From Algorithm to Exam Room: Navigating the Use of Artificial Intelligence in Health Care

By Jane Bello Burke

Introduction

In health care today, artificial intelligence (AI) is reshaping clinical workflows. One transformative application is ambient listening, sometimes referred to as the "virtual scribe." This technology uses AI to capture conversations between clinicians and patients and to generate clinical documentation.

As major electronic health record vendors increasingly embed ambient listening capacity into their platforms,[1] AI is becoming an integral part of mainstream healthcare. From a compliance perspective, what are the implications for the healthcare provider?

How the Technology Works

At its core, the virtual scribe brings together several advanced technologies. To issue-spot, it is necessary to understand the operation and limitations of the technology.

In a clinical setting, the use of a virtual scribe might proceed as follows. A provider begins a patient encounter by starting an audio recording on a mobile device at the outset of a patient visit or care team meeting.[2] As the conversation unfolds, automatic speech recognition[3] converts spoken dialogue into text. The AI model[4] passes the text through a large language model, which has been trained on vast amounts of general and medical language.[5] It filters out irrelevant chatter (at least in theory), attempts to distinguish between speakers, and extracts key clinical elements such as symptoms, diagnoses, and treatment plans. The system generates a draft clinical note for the clinician to review. Some platforms go a step further and prepare suggested orders for tests or prescriptions for the clinician to review and finalize.

Identifiable Risks

With the impressive capabilities and quick adoption of virtual scribes, there are several sources of error and a host of potential risks demanding careful compliance oversight.

One common challenge is the misinterpretation of audio, as strong accents, poor auditory quality, or background noise can distort the transcription or cause the system to misattribute statements to an incorrect speaker.[6] Another issue is the concept of hallucination,[7] which describes AI's tendency to insert fabricated or incorrect details with unwarranted confidence. Hallucination occurs in generative AI because the model relies on patterns and probability rather than cognition or reasoning.[8]

Model bias[9] is a related concern: if the training data reflect societal inequities, such as underrepresentation of certain racial, gender, or socioeconomic groups, the AI can reproduce and even amplify the disparities. Over time, AI models can experience drift or degradation,[10] continually reducing accuracy unless closely monitored and retrained. These issues are compounded by the "black box problem,"[11] the idea that the internal workings of proprietary AI systems are opaque, which makes it difficult for users to understand their functionality or to audit their outputs.

Clearly, human oversight is essential. And yet, even when oversight occurs, the process is vulnerable to automation bias,[12] the tendency to overtrust AI outputs and to overlook errors, especially as the technology becomes increasingly reliable. In essence, as AI becomes more accurate, human safeguards tend to become more fragile.

Current Oversight and Regulation

In the face of these changes, what does the provider need to do to demonstrate compliance?

Currently, there is no fully developed body of law around AI, but instead, a complex legal landscape that is continually evolving. The current guardrails exist in a patchwork of existing federal and state laws, developing AI-specific legislation, shifting executive orders,[13] federal regulatory activity[14] and agency guidance,[15] and voluntary standards. This will change – and there is already developing – a field of AI law, in which there will be experts as with privacy law today. But as of this writing, we are not there yet.

Vendor Contracting and Privacy Considerations

In identifying the rules of the road, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a good place to start.[16] The implications of HIPAA for AI-enabled technology are profound.

Under the Privacy Rule, a healthcare provider that accepts third-party payment and bills electronically for services is a covered entity and duty-bound to comply with HIPAA's requirements.[17] A software developer, however, typically is not a health plan, a health care clearinghouse, or a health care provider and typically does not transmit health information in electronic form, so typically it is not a covered entity. The use of the virtual scribe involves the receipt of a protective health agreement (PHI)[18] for a HIPAA-related function – data analysis – so the developer meets the definition of a business associate.[19] Therefore, the parties need a business associate agreement (BAA),[20] and the "minimum necessary"[21] standard applies.

As a result of the BAA, the software developer will have contractual obligations to protect the confidentiality of the provider/client's PHI. If the business associate violates these obligations, the breach triggers contractual remedies and potential liability.[22]

What about the vendor's use of PHI to train its model? Some vendors claim their models do not learn from patient data, while others do want to use the recordings to improve their systems. Under HIPAA, covered entities and their business associates may use or disclose PHI for the covered entity's own treatment, payment, or health care operations if otherwise consistent with HIPAA.[23] But a vendor's use of PHI to train a commercial AI model will not necessarily fall within these categories.[24]

