enter into a business associate (BA) agreement (BAA) with DAX Express.[120] Importantly, the BAA must be executed before the provider allows DAX Express to listen to the provider's conversations and to draft medical record entries on the provider's behalf.[121] As a result of the BAA, DAX Express will have a contractual obligation to protect the confidentiality of the PHI created on behalf of, or received from, the provider. If DAX Express violates these obligations, it could be liable to the provider for breach of contract. In addition, and post-HITECH, DAX Express also is directly regulated by the HIPAA Rules.[122] This means that if DAX Express violates one or more of the HIPAA Rules, DAX Express could be subject to civil and criminal penalties imposed by the federal government.

What if an AI-powered tool does not simply assist a human provider, as in the examples described above, but independently stands in place of the human provider? In the context of mental health care, for example, could a chatbot that behaves like a human therapist—by asking questions of and providing insights to patients during an online session—be regulated by the HIPAA Rules? Currently, the HIPAA Rules define a "health care provider" as a person or organization who

---

118 *Id.*; *Fully Automated Clinical Documentation*, TOTAL VOICE TECHS., https://www.totalvoicetech.com/dax-copilot/?matchtype=e&network=o&device=c&utm_term=dax%20express&utm_campaign=search&utm_source=bing&utm_medium=ppc&utm_content=&hsa_acc=7851708905&hsa_cam=20718344863&hsa_grp=1231454035877382&hsa_ad=&hsa_src=o&hsa_tgt=kwd-76966149474445:loc-4126&hsa_kw=dax%20express&hsa_mt=e&hsa_net=adwords&hsa_ver=3&msclkid=9f4b4bbcf1ed184a14272e14d52d9ed5 (last visited Jan. 17, 2024).

119 *See supra* note 88 and accompanying text.

120 *See* 45 C.F.R. § 164.502(e)(1)(i) ("A covered entity may disclose protected health information to a business associate and may allow a business associate to create, receive, maintain, or transmit protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information."); *see also id.* §164.502(e)(2) ("The[se] satisfactory assurances . . . must be documented through a [HIPAA-compliant business associate agreement].").

121 *See* 45 C.F.R. § 164.502(e)(1)–(2).

122 *See* text accompanying *supra* note 88.

furnishes, bills, or gets paid for "health care" in the normal course of business.[123] "Health care" is further defined to include "counseling," including counseling relating to a "mental health condition."[124] It is not a stretch to say that a therapy chatbot could technically meet this definition. Rosebud, for example, describes itself as an AI-powered tool for personal growth and mental health that, among other capabilities, helps users reframe negative thoughts.[125] Users of Rosebud enter text into an "online journal" and then Rosebud not only responds but offers actionable insights that are designed to improve users' mental health.[126] It is unclear whether the HIPAA definition of a "health care provider" (first finalized by HHS more than twenty-four years ago, in December 2000) could be interpreted to capture AI-powered, non-human chatbots such as Rosebud. Regardless, Rosebud's services are provided free of charge and Rosebud does not accept or bill insurance electronically.[127] As such, Rosebud could not be a covered health care provider under the current HIPAA Rules.[128] That said, if public or private health insurers reimbursed Rosebud for its therapy services and Rosebud electronically submitted claims for such reimbursement, the answer could be different.

The covered entity and business associate examples discussed above all involve the use of AI in the *provision* of health care. AI also can be used in *paying* for health care; that is, in health insurance. For example, health insurers have used AI (including faulty AI) to approve and deny claims and to streamline initial and subsequent insurance coverage denials.[129] In one example, insurer UnitedHealth was

---

123 *See* 45 C.F.R. § 160.103 (defining health care provider).

124 *See id.* (defining health care).

125 *See Welcome to Rosebud,* ROSEBUD, https://my.rosebud.app/?utm_source=google&utm_medium=&utm_campaign=performance-max&utm_content=&utm_term=&gad_source=1&gclid=Cj0KCQiA1rSsBhDHARIsANB4EJbRoOIf-ACyU-sElvIdlZBJ10a-Ge7WX0V6ZvyXQIU-sxwCwD4dlYaAuFkEALw_wcB (last visited Dec. 28, 2023).

126 *See id.*

127 *See id.*

128 *See* text accompanying *supra* notes 78–81.

129 *See, e.g.*, Elizabeth Napolitano, *UnitedHealth Uses Faulty AI to Deny Elderly Patients Necessary Coverage, Lawsuit Claims*, CBS NEWS (Nov. 20, 2023), https://www.cbsnews.com/news/unitedhealth-lawsuit-ai-deny-claims-medicare-

accused of using an AI model developed by NaviHealth called "nH Predict" to "prematurely and in bad faith discontinue payment" to its elderly beneficiaries, causing them medical or financial hardships.[130] Whether the elderly beneficiaries' information is protected by the HIPAA Rules depends, again on whether the health insurer (in this case, UnitedHealth) falls within the definition of a covered entity or business associate.[131] Because UnitedHealth pays for the cost of medical care,[132] UnitedHealth falls within the definition of a covered health plan. As discussed in more detail below in Part V, however, the HIPAA Rules do not forbid UnitedHealth Group from using AI-powered tools to analyze members' protected information to make claims determinations, including coverage denials.[133] Indeed, the HIPAA Privacy Rule expressly authorizes UnitedHealth and other health plans to use and disclose PHI for "payment" activities (defined to include "coverage . . . determinations" and "review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges")[134] without the patient's prior written authorization.[135] That said, authorities outside the HIPAA Privacy Rule regulate insurers' use of AI in coverage determinations.

advantage-health-insurance-denials/ (reporting that, "The families of two now-deceased former beneficiaries of UnitedHealth have filed a lawsuit against the health care giant, alleging it knowingly used a faulty artificial intelligence algorithm to deny elderly patients coverage for extended care deemed necessary by their doctors.").

130 *See* Plaintiffs' Class Action Complaint at 3, ¶5, Lokken v. UnitedHealth Group, No. 0:23-CV-03514 (D. Minn. Nov. 14, 2023). "This putative class action arises from Defendants' illegal deployment of artificial intelligence (AI) in place of real medical professionals to wrongfully deny elderly patients care owed to them under Medicare Advantage Plans by overriding their treating physicians' determinations as to medically necessary care based on an AI model that Defendants know has a 90% error rate." *Id.* at 1, ¶1.

131 45 C.F.R. § 160.103 (defining covered entity); *id.* § 160.102(a) (applying the HIPAA Rules to covered entities).

132 *See supra* notes 84–85 and accompanying text (defining health plan).

133 *See infra* note 215.

134 *See* 45 C.F.R. § 164.501 (defining payment to include these activities).

135 *See id.* § 164.506(a), (c)(1) (allowing covered entities to use and disclose a patient's PHI for payment activities without the patient's prior written authorization).

