THE USE OF ARTIFICIAL INTELLIGENCE IN HUMAN SUBJECT RESEARCH: PRIVACY RISKS, LEGAL IMPLICATIONS, AND ETHICAL CONSIDERATIONS

Rebecca Siviglia, Esq.*

TABLE OF CONTENTS

 J.D., Florida State University College of Law, 2015; B.S., Florida State University, 2011. The author serves as Assistant General Counsel at Moffitt Cancer Center, an NCI-designated comprehensive cancer center and research institute, where she specializes in life sciences, data privacy, and regulatory and compliance matters. The opinions expressed in this Article are hers alone. The content herein is drawn from the author's research and expertise. This Article in no way reflects the views or perspectives of the author's employer. This Article is not designed to offer any legal, regulatory, compliance, or professional advice. The author would like to thank the many individuals that helped make this paper a reality, especially family, friends, colleagues, and the staff of the Stetson Business Law Review. This Article is dedicated to cancer patients, physicians, researchers, and those within the cancer community who are fighting for a world in which cancer no longer exists.

INTRODUCTION

For industries such as healthcare and human subject research, which have leveraged forms of artificial intelligence ("AI") for decades, the recent call to action for the utilization of AI is nothing new.[1] However, Generative AI is a more novel concept that renews discussions and concerns about data privacy, specifically around the use and protection of sensitive data.[2] Generative AI has led to an influx of new AI systems that require unprecedented amounts of data to operate effectively, and when implemented successfully, have the potential to enhance clinical care and treatment outcomes.[3] Additionally, Generative AI has lowered the costs of many AI systems, thereby increasing accessibility to a broader range of users.[4] The use of AI also has possible monetary benefits, including the opportunity to lower costs associated with healthcare and human subject research, while driving efficiency and research forward; Generative AI will be an estimated 1.3 trillion dollar market across industries by 2032.[5] With the advances and accessibility of Generative AI, important questions have been renewed about the potential risks of using AI systems within human subject research, particularly around data privacy protections, patient consent requirements, ethical considerations, and legal implications.[6]

To address and analyze these issues, this Article provides a summary of the guidance issued by federal government agencies on the use of AI when interacting with sensitive data, focusing on Generative AI and traditional forms of AI, such as machine learning and federated learning. This Article will discuss the various applicable privacy concerns and risks, which are partially

1. NORA WELLS ET AL., CONG. RSCH. SERV., R48319, ARTIFICIAL INTELLIGENCE (AI) IN HEALTH CARE 3 (2024).

2. *Strategic Plan for the Use of Artificial Intelligence in Health, Human Services, and Public Health*, U.S. DEP'T OF HEALTH & HUM. SERVS. 6, 28 (2025), https://irp.nih.gov/system/files/media/file/2025-03/2025-hhs-ai-strategic-plan_full_508.pdf [https://perma.cc/4RJT-UJAJ] [hereinafter U.S. DEP'T OF HEALTH & HUM. SERVS.].

3. *See* Sandeep Reddy, *Generative AI in Healthcare: An Implementation Science Informed Translational Path on Application, Integration and Governance*, 19 IMPLEMENTATION SCI. 27, 1–3 (2024), https://implementationscience.biomedcentral.com/counter/pdf/10.1186/s13012-024-01357-9.pdf [https://perma.cc/UBJ3-HQ28].

4. *See* Nicola Jones, *Where AI Is Now: Smaller, Better, Cheaper Models*, NATURE MAG.: SCIENTIFIC AMERICAN (April 9, 2025), https://www.scientificamerican.com/article/ai-report-highlights-smaller-better-cheaper-models/ [https://perma.cc/L4TC-ANZP].

5. U.S. DEP'T OF HEALTH & HUM. SERVS., *supra* note 2, at 6, 11.

6. *See id.* at 11–12, 28, 38.

due to gaps in laws and regulations, such as lack of transparency or understanding, the likelihood of re-identification, bias and discrimination, the nature of the black box, and the consequences of using inaccurate source data and subsequent output. This Article will discuss the concept of consenting