For the provider seeking to adopt a virtual scribe, what are the alternatives for maintaining compliance? One option would be to secure patient authorization for the vendor's specific use of PHI for development, training, and product improvement.[25] This approach, however, can be hit-or-miss. A second option would be to require the vendor to use de-identified data for any training purposes.[26] De-identified data is not considered PHI, and HIPAA does not require patient permission to use it.[27]

Yet, the use of de-identified data can carry its own risks. In *Dinerstein v. Google*,[28] a former hospital patient brought a class action alleging that a university hospital had improperly sold his and other patients' anonymized health records to Google for research involving the creation of predictive health models in violation of HIPAA and state law. Although the hospital had provided de-identified information, the plaintiff claimed Google could use the anonymized data, together with other information in its possession from patient use of Google products while in the hospital (like the Google search engine, Gmail and Google maps), to re-identify patients. The Seventh Circuit upheld dismissal on standing grounds, because the plaintiff failed to show either injury-in-fact from disclosure or that Google had taken steps to re-identify the patients. The case illustrates the risks for health care providers if a plaintiff can demonstrate actual harm from re-identification, and raises issues about the adequacy of current requirements and processes to protect patient privacy and confidentiality.

TJC/CHAI Joint Guidance on the Responsible Use of AI in Healthcare

In the face of these uncertainties, what's a healthcare provider to do? Several emerging frameworks provide guidance on strategies to protect patient information.

One of these resources is the September 2025 guidance from the Joint Commission (TJC) and the Coalition for Health AI (CHAI) on the responsible use of AI in healthcare.[29] The TJC/CHAI joint guidance contains a wealth of information on key elements for implementing clinical and administrative AI. These include: (i) AI policies and governance structures; (ii) patient privacy and transparency; (iii) data security and data use protections; (iv) ongoing quality monitoring; (v) voluntary, blinded reporting of AI safety-related events; (vi) risk and bias assessments; and (vii) education and training.

In the context of AI-enabled technology, the TJC/CHAI guidance suggests provisions for healthcare providers to consider in their data use agreements with vendors. These include, for example, using only the minimum necessary data for the specified purposes; clearly defining the permissible uses of exported data and prohibiting other uses; prohibiting the re-identification of de-identified data, and reserving the

right to audit third-party vendors for compliance and to impose penalties for non-compliance with data use agreements. The guidance also offers recommendations for processes to monitor and evaluate the safe performance of AI-enabled clinical tools.

As the regulatory landscape governing ambient listening and other AI tools evolves, adherence to these practices and other developing strategies may help providers sidestep legal, financial and reputational risks.

Conclusion

Ambient listening technologies offer enormous promise for reducing administrative burdens and improving documentation quality. Realizing the promise in a compliant manner will require a clear understanding of the capabilities and limitations of AI in the clinical setting, coupled with the use of contractual and systemic guardrails to reduce the potential for error and to protect patient data.

Jane Bello Burke, a partner at Hodgson Russ LLP, counsels health care providers and practitioners on a wide range of regulatory and compliance matters. She can be reached at JBBurke@hodgsonruss.com. This article originated as a presentation at the Health Law Section Fall 2025 Meeting in November 2025. The author gratefully acknowledges the contributions of William McMillan in the preparation of this article.