IV. PROTECTED INFORMATION: PHI, EPHI, AND UPHI

Once a determination has been made that a hypothetical involves a HIPAA covered entity or business associate, the next step is to determine whether the information the covered entity or business associate is using or disclosing in connection with AI is protected by the HIPAA Rules. The HIPAA Rules are a bit confusing in that each Rule protects a different class of information. The HIPAA Privacy Rule regulates covered entities and business associates with respect to their uses and disclosures of protected health information (PHI)[136] whereas the HIPAA Security Rule regulates covered entities and business associates with respect to their electronic protected health information (ePHI).[137] In addition, the HIPAA Breach Notification Rule regulates covered entities and business associates with respect to breaches of unsecured protected health information (uPHI).[138] Health information collected, created, used, or disclosed in connection with AI must fall into the definition of PHI, ePHI, or uPHI to be protected by the HIPAA Privacy, Security, and Breach Notification Rules, respectively.[139]

A. PHI

Because the definitions of ePHI and uPHI are based on the definition of PHI,[140] PHI will be our starting point. PHI is generally defined as individually identifiable health information (IIHI).[141] In turn, IIHI is defined as information that: (1) "[i]s created or received by a health

---

136 *See id.* § 164.500(a) ("Except as otherwise provided herein, the [HIPAA Privacy Rule] appl[ies] to covered entities with respect to protected health information.").

137 *See id.* § 164.302 ("A covered entity or business associate must comply with the [HIPAA Security Rule] with respect to electronic protected health information of a covered entity.").

138 *See id.* § 164.404(a)(1) ("A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach.").

139 *See id.* § 160.103.

140 *See id.* (defining ePHI as "information that comes within paragraphs (1)(i) or (1)(ii) of the definition of protected health information"); *see also id.* § 164.402 (defining uPHI as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary . . . ").

141 *Id.* § 160.103 (defining protected health information).

care provider, health plan, employer, or health care clearinghouse"; and (2) "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual"; and that either (i) "identifies the individual"; or (ii) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual."[142] Health information created or received by a traditional covered health care provider, such as a physician or hospital, that identifies a patient and relates to the patient's physical or mental health, will typically meet this definition.[143] A classic example of PHI is a patient's identifiable paper or electronic medical record. The record will contain the patient's name (meeting the individually identifiable prong of the definition) as well as physical or mental health information about the patient (thus meeting the health-related prong of the definition).[144]

B. ePHI

PHI becomes ePHI protected by the Security Rule if the PHI is transmitted by electronic media or maintained in electronic media.[145] Thus, a patient's old-fashioned, paper medical record that is not digitized and transmitted by electronic media is PHI but not ePHI. However, a patient's electronic medical record would be both PHI (protected by the Privacy Rule) and ePHI (protected by the Security Rule). Likewise, individually identifiable health information entered by a patient into an online symptom checker or medical chatbot would be both PHI and ePHI. Individually identifiable health information created by ChatGPT about a patient and included in the patient's medical record also would meet the definition of PHI and ePHI.

C. uPHI

PHI becomes uPHI protected by the Breach Notification Rule if it is not rendered unusable, unreadable, or indecipherable to

---

142 *Id.* § 160.103 (defining individually identifiable health information).

143 *See infra* Part IV(F) (explaining the four classes of individually identifiable health information that are excepted from the definition).

144 *See infra* Part IV(F).

145 45 C.F.R. § 160.103 (defining ePHI).

unauthorized persons through the use of certain HHS-approved methodologies or technologies.[146] These methodologies and technologies include the shredding or destruction of paper PHI; the clearing, purging, or destruction of electronic media; and the encryption of electronic PHI.[147] For example, a covered physician who maintains a copy of a patient's unencrypted electronic medical record on their non-password-protected laptop would be in possession of uPHI. If that uPHI is breached,[148] the physician would incur notification obligations.

D. De-Identified Information

That said, health information that does not identify an individual and with respect to which there is no reasonable basis to believe can be used to identify an individual is not PHI (and therefore not ePHI or uPHI).[149] There are two ways a covered entity may determine that health information is not individually identifiable, including through an expert determination method and through a safe harbor method.[150] Under the expert determination method, a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable can: (i) apply such principles and methods and determine that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and (ii) document the methods and results of the analysis that justify such determination.[151] Under the safe harbor method, a covered entity must remove eighteen different identifiers relating to the individual (or of relatives, employers, or household members of the individual) and the covered entity must not have actual knowledge that the remaining information could be used alone or

146 *Id.* § 164.402 (defining uPHI).

147 *See Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals*, U.S. DEP'T OF HEALTH & HUM. SERVS. (July 26, 2013), https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html .

148 45 C.F.R. § 164.402 (defining breach).

149 *Id.* § 164.514(a).

150 *Id.* §164.514(b).

151 *Id.* § 164.514(b)(1).

in combination with other information to identify the individual who is the subject of the information.[152] The eighteen identifiers that must be removed include names; all geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geocodes;[153] all elements of dates (except year, unless over eighty-nine years)[154] for dates directly related to an individual; telephone numbers; fax numbers; e-mail addresses; social security numbers; medical record numbers; health plan beneficiary numbers; account numbers; certificate/license numbers; vehicle identifiers and serial numbers, including license plate numbers; device identifiers and serial numbers; Universal Resource Locators (URLs); Internet Protocol (IP) address numbers; biometric identifiers, including finger and voice prints; full face photographic images and any comparable images; and any other unique identifying number, characteristic, or code.[155]

Most covered health care providers (including in-person and virtual health care providers) collect identifiers from their patients, including names, addresses, birthdates, email addresses, and health plan beneficiary numbers.[156] Covered providers and business associates thereof must protect these identifiers in accordance with the HIPAA Privacy Rule and, if those identifiers are maintained in or transmitted by electronic media, in accordance with the HIPAA Security Rule.[157] On the other hand, some health information collected or created by a covered health care provider will not be individually identifiable.

Some AI-powered symptom checkers, for example, only require users to enter their biological sex as well as their age in years before

---

152 *Id.* § 164.514(b)(2).

153 *Id.* § 164.514(b)(2)(i)(B) ("[E]xcept for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.").

154 *See id.* § 164.514(b)(2)(i)(C) (listing as an identifier "All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older").

155 *Id.* § 164.514(b)(2)(i).

156 *See id.*

157 *See id.*

entering their symptoms.[158] Biological sex and age in years (when such age is eighty-nine years or younger) are not identifiers under the HIPAA Privacy Rule.[159] Therefore, if a user eighty-nine years of age or younger only enters the user's age, biological sex, and symptoms, and no other identifiers are captured, the information is not considered individually identifiable under the safe harbor and would not be protected by the HIPAA Privacy Rule.[160] On the other hand, if a user ninety years of age or older enters the user's age, biological sex, and symptoms, the de-identification safe harbor would not be satisfied and the information would need to be protected in accordance with the HIPAA Privacy and Security Rules if the symptom checker is operated by a covered entity or business associate.[161]

Along the same lines, if a medical chatbot does not collect and does not have access to a user's identifiers, the other information collected by the chatbot (e.g., "my stomach hurts and I don't know what to do") is not protected by the HIPAA Privacy or Security Rules.[162] That said, if a medical chatbot collects or has access to a user's identifiers (e.g., "My name is Stacey Tovino and I have a stomachache;" or "My home address is X and I have a headache;" or if the medical chatbot becomes accessible only when the patient is logged into a portal, providing the chatbot with access to individually identifiable health information contained in the portal), the information collected by the chatbot must be protected in accordance with the HIPAA Privacy and Security Rules if the chatbot is operated by a covered entity or business associate.[163]

---

158 *See, e.g.*, *WebMD Symptom Checker*, WEBMD, https://symptoms.webmd.com (last visited Dec. 29, 2023).

159 *See* text accompanying note 156 (listing eighteen different identifiers but neither including stomach complaints nor a patient's lack of knowledge regarding what to do).

160 *See* 45 C.F.R. § 164.514(b)(2)(i).

161 *See id.*

162 *See id.*

163 *See id.*

E. Re-Identified Information

One of the biggest privacy issues associated with AI is its ability to help re-identify purportedly de-identified information.[164] As background, the HIPAA Privacy Rule was first finalized over twenty-four years ago, in December of 2000.[165] At that time, the removal of direct identifiers, including the eighteen identifiers included in that rule's de-identification safe harbor,[166] was thought to be sufficient to permanently protect medical record subjects from ever being identified. Times have (really) changed.[167] Since then, a number of data re-identification attacks have occurred,[168] and AI is helping to lead the re-identification charge.[169] The question becomes whether the HIPAA Rules, as they are currently written, are capable of responding to this risk.

The concept of re-identification is referenced only a few times in the HIPAA Privacy Rule.[170] The first time is in the existing de-identification safe harbor.[171] Remember that, under the safe harbor, covered entities must remove eighteen different identifiers relating to the individual (or of relatives, employers, or household members of the individual) and the covered entity must not have actual knowledge that the remaining information could be used alone or in combination with other information to identify the individual who is the subject of the

---

164 *See generally* Tovino, *supra* note 20, at 992–1006 (summarizing the developing reidentification literature).

165 *See* 65 Fed. Reg. 82462 (Dec. 28, 2000).

166 *See supra* notes 152–155 and accompanying text.

167 *See generally* Gina Kolata, *Your Data Were Anonymized? These Scientists Can Still Identify You*, N.Y. TIMES (July 23, 2019), https://www.nytimes.com/2019/07/23/health/data-privacy-protection.html ("Computer scientists have developed an algorithm that can pick out almost any American in databases supposedly stripped of personal information.").

168 *See generally* Michael Platzer, *AI-Based Re-Identification Attacks–and How to Protect Against Them*, MOSTLY AI (Apr. 22, 2022), https://mostly.ai/blog/synthetic-data-protects-from-ai-based-re-identification-attacks (addressing how AI can help identify the subjects of allegedly de-identified data).

169 *See generally* Ben Dickson, *Inference Attacks: How Much Information Can Machine Learning Models Leak?*, THE DAILY SWIG (Apr. 14, 2021), https://portswigger.net/daily-swig/inference-attacks-how-much-information-can-machine-learning-models-leak (explaining how AI can help identify the subjects of allegedly de-identified data).

170 *See* 45 C.F.R. § 164.514.

171 *See id.* § 164.514(b)(2).

information.[172] The million dollar question is when would a covered entity have actual knowledge that the remaining information could be used alone or combination with other information to re-identify the individual?

Given that the science of re-identification is moving quickly, it is possible that more covered entities in the future will have such knowledge—or at least ought to have such knowledge—when they disclose even de-identified patient records to large technology companies that have vast data with which de-identified data can be matched. And patients are picking up on this thought. In *Dinerstein v. Google*, a former patient named Matt Dinerstein sued Google and the University of Chicago Medical Center alleging that the medical center improperly sold his and other patients' (largely de-identified) medical records to Google.[173] As background, Google had purchased the data from the medical center in an attempt to develop AI-powered software capable of reducing medical complications, eliminating unnecessary hospital stays, and improving health outcomes.[174] The plaintiff, who learned of the sale, was upset because he thought that Google could re-identify him and other medical center patients by combining their mostly de-identified medical records with other information about the patients in Google's possession, such as data collected during the patients' routine use of Gmail, Google Maps, and other Google products.[175] The Seventh Circuit ultimately rejected Dinerstein's argument because he failed to show that he was actually harmed by the disclosure of his medical records.[176] He also failed to show that Google had taken any steps to re-identify him and the other patients.[177] That said, the Seventh Circuit did not foreclose the possibility that a future lawsuit could survive if the plaintiff could demonstrate re-identification and actual harm resulting therefrom.

Dinerstein raises the important issue of when a covered entity would have actual knowledge that, by disclosing purportedly de-

---

172 *See id.*

173 Dinerstein, *supra* note 19, at 502.

174 *Id.* at 507.

175 *Id.* at 510.

176 *Id.* at 522.

177 *Id.* at 515.

identified data to a large technology company that has considerable data of its own, the de-identified data could be matched and thus re-identified. Stated another way, *Dinerstein* suggests that it may be increasingly difficult for covered entities to meet the de-identification safe harbor because they will (or should have) some type of knowledge that the recipient of the allegedly de-identified data will be able to re-identify the data.[178] A number of additional questions quickly follow. For example, can a small, non-tech savvy covered entity (e.g., a social worker with little interest in or knowledge of AI but a desire to make some quick change to support children enrolled in expensive private universities) stick their head in the sand, ignore the well-publicized power of AI to re-identify data, and sell de-identified data without patient authorization? Would this be a HIPAA Privacy violation? Because it is not clear, HHS needs to immediately issue guidance clarifying: (1) what HHS means by "actual knowledge" in the de-identification safe harbor; (2) if and when such knowledge should be imputed to covered entities based on rapid advancement in the science of re-identification and sufficient publicity regarding such advancement; and (3) how HHS plans to regulate the creation, use, or disclosure of synthetic data,[179] which is frequently (but maybe not altogether accurately) hailed as the solution to the risk of re-identification in human data.[180] Currently, the HIPAA Rules regulate only identifiable data, not synthetic data which is thought to be non-identifiable.[181] That

---

178 *See id.* at 516.

179 *Privacy Tech-Know Blog: When What Is Old Is New Again–The Reality of Synthetic Data,* OFF. OF THE PRIV. COMM'R OF CANADA (Oct. 12, 2022), https://www.priv.gc.ca/en/blog/20221012/ (Synthetic data may be defined as "fake data produced by an algorithm whose goal is to retain the same statistical properties as some real data, but with no one-to-one mapping between records in the synthetic data and the real data.").

180 *See id.* (noting that "[r]e-identification [in synthetic data] is still possible if records in the source data appear in the synthetic data" and identifying other problems associated with synthetic data, including the fact that "[o]utliers are at risk of membership inference attacks" and that "[s]ynthetic data does not protect against attribute disclosure.").

181 45 C.F.R. 164.514(a) ("Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable."); *Synthetic Data Generation: Definition, Types, Techniques, and Tools*, TURING, https://www.turing.com/kb/synthetic-data-generation-techniques# (last visited Feb. 21, 2024) ("Fully synthetic data does not have any connection to real data. This indicates that all the required variables are available, yet the data is not identifiable.").

said, if AI can re-identify data subjects from synthetic data, then perhaps the HIPAA Rules need to be amended to clarify this possibility.

A second place in the HIPAA Privacy Rule that references re-identification is a regulation that states that "[d]isclosure of a code or other means of record identification designed to enable coded or otherwise de-identified information to be re-identified constitutes disclosure of protected health information."[182] The HIPAA Privacy Rule has a third regulation that permits a covered entity to assign a code to allow de-identified information to be re-identified by the covered entity, but only if the covered entity does not disclose the code to others.[183] Although a covered entity would be inviting a serious HIPAA Privacy violation by disclosing an actual re-identification code to a technology company with whom it has shared de-identified data, could the covered entity's act of just disclosing the de-identified data to a technology company like Google (that is clearly capable of re-identifying data due to the vast quantity of data it holds about all of us) be considered almost like the disclosure of a code? Again, HHS needs to issue guidance on this issue.