Endnotes

1. *See, e.g.*, Bobek, M., *Most common hospital EHR systems by market share*, Definitive Health care (May 7, 2025) (https://www.definitivehc.com/blog/most-common-inpatient-ehr-systems).
2. *See* Mess, SA, MD, Mackey, AJ, PhD, Yarowsky, DE, PhD, "Artificial Intelligence Scribe and Large Language Model Technology in Health care Documentation: Advantages, Limitations, and Recommendations, Plastic & Reconstructive Surgery-Global Open" (Jan. 2025), https://journals.lww.com/prsgo/fulltext/2025/01000/artificial_intelligence_scribe_and_large_language.31.aspx.
3. Automatic speech recognition (ASR) is the process and related technology for converting a speech signal into the matching sequence of words using algorithms implemented in computing devices. Fendji, J.L.K.E., Tala, D.C.M., Yenke, B.O., & Atemkeng, M., *Automatic Speech Recognition Using Limited Vocabulary: A Survey. Applied Artificial Intelligence,* 36(1) Applied Artificial Intelligence (2022), https://www.tandfonline.com/doi/full/10.1080/08839514.2022.2095039#abstract.
4. New York defines the term "AI model" as "a component of an information system that implements artificial intelligence technology and uses computational, statistical, or machine-learning techniques to produce outputs from a given set of inputs." N.Y. Gen. Bus. Law § 1700(3).
5. A large language model is a type of artificial intelligence designed to understand and generate human-like text based on the input it receives. For a non-technical explanation, *see* Stanford University IT, *AI Demystified: Introduction to Large Language Models*, https://uit.stanford.edu/service/techtraining/ai-demystified/llm).
6. *See* Topaz M., Peltonen L.M., Zhang Z., *Beyond Human Ears: Navigating the Uncharted Risks of AI Scribes in Clinical Practice,* 8(1) npj Digit. Med. 569 (Sept. 24, 2025), https://pmc.ncbi.nlm.nih.gov/articles/PMC12460601/pdf/41746_2025_Article_1895.pdf.
7. *See* Morreim, E.H., *Errors in the EMR: Under-Recognized Hazard for AI in Health care*, 24(1) Hous. J. Health L. & Policy 139-42 (2025).
8. *See* Özer, M., "Is Artificial Intelligence Hallucinating? Turk Psikiyatri Derg. 14;35(4):333–35. (Oct. 14, 2024), https://pmc.ncbi.nlm.nih.gov/articles/PMC11681264/.
9. *See* Belenguer, L., *AI Bias: Exploring Discriminatory Algorithmic Decision-Making Models and the Application of Possible Machine-Centric Solutions Adapted from the Pharmaceutical Industry*, AI Ethics 2, 771–87 (2022), https://pmc.ncbi.nlm.nih.gov/articles/PMC8830968/#Sec.
10. *See* Guan, H., Bates, D., Zhou, L., *Keeping Medical AI Healthy and Trustworthy: A Review of Detection and Correction Methods for System Degradation, arXiv preprint arXiv:2506.17442* (2025), https://arxiv.org/pdf/2506.17442.
11. *See* Bathaee, Y., *The Artificial Intelligence Black Box and the Failure of Intent and Causation,* 31(2) Harv. J. of L. & Tech. (Spring 2018), https://jolt.law.harvard.edu/assets/articlePDFs/v31/The-Artificial-Intelligence-Black-Box-and-the-Failure-of-Intent-and-Causation-Yavar-Bathaee.pdf.
12. *See* Hoffman, B., *Automation Bias: What It Is and How To Overcome It,* Forbes (Mar. 10, 2024), https://www.forbes.com/sites/brycehoffman/2024/03/10/automation-bias-what-it-is-and-how-to-overcome-it/.
13. *Compare* Exec. Order No. 14,110, *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence,* 88 Fed. Reg. 75191 (Oct. 30, 2023) (setting out eight guiding principles and priorities to advance the safe, secure and trustworthy development and use of AI), *with* Exec. Order No. 14,179, *Removing Barriers to American Leadership in Artificial Intelligence,* 90 Fed. Reg. 8741 (Jan. 23, 2025) (rescinding E.O. 14110 and emphasizing innovation to sustain and enhance America's global AI dominance and promote human flourishing, economic competitiveness, and national security). *See* White House, *Winning the Race: America's AI Action Plan* (Jul. 23, 2025), https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf (setting out an AI Action Plan with three pillars, innovation, infrastructure, and international diplomacy and security); Exec. Order No. 14,318, *Accelerating Federal Permitting of Data Center Infrastructure,* 90 Fed. Reg. 35385 (July 23, 2025) (to facilitate rapid and efficient buildout of the AI infrastructure by easing federal regulatory burdens); Exec. Order No. 14,319, "Preventing Woke AI in the Federal Government," 90 Fed. Reg. 35,389 (July 23, 2025) (to promote the innovation and use of "trustworthy AI" developed in accordance with the "Unbiased AI Principles" of "truth-seeking" and "ideological neutrality); Exec. Order No. 14,320, "Promoting the Export of the American AI Technology Stack," 90 Fed. Reg. 35393 (July 23. 2025) (to preserve and extend American leadership in AI and decrease international dependence on AI technologies developed by U.S. adversaries by supporting the global deployment of U.S.-origin AI technologies). *See also* Exec. Order No. 14,365, "Ensuring a National Policy Framework for Artificial Intelligence," 90 FR 58,499 (Dec. 11, 2025) (to develop a "minimally burdensome" national AI standard

to protect children, prevent censorship, respect copyrights, safeguard communities and preempt conflicting state laws).