F. Exceptions to PHI

Even when health information is clearly individually identifiable, the HIPAA Privacy Rule does not protect such information in four additional situations; that is, when the information meets the definition of an education record, a student treatment record, or an employment record held by a covered entity in its role as an employer, or if the individual who is the subject of the record has been deceased for more than fifty years.[184] With respect to the first situation, an education record is a record that directly relates to a student and that is maintained by the educational agency or institution.[185] For example, a university that requires a student to upload a digital COVID vaccine record has obtained an education record protected by the Family Educational Rights and Privacy Act of 1974 (FERPA), not PHI, ePHI, and uPHI

---

182 45 C.F.R. § 164.502(d)(2)(i).

183 *Id.* § 164.514(c)(2).

184 *Id.* §160.103 (listing these exceptions from the definition of PHI).

185 34 C.F.R. § 99.3 (defining education record).

protected by the HIPAA Rules.[186] By further example, technology companies are now offering AI-powered chatbots to institutions of higher education.[187] A student who provides individually identifiable health information during a conversation with an educational institution's chatbot (e.g., "Good morning. Do you have an accessible dormitory I can move to? I ask because I now use a wheelchair due to a spinal cord injury. Thank you, Jane Doe.") would be protected by FERPA but not by HIPAA.[188]

With respect to the second situation, a student treatment record is a record relating to a student who is eighteen years of age or older, or is attending an institution of postsecondary education, that is made or maintained by a health professional or paraprofessional at a university-operated student health center and that is not available to anyone other than persons providing treatment to the student.[189] Although these student treatment records will contain individually identifiable health information, they are excluded from the definition of PHI and, thus, excluded from protection under the HIPAA Rules.[190]

---

[186] *See id.*

[187] *See, e.g.*, *Increase Higher Ed Student Retention with Message's Chatbot Technology*, MOD. CAMPUS, https://go.moderncampus.com/signal-vine-chatbot?campaign=google-Message-Chatbot-2023.11campaignid=20749065060&adgroupid=154036551246&utm_source=google&utm_medium=g&utm_campaign=google-Message-Chatbot-2023.11&utm_content=679976922157&utm_term=chatbot%20for%20university&hsa_cam=20749065060&hsa_grp=154036551246&hsa_mt=p&hsa_src=g&hsa_ad=679976922157&hsa_acc=6272256365&hsa_net=adwords&hsa_kw=chatbot%20for%20university&hsa_tgt=kwd-453385018771&hsa_ver=3&gad_source=1 (last visited Dec. 29, 2023).

[188] *See* Tovino, *supra* note 23, at 111–14 (discussing at length the difference in protections under HIPAA and FERPA).

[189] 20 U.S.C. § 1232g(a)(4)(B)(iv) (The regulations implementing FERPA provide a slightly different definition; that is, records on a student who is 18 years of age or older, or is attending an institution of postsecondary education, that are: (i) made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his or her professional capacity or assisting in a paraprofessional capacity; (ii) made, maintained, or used only in connection with treatment of the student; and (iii) disclosed only to individuals providing the treatment. For the purpose of this definition, "treatment" does not include remedial educational activities or activities that are part of the program of instruction at the agency or institution. 34 C.F.R. § 99.3 (2022) (excluding student treatment records from the definition of education record and defining student treatment records)).

[190] 45 C.F.R. § 160.103 (defining PHI; excepting student treatment records defined at 20 U.S.C. § 1232g(a)(4)(B)(iv)).

(Interestingly, they are not protected by FERPA, either.[191]) For example, if a postsecondary student health center has a mobile app that students can use to describe a health symptom and request a medical appointment therefore, most individually identifiable health information collected by the app will meet the definition of a student treatment record. As a result, the information collected by the app will not be PHI or ePHI protected by the HIPAA Privacy and Security Rules and will only be protected by state law.[192] By further example, if a postsecondary student health center makes an AI-powered medical chatbot available to students on campus for similar reasons (e.g., describing a health symptom and securing a medical appointment therefore or, perhaps, asking whether seeing a doctor for a particular symptom would be advisable) any individually identifiable information provided to the chatbot will also not be PHI or ePHI protected by the HIPAA Privacy and Security Rules and will only be protected by state law.[193]

With respect to the third situation, employment records held by a covered entity in its role as an employer, not a covered entity, also are not protected by the HIPAA Privacy Rule.[194] For example, if a covered hospital employs nurses and other health care providers and requires such providers to provide paper or electronic proof of their COVID vaccination, the employees' vaccine records are employment records protected by employment law,[195] not PHI protected by HIPAA. Along the same lines, employers that use AI-powered chatbots to automate human resources (HR) tasks, such as streamlining employee onboarding, processing paid time off (PTO) and Family and Medical Leave Act (FMLA) requests, responding to employee questions relating to policies and procedures, and otherwise providing 24/7 HR support also

---

191 *See* Tovino, *supra* note 23, at 111–14 (explaining the information protected by both FERPA and HIPAA; explaining that student treatment records are protected by neither).

192 *See id.* at 88–92 (explaining, and disagreeing with, this interesting legal result).

193 *Id.* (explaining this result).

194 45 C.F.R. § 160.103 (defining PHI; excepting employment records held by a covered entity in its role as an employer).

195 *See* 42 U.S.C. §§12101–12213. For example, Title I of the Americans with Disabilities Act, which prevents employers from discriminating against qualified individuals with disabilities on the basis of such disabilities, would apply. *Id.* §12112(a).

may receive individually identifiable health information.[196] For example, an employee of a health insurance company may use a chatbot to request FMLA, explaining that a serious health condition makes the employee unable to perform the essential functions of their job. Here, the employee would be disclosing individually identifiable health information with the chatbot but the employee would not be disclosing PHI protected by the HIPAA Rules.[197] Instead, the information relating to the serious health condition is an employment record held by the health insurance company in its role as an employer, not in its role as a HIPAA covered health plan.[198]

With respect to the fourth and final situation, health information regarding individuals who have been deceased for more than fifty years also is not PHI protected by the HIPAA Rules.[199] A classic example would be a medical record relating to a patient who passed away more than fifty years ago (*e.g.*, in 1970). That medical record is not PHI protected by the HIPAA Rules.[200] An AI-related example would be a hospital that shares identifiable medical records of people who passed away more than fifty years ago with a pharmaceutical company. The pharmaceutical company will then use AI and machine learning to analyze the records, uncover new insights, and drive pharmaceutical development that has the potential to quickly improve patient outcomes.[201] As discussed in more detail in Part V, immediately below,

---

196 *See* 5 *Ways to Use Chatbots for Internal Employees*, INBENTA, https://www.inbenta.com/articles/5-ways-to-use-chatbots-for-internal-employees/ (last visited Dec. 31, 2023).

197 45 C.F.R. § 160.103 (defining PHI; excepting from that definition information held by a covered entity in its role as an employer, not as a covered entity).

198 *See id.*

199 *See id.* (defining protected health information but excluding from that definition records regarding people who have been deceased for more than 50 years).

200 *See id.*

201 *See* Ashley Welch, *Artificial Intelligence Is Helping Revolutionize Healthcare As We Know It*, JOHNSON & JOHNSON (Sept. 13, 2023), https://www.jnj.com/innovation/artificial-intelligence-in-healthcare?=&utm_source=google&utm_medium=cpc&utm_campaign=GO-USA-ENG-PS-Corporate+Equity-GP-PH-RN-NB_STORIES_ARTIFICIAL+INTELLIGENCE&utm_content=AI+-+Machine+Learning&utm_term=machine+learning+and+health+care (quoting a technology leader as stating, "Using the latest innovations in AI and machine learning (ML), we are able to quickly analyze these vast datasets (including electronic medical records, lab results or even medical imaging like X-rays, MRIs and CT scans), uncover new insights and then drive actions with real potential to improve patient outcomes.").

the hospital is not required to obtain prior written authorization from the deceased patients' relatives or legal representatives before sharing their loved ones' data with the pharmaceutical company because the information is not PHI regulated by the Privacy Rule.

V. USE AND DISCLOSURE REQUIREMENTS

Once a covered entity or business associate is using or disclosing PHI, the HIPAA Privacy Rule's three use and disclosure requirements come into play. The first use and disclosure requirement allows a covered entity to use and disclose PHI without any prior permission from the individual who is the subject of the PHI but only to carry out certain treatment (T), payment (P), and health care operations (O) activities (collectively TPO activities),[202] as well as certain public benefit (PB) activities.[203] Thus, one way to support the data sharing that is necessary to realize AI's full potential (for those who are in favor of empowering AI) is to take full advantage of the permissive TPO- and PB-related uses and disclosures.[204] Traditional (non-AI) and AI-related examples of T, P, and O as well as PB are provided below.

Treatment (T) is defined as "the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another."[205] In a non-AI treatment example, a covered physician would be permitted to transmit a patient's prescription to a pharmacy without the patient's prior permission because prescribing a therapeutic falls within the definition of treatment. That is, it is the provision of health care because "health care" is defined to include "therapeutic" care.[206] In an AI treatment example, a covered radiologist or pathologist would be permitted to obtain diagnostic assistance from an AI-powered tool, also

---

202 45 C.F.R. § 164.506(c).

203 *Id.* § 164.512.

204 *See id.*; *see also id.* § 164.506(c).

205 *Id.* § 164.501 (defining treatment).

206 *Id.* § 160.103 (defining health care).

without the patient's prior permission, because the definition of "health care" (on which the definition of "treatment" is based) includes diagnostic services.[207] There is nothing in the HIPAA Privacy Rule, as it is currently written (including the minimum necessary rule),[208] that impacts the ability of a physician or other provider to use or disclose PHI in connection with AI to treat a patient so long as any necessary business associate agreements (BAA) are in place.[209] That said, authorities outside the HIPAA Privacy Rule do regulate covered entities' use of AI in the health care context. For example, Section 1557 of the Affordable Care Act: (1) prohibits certain health care providers from discriminating against patients through their use of patient care decision support tools, including AI-powered tools; (2) requires these providers to make reasonable efforts to identify uses of AI-powered tools that create discrimination risks by relying upon input variables that measure race, color, national origin, sex, age, and disability; and (3) requires these providers to make reasonable efforts to mitigate those discriminatory risks.[210]

Payment (P) is defined, in relevant part, as the "activities undertaken by . . . [a] health care provider or health plan to obtain or provide reimbursement for the provision of health care."[211] Payment includes, but is not limited to, billing, claims management, determinations of

---

207 *Id.* (defining health care).

208 The minimum necessary rule provides that when covered entities or business associates are using or disclosing PHI or are requesting PHI from another covered entity or business associate, they must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. *Id.* § 164.502(b). That said, the minimum necessary rule does not apply to disclosures to or requests by a health care provider for treatment. *Id.* § 164.502(b)(2)(i).

209 *See* 45 C.F.R. § 164.404; *see also* Rajpurkar & Lungren, *supra* note 106, at 1981; *see also* Haug & Drazen, *supra* note 106, at 1204; *see also* Zech et al., *supra* note 107; *see also* Prakash et. al., *supra* note 108, at 191 (discussing the BAA requirement).

210 *See* Affordable Care Act (ACA) § 1557, 42 U.S.C. § 18116(a) ("an individual shall not . . . be subjected to discrimination under, any health program or activity, any part of which is receiving Federal financial assistance . . . or under any program or activity that is administered by an Executive Agency . . ."); Letter from Melanie Fontes Rainer, Dir., Off. Civ. Rts., U.S. Dep't Health & Human Servs., to Colleagues, Re: Ensuring Nondiscrimination in the Use of Artificial Intelligence and Other Emerging Technologies (Jan. 10, 2025), https://www.hhs.gov/sites/default/files/ocr-dcl-section-1557-artificial-intelligence.pdf (explaining that ACA Section 1557 prohibits certain health care providers from discriminating against individuals through their use of AI-powered patient care decision support tools).

211 45 C.F.R § 164.501 (defining payment).

eligibility or coverage, and utilization review activities such as precertification and preauthorization.[212] In a non-AI example, a covered physician would be permitted to disclose a patient's PHI to the patient's insurer for reimbursement purposes without the patient's authorization because "billing" falls within the definition of payment.[213] In an AI example, a health plan would be allowed to use an AI-powered tool that helps make coverage determinations, including denying health care claims, because "claims management" and "determination of eligibility or coverage" fall within the definition of payment[214] and the TPO regulation allows covered entities to disclose PHI for their own payment activities.[215] The only prerequisite would be the execution of any necessary BAAs if the AI-powered tool is operated by a third party and is not owned and operated by the health plan.[216] Although the HIPAA Privacy Rule currently does not restrict the ability of a covered insurer to use AI for payment activities, authorities outside the HIPAA Privacy Rule do. For example, California's new Physicians Make Decisions Act, effective January 1, 2025, requires insurance coverage decisions to be made by licensed health care providers, not (solely) AI algorithms.[217]

Health care operations (O) is defined with respect to a laundry list of activities, some of which include "conducting quality assessment and improvement activities, including outcomes evaluation" as well as "conducting or arranging for . . . legal services."[218] In a non-AI example, a covered physician who is being sued by a patient for medical malpractice would be permitted to disclose the patient's medical

---

212 *Id.*

213 *Id.*

214 *Id.*

215 *Id.* § 164.506(c)(1).

216 *See id.* § 164.404; Rajpurkar & Lungren, *supra* note 106, at 1984; Haug & Drazen, *supra* note 106, at 1204; Zech et al., *supra* note 107; Prakash et. al., *supra* note 108, at 191 (discussing the BAA requirement).

217 CAL. HEALTH & SAFETY CODE § 1367.01(k) ("A health care service plan . . . that uses an artificial intelligence, algorithm, or other software tool for the purpose of utilization review or utilization management functions, based in whole or in part on medical necessity . . . shall . . . ensure all of the following: . . . (B) The artificial intelligence, algorithm, or other software tool does not base its determination solely on a group dataset. . . . (D) The artificial intelligence, algorithm, or other software tool does not supplant health care provider decisionmaking.").

218 45 C.F.R. § 164.501 (defining health care operations).

record to the physician's attorney without the prior permission of the patient because the physician would be "arranging for . . . legal services."[219] The only pre-requisite would be the physician executing a BAA with the attorney if the attorney is not part of the physician's workforce (e.g., if the attorney is the physician's outside counsel rather than an employed general counsel).[220] In an AI-example, a hospital would be permitted to use an AI-powered tool, or disclose PHI to a business associate who uses AI, to conduct quality assessment and improvement activities—all without the patient's prior permission.[221] Again, there is nothing in the HIPAA Privacy Rule that forbids a covered entity from using or disclosing PHI in connection with TPO activities when AI is used to assist in those TPO activities (assuming compliance with the minimum necessary rule[222] and the execution of any necessary business associate agreements).[223] Again, one way to support the data sharing necessary to realize the full potential of AI (for those who are in favor of empowering AI) is for covered entities and business associates to take full advantage of these permissive TPO-related uses and disclosures.