14. For example, the Office for Civil Rights enforces federal patient privacy and security standards and the nondiscrimination requirements of Section 1557 of the Affordable Care Act. *See* 42 C.F.R. § 92.210 (prohibiting health care providers and plans from discriminating on the basis of race, color, national origin, sex, age, or disability in its health programs or activities through the use of patient care decision support tools and requiring them to make reasonable efforts to identify, and to mitigate, the risk of discrimination resulting from, the use of such tools); Department of Health and Human Services (HHS), Nondiscrimination in Health Programs and Activities Proposed Rule (Section 1557 of the Affordable Care Act), 89 Fed. Reg. 37522 (May 6, 2024). The Office of the National Coordinator for Health IT enforces certain provisions of the 21st Century Cures Act, including 45 C.F.R. Part 170, which requires certified health IT developers to provide transparency information about predictive decision support intervention tools and to engage in risk management practices. *See* "Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing" (the HTI-1 Final Rule), 89 Fed. Reg. 1192 (Jan. 9, 2024).

15. The Food and Drug Administration (FDA) issues guidance on the scope of FDA oversight of clinical decision support software in health care settings meeting the definition of medical device and requiring approval upon a demonstration of the device software function's safety and effectiveness. *See, e.g.*, "Clinical Decision Support Software Guidance for Industry and Food and Drug Administration Staff" (Jan. 6, 2026), https://www.fda.gov/media/109618/download.

16. 42 U.S.C. §§ 1320d–1320d-9, as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH), and the implementing regulations at 45 C.F.R. Part 160, 162 and 164.

17. A "covered entity" is a health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a HIPAA-covered transaction covered. 45 C.F.R. § 160.103 (definitions); *see* HHS Office for Civil Rights (OCR), *Covered Entities and Business Associates,* https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html).

18. Protected health information (PHI) means individually identifiable health information, except as provided in § 160.103(2) (regarding certain records), that is: (i) transmitted by electronic media; (ii) maintained in electronic media; or (iii) transmitted or maintained in any other form or medium. Individually identifiable health information, in turn, is information that is a subset of health information, including demographic information collected from an individual, and: (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) relates 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 (i) that identifies the individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual. 45 C.F.R. § 160.103 (definitions); *see* OCR website, "Summary of the HIPAA Privacy Rule*"*, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

19. A "business associate" is a person, other than a member of the covered entity's workforce, who (or entity that) performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. The Privacy Rule lists some of the functions or activities (including claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management; and repricing) and services (including legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; and financial) that make a person or entity a business associate, if the activity or service involves the use or disclosure of protected health information. *See* 45 C.F.R. § 160.103 (definitions); OCR website, "Business Associates" (https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html).

20. A BAA is a contract through which the covered entity obtains satisfactory assurances from a business associate that it will appropriately safeguard PHI. 45 C.F.R. § 164.502(e)(1).

21. The minimum necessary standard requires a covered entity or business associate to make reasonable efforts to limit requests or disclosures of protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. 45 C.F.R. §§ 164.502(b), 164.514(d); *see* OCR website, "Minimum Necessary Requirement" (https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/minimum-necessary-requirement/index.html).

22. Under HITECH and OCR's 2013 final rule, 78 Fed. Reg. 5566 (Jan. 25, 2013), OCR has authority to take enforcement action against business associates for certain HIPAA violations. *See* Direct Liability of Business Associates (https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/factsheet/index.html#:~:text=The%20Health%20Information%20Technology%20for%20Economic%20and,other%20persons%20for%20filing%20a%20HIPAA%20complaint**).

23. 45 C.F.R. §§ 164.502(a)(1)(ii), 164.506(c).

24. *See* 45 C.F.R. § 164.501 for the definition of treatment, payment and health care operations.

25. *See* 45 CFR § 164.508. When a covered entity obtains or receives a valid authorization for its use or disclosure of protected health information, the use or disclosure must be consistent with the authorization. 45 C.F.R. § 164.508(a)(1).

26. HIPAA offers two methods to de-identify information: (i) through a qualified, independent expert who uses generally accepted principles and methods to render information not individually identifiable; or (ii) through the removal of 18 specified identifiers, provided the covered entity does not have actual knowledge that the remaining information could be used alone or in combination with other information to identify the subject of the information. 45 C.F.R. § 164.514(b).

27. Under 45 C.F.R. § 164.514(a), "[h]ealth information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information."

28. 73 F.4th 502 (7th Cir. 2023).

29. TJC and CHAI, "The Responsible Use of AI in Health care" (Sept. 2025) (https://digitalassets.jointcommission.org/api/public/content/dcfcf4f1a0cc45cdb526b3cb034c68c2?v=3edb8a95&_gl=1*56oxrn*_gcl_au*MzU4MDg2NTkuMTc2ODg4NDMzNg..*_ga*MTc0NDY4NDA2Ni4xNzY4ODg0MzM2*_ga_K31T0BHP4T*czE3Njg4ODQzMzYkbzEkZzAkdDE3Njg4ODQzMzYkajYwJGwwJGgw).