In addition to TPO-related uses and disclosures, PB-related uses and disclosures are also permitted without the prior written authorization of the data subjects.[224] Illustrative (not exhaustive) PB-related uses and disclosures include those made in connection with certain: (1) federal, state, local, and tribal laws, as well as court orders, that require information to be used or disclosed; (2) public health activities, including mandatory disease reporting; (3) elder abuse, neglect, and exploitation reporting activities; (4) health care oversight activities, including fraud and abuse disclosures to state Medicaid offices; (5) judicial and administrative proceedings in which a qualified protective order has

---

219 *Id.*

220 *See* 45 C.F.R. § 164.404; Rajpurkar & Lungren, *supra* note 106, at 1981; Haug & Drazen, *supra* note 106, at 1201; Zech et al., *supra* note 107; Prakash et. al., *supra* note 108, at 191 (discussing the BAA requirement).

221 *See id.*

222 *See* 45 C.F.R. § 164.502(b) (not containing an exception for disclosures for health care operations activities).

223 *Id.* § 164.504(e)(1) (addressing business associate agreements). That said, authorities outside the HIPAA Privacy Rule can and do restrict the use of AI in health care operations activities.

224 *Id.* § 164.512 (listing twelve public benefit (PB) activities for which PHI may be used or disclosed without prior patient authorization).

been obtained or other privacy requirements have been satisfied); (6) law enforcement activities; (7) coroner, medical examiner, and funeral director activities; (8) organ procurement activities; (9) research activities; (10) disclosures necessary to avert a serious threat to health and safety; (11) military and intelligence activities; and (12) workers' compensation activities.[225] In a non-AI example of a permissive PB-related disclosure, a covered physician who diagnoses a patient with COVID-19 would be permitted to report the diagnosis to the state department of health because mandatory disease reporting is considered a public health activity. The report could be made without the patient's prior written authorization[226] and, even, over the patient's express objection.[227] In an AI-example, a hospital may use an AI-powered tool capable of detecting incorrectly entered diagnostic or procedure codes and may disclose information evidencing, for example, upcoding to a public health care program as part of voluntary fraud and abuse reporting.[228] This type of self-disclosure can be made without patient authorization.[229] Again, one way to support the data sharing necessary to realize the full potential of AI (for those who are in favor of empowering AI) is for covered entities and business associates to take full advantage of the twelve permissive PB-related uses and disclosures.

The first use and disclosure requirement allowed TPO[230] and PB-related[231] uses and disclosures. The second use and disclosure requirement permits a covered entity to use or disclose an individual's PHI for certain activities, but only if the individual is informed (orally or in writing) in advance of the use or disclosure and is given the (oral or written) opportunity to agree to, prohibit, or restrict the use or disclosure.[232] The certain activities[233] captured by this second use and

---

225 *See id.*

226 *See id.* § 164.512(b).

227 Indeed, many state mandatory disease reporting laws make it a misdemeanor for a physician not to report a disease required to be reported.

228 *See* 45 C.F.R. § 164.512(d) (permitting covered entities to disclose PHI to a health oversight agency for a health oversight activity).

229 *See id.*

230 *Id.* § 164.506(c)(1)–(5).

231 *Id.* § 164.512.

232 *Id.* § 164.510.

233 The certain activities include, but are not limited to, disclosures of PHI: (1) from a health care

disclosure requirement have potential (but limited) relevance in the context of AI and will not be discussed further. However, the third use and disclosure requirement—a default rule—requires a covered entity to obtain the prior written authorization of the individual who is the subject of PHI before using or disclosing the PHI in any situation that does not fit within the first two rules.[234] In a non-AI example, this default rule would be violated if a covered hospital used an online tracking technology on its website to collect PHI from patients who visited the website and then disclosed that PHI for a non-TPO or non-PB purpose without first obtaining the patient's prior written authorization.[235] In an AI example, the default rule would be violated if a covered hospital sold PHI (versus de-identified information) to a technology company so the company could use the data to create and train AI-powered tools if the hospital did not obtain prior authorization from each patient whose PHI was sold and the authorization form did not disclose the hospital's receipt of remuneration from the technology company.[236] For those who want to free data sharing to empower AI, this authorization requirement is the biggest hurdle. For those who want to protect data, this authorization requirement is the armor.

The AI example described above is not theoretical and, indeed, has already been implicated in litigation.[237] As discussed in Part IV(E),

---

provider's facility directory; (2) to a person who is involved in an individual's care or payment for care; and (3) for certain notification purposes, such as when an attending physician or a hospital social worker notifies a partner or spouse of a patient's death. For example, a covered hospital can disclose a patient's hospital room number and general condition in one word (e.g., good, fair, poor, stable) to a person who calls the hospital and asks about the patient by name if the patient has agreed or not objected to the disclosure. *Id.* § 164.510.

234 *Id.* § 164.508.

235 *Use of Online Tracking Technologies by Covered Entities and Business Associates*, U.S. DEP'T HEALTH & HUMAN SERVS. (Dec. 1, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html ("For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.").

236 *See* 45 C.F.R. § 164.502(a)(5)(ii), .508(a)(4) (regulating the sale of PHI; generally requiring patients to sign a prior written authorization form before the sale of their PHI takes place unless an exception applies; also requiring the authorization form to state that the disclosure of PHI will result in remuneration being paid to the covered entity).

237 *See, e.g.*, U.S. DEP'T HEALTH & HUMAN SERVS., *supra* note 147; 45 C.F.R. § 164.402; 45 C.F.R. § 164.514(a); 45 C.F.R. § 164.514(b)(1) (discussing the *Dinerstein* case, which involved a medical center that sold allegedly de-identified information to a technology company without prior

medical centers such as the University of Chicago Medical Center have sold data they claim were de-identified to technology companies in an attempt to avoid regulation by the HIPAA Rules, including the HIPAA Privacy Rule's prior written authorization requirement.[238] That said, the recipient technology company (*e.g.*, Google) already has (or probably soon will have) the AI-supported capability of re-identifying the data, thus raising the question (at least for the plaintiff who sued the University of Chicago Medical Center) of whether the HIPAA Privacy Rule was violated. As discussed in Part IV(E), HHS needs to immediately issue guidance regarding the interplay between covered entities' disclosure of purportedly de-identified information and the ability of technology companies to re-identify that information using AI.

Although the HIPAA Privacy Rule regulates the use and disclosure of PHI that has already been collected, interestingly the HIPAA Privacy Rule does not regulate the initial gathering, collection, or creation of PHI.[239] For example, the HIPAA Privacy Rule does not regulate the questions an AI-powered symptom checker or medical chatbot may ask of a patient.[240] That said, once PHI is collected by a covered entity, the HIPAA Privacy Rule does regulate how that covered entity subsequently uses and discloses that information.[241] For example, if a covered entity that operates a symptom checker or medical chatbot wants to subsequently use or disclose the individual's PHI for marketing purposes, the covered entity would be required to obtain the patient's prior written authorization.[242] Otherwise, a violation of the HIPAA Privacy Rule has occurred.

written authorization of the patients who were the subjects of that information; the plaintiff claimed that because the technology company could use AI to re-identify the patients, privacy had been violated).

238 *See infra* Part IV (explaining that the HIPAA Rules only protect PHI, ePHI, and uPHI, not de-identified information).

239 *See* 45 C.F.R. § 164.502–.514 (codifying requirements relating to "uses" and "disclosures" but establishing no requirements relating to the gathering, collection, or creation of PHI).

240 *See id.*

241 *See id.*

242 *See id.* § 164.508(a)(3)(i) (generally requiring prior patient authorization before uses or disclosures of PHI for marketing activities).

VI. INDIVIDUAL RIGHTS

In addition to the use and disclosure requirements, the HIPAA Privacy Rule also establishes five rights for individuals who are the subject of PHI. These individual rights include the right to receive a notice of privacy practices, the right to request additional privacy protections, the right to access PHI, the right to request amendment of PHI and the right to receive an accounting of PHI disclosures.[243] The use of AI in healthcare raises novel and interesting issues regarding some of these rights.

For example, the first individual right provides that, "an individual has a right to adequate notice of the uses and disclosures of [PHI] that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information."[244] This notice, referred to as the notice of privacy practices (NOPP), has certain required elements.[245] For example, patients must be given a description, including at least one example, of the types of uses and disclosure that their covered entities are permitted to make for treatment, payment, and health care operations (TPO) without patient authorization.[246] Patients also must be given a description of the types of uses and disclosures that require an authorization.[247] To date, the descriptions and examples provided by most covered entities in their NOPPs are non-AI related. For example, in the Author's current city of Norman, Oklahoma, the local hospital (Norman Regional Hospital) provides the following TPO descriptions and examples in its NOPP:

> Treatment. We will use your medical information to provide you with medical treatment and services. We maintain medical information about our patients in an electronic medical record that allows us to share medical information for treatment purposes. This facilitates access to medical information by other health care providers who provide care to you. Example: Your medical information may be disclosed to doctors, nurses,

---

243 45 C.F.R. § 164.520–.528.

244 *Id.* § 164.520(a)(1).

245 *Id.* § 164.520(b)(1).

246 *Id.* § 164.520(b)(1)(II)(A).

247 *Id.* § 164.520(b)(1)(II)(E).

> technicians, students or other personnel who are involved in taking care of you. . . .
>
> Payment. We may use medical information about you for our payment activities. Common payment activities include, but are not limited to: Determining eligibility or coverage under a plan; and Billing and collection activities. Example: Your medical information may be released to an insurance company to obtain payment for services. . . .
>
> Operations. We may use your medical information for operational or administrative purposes. These uses are necessary to run our business and to make sure patients receive quality care. Common operation activities include, but are not limited to: Conducting quality assessment and improvement activities; . . . Arranging for legal or auditing services; . . . Examples: (1) We may use your medical information to conduct internal audits to verify that billing is being conducted properly. (2) We may use your medical information to contact you for the purposes of conducting patient satisfaction surveys or to follow-up on the services we provided.[248]

Note that not one of these descriptions or examples involves AI. One question is whether HHS needs to amend the HIPAA Privacy Rule to require covered entities to make patients aware of at least some of the ways in which AI is involved in the collection, creation, use, and disclosure of their PHI. The Author believes that such amendments are needed. For example, the HIPAA Privacy Rule could require patients to be given examples of how their radiologists and pathologists use AI-assisted diagnostic tools. Patients also could be told that ChatGPT will be listening to and summarizing their encounters with their physicians and that these summaries will be placed in the patient's permanent medical record. Along the same lines, patients could be told that their health plans use AI to review and deny health care claims. Patients could also be told that their de-identified information is being disclosed to technology companies, but these companies have or may have the capability of re-identifying the data. Informing patients of the ways in which AI is used to collect, create, evaluate, use, and disclose their PHI would support the purpose behind the HIPAA Privacy Rule's NOPP requirement; that is, "the right to adequate notice of the

---

248 *See Notice of Privacy Practices*, NORMAN REG'L HEALTH SYS., (underlined emphasis added; left and right justification changed from the original to improve readability in this Article), https://www.normanregional.com/privacy (last visited Jan. 1, 2024).

uses and disclosures of [PHI] that may be made by the covered entity."[249]

In addition to the right to adequate notice through an NOPP, patients also have the right to request additional privacy protections. Here, the HIPAA Privacy Rule provides: "A covered entity must permit an individual to request that the covered entity restrict . . . [u]ses or disclosures of protected health information about the individual to carry out treatment, payment, or health care operations."[250] With one exception that rarely applies,[251] covered entities are not required to agree to a requested restriction.[252] If a covered entity does agree to a requested restriction, however, the entity must adhere to its agreement.[253]

One question raised by AI is whether patients can request their covered entities not to use or disclose their PHI in connection with an AI-powered tool, or not to allow an AI-powered tool (such as DAX Express[254]) to generate PHI about them. Under the current HIPAA Privacy Rule, the answer is yes if the request is limited to the contexts of treatment, payment, and health care operations.[255] For example, a patient does have a legal right to ask a physician not to have DAX Express listen to the patient's encounter with the physician and write a summary of that encounter, as this is a treatment-related request.[256] That said, the physician is not required to agree to the restriction.[257] If the physician does agree to the restriction, the physician would be prohibited from using DAX Express to listen to and summarize the encounter with the patient.[258]

---

249 45 C.F.R. § 164.520(a)(1).

250 *Id.* § 164.522(a)(1)(i).

251 *Id.* § 164.522(a)(1)(vi) (relating to requests for restrictions on the use or disclosure of PHI relating to services for which the patient has paid out of pocket in full).

252 *Id.* § 164.522(a)(1)(ii).

253 *Id.* § 164.522(a)(1)(iii).

254 *See* text accompanying *supra* notes 116–122.

255 45 C.F.R. § 164.502(a)(1)(ii).

256 45 C.F.R. § 164.522(a)(1)(i)(A).

257 *Id.* § 164.522(a)(1)(ii).

258 *Id.* § 164.522(a)(1)(iii).

Along the same lines, a patient does have a legal right to ask a covered health plan not to use an AI-powered tool to evaluate the patient's health care claim and to deny the patient insurance coverage as this is a payment-related request.[259] That said, the health plan is not required to agree to the requested restriction.[260] If the health plan does agree to the requested restriction, it may not use the AI-powered tool to evaluate the patient's health care claim.[261] As an aside, and to prevent the health plan from getting the patient's information in the first place, the patient can ask their provider not to disclose their PHI to the health plan for payment; however, to ensure that the provider agrees to the patient's request, the patient must pay out of pocket, in full, for their treatment.[262] Called "pay for privacy," this provision allows patients to keep PHI from their health plans but only if they can afford to pay for their health care services by cash, credit, check, or other acceptable non-insurance means at the point of health care service.[263]

In addition to the right to receive an NOPP and the right to request additional privacy protections, patients also have a right to request amendment of PHI. Here, the HIPAA Privacy Rule provides that "an individual has the right to have a covered entity amend protected health information or a record about the individual in a designated record set for as long as the protected health information is maintained in the designated record set."[264] One can imagine a patient encounter that was summarized inaccurately by DAX Express. In this case, the patient would have the legal right to request the covered entity to amend the incorrect, AI-generated PHI about the patient.[265] That said, the HIPAA Privacy Rule allows the covered entity to deny the patient's request in several situations, including if the information is "accurate and complete."[266] One certainly can conceive of a hypothetical in which DAX Express listens to and writes an encounter summary that

---

259 Remember, the definition of payment includes "determinations of . . . coverage." *Id.* § 164.501 (defining payment).

260 *Id.* § 164.522(a)(1)(ii).

261 *Id.* § 164.522(a)(1)(iii).

262 45 C.F.R. § 164.522(a)(1)(vi).

263 *Id.*

264 *Id.* § 164.526(a)(1).

265 *Id.*

266 *Id.* § 164.526(a)(2)(iv).

is subtly (but not wholly) inaccurate, the patient wishes to have the summary amended, but the provider believes the summary is accurate enough. Whether the amendment would be required in this case would be a fact issue. Guidance from HHS on the definition of "accurate and complete" would be helpful given evidence showing that ChatGPT is not always accurate.[267]

Note that the HIPAA Privacy Rule also allows the covered entity to deny the patient's request if the PHI was "not created by the covered entity."[268] One can imagine a situation in which DAX Express generates a summary of a patient encounter, the patient wishes the summary to be amended, and the physician refuses to do so on the grounds that DAX Express, not the physician, created the summary. In this case, HHS likely would attribute the summary to the physician (since the physician is the covered entity who is assisted by DAX Express) and require the physician to amend the summary. That said, if the physician does not or will not amend the summary, technically DAX Express would be required to correct the summary.[269]

VII. BREACH NOTIFICATION ISSUES

Parts V and VI of this Article focused on the use and disclosure requirements as well as the individual rights set forth in the HIPAA Privacy Rule. One question is how AI will implicate the HIPAA Breach Notification Rule. Remember, the HIPAA Breach Notification Rule requires covered entities, following the discovery of a breach[270] of uPHI,[271] to notify each individual whose uPHI has been, or is reasonably believed by the covered entity to have been, accessed, acquired,

---

267 *See, e.g.*, *ChatGPT: Friend or Foe?*, 5 LANCET DIGIT. HEALTH e102 (2023) (noting that ChatGPT incorrectly added extra information to a patient's discharge summary).

268 45 C.F.R. § 164.526(a)(2)(i).

269 The HIPAA Privacy Rule requires business associates, such as DAX Express, to "make available PHI for amendment and incorporate any amendments." *See id.* § 164.504(e)(2)(ii)(F).

270 *Id.* § 164.402 (defining breach as the "acquisition, access, use, or disclosure of [PHI] in a manner not permitted under [the HIPAA Privacy Rule] which compromises the security or privacy of the [PHI];" providing exceptions to the definition of breach).

271 *Id.* § 164.402 (defining uPHI as PHI that is "not rendered unusable, unreadable, or indecipherable to unauthorized persons" through the use of certain HHS-specified technologies or methodologies).

used, or disclosed as a result of such breach.[272] The notification, which must be provided without undue delay and within sixty calendar days after the discovery of the breach, must include: (1) a brief description of the nature of the breach, including the date of the breach and the date of its discovery; (2) a description of the types of uPHI involved in the breach; (3) any steps the individual should take to protect herself from potential harm resulting from the breach; (4) a brief description of the steps taken by the covered entity to investigate the breach, to mitigate harm to individuals whose uPHI was part of the breach, and to protect against future breaches; and (5) contact information sufficient to allow individuals to ask questions or learn additional information about the breach.[273]

When a breach involves the uPHI of more than 500 residents of a state or jurisdiction, the HIPAA Breach Notification Rule also requires the covered entity to notify prominent media outlets serving the state or jurisdiction.[274] When a breach involves the uPHI of 500 or more individuals, regardless of their state of residency, the covered entity must also notify the Secretary of HHS within sixty calendar days after the discovery of the breach.[275] Finally, when the breach involves the uPHI of less than 500 individuals, regardless of their state of residency, the covered entity must notify the Secretary of HHS not later than sixty calendar days after the end of the calendar year.[276]

How the HIPAA Breach Notification Rule will be implicated in AI contexts depends on a careful understanding of the words "breach"[277] and "uPHI"[278] as well as the phrase "has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or

---

272 *Id.* § 164.404(a)(1). The summary of the HIPAA Breach Notification Rule set forth in this Part VII is taken with permission from Tovino, *supra* note 23, at Part I(A)(3).

273 45 C.F.R. § 164.404(b)–(c).

274 *Id.* § 164.406(a).

275 *Id.* § 164.408(b).

276 *Id.* § 164.408(c).

277 *Id.* § 164.402 (defining breach as the "acquisition, access, use, or disclosure of [PHI] in a manner not permitted under [the HIPAA Privacy Rule] which compromises the security or privacy of the [PHI]"; providing exceptions to the definition of breach).

278 *Id.* § 164.402 (defining uPHI as PHI that is "not rendered unusable, unreadable, or indecipherable to unauthorized persons" through the use of certain HHS-specified technologies or methodologies).

disclosed as a result of such breach."[279] For example, if a hospital de-identifies medical record data in accordance with the de-identification safe harbor[280] and discloses it to a technology company that wishes to create and train AI-powered tools, technically the HIPAA Rules do not apply because the information disclosed is de-identified and therefore does not meet the definition of PHI (or ePHI or uPHI). However, if the technology company can re-identify the data, has there been a breach? Stated another way, does the re-identified data meet the definition of uPHI (even though, originally, it did not meet the definition of PHI)? When the data is re-identified, does that constitute the "acqui[sition] . . . as a result of [a] . . . breach"?[281] HHS needs to issue guidance regarding the application of defined terms in the HIPAA Breach Notification Rule to common scenarios involving AI.

VIII. CONCLUSION

This Article has described a variety of ways in which health information is collected, created, used, and/or disclosed in the context of AI and has identified illustrative privacy, security, and breach notification issues that flow therefrom. This Article also has analyzed these issues under the HIPAA Privacy, Security, and Breach Notification Rules, identifying: (1) significant gaps in privacy, security, and breach notification regulation in the context of AI-powered tools; (2) a significant hurdle that can interfere with data sharing and AI's goal of improving health care (*i.e.*, the requirement for prior patient authorization in many data sharing scenarios); and (3) major regulatory provisions that require clarification and/or amendment to respond to the expansion of AI in healthcare.

Although this Article has focused on the HIPAA Rules, the privacy and security of health information collected, created, used, and/or disclosed in connection with AI is governed by a frustrating patchwork of other federal and state laws that are important to know. For example, additional privacy and security requirements are sourced in state professional practice acts that apply to licensed health

---

279 45 C.F.R. § 164.404(a)(1). The summary of the HIPAA Breach Notification Rule set forth in this Part VII is taken with permission from Tovino, *supra* note 23, at Part I(A)(3).

280 *See* text accompanying *supra* notes 152–55.

281 45 C.F.R. § 164.404(a)(1).

professionals who practice in the state.[282] Still other privacy and security rules are sourced in state facility licensing laws that apply to certain, but not all, health care facilities that are located in the state.[283] Additional privacy rules are sourced in state medical record privacy laws, which are designed to extend federal-like protections to information not protected by federal law.[284] As of this writing, twenty states have new data protection laws that protect the privacy and security of certain (but not all) health information.[285] All of these laws need to be considered in an AI-involved scenario in order for a privacy, security, or breach notification analysis to be complete.

[282] *See* Tovino, *supra* note 20, at 23, Part II (discussing state professional practice acts).

[283] *See id.* (discussing state facility licensing laws).

[284] *See id.* (discussing state medical record privacy laws).

[285] *See id.* (discussing new state consumer data protection laws); Pittman, *supra* note 28, at 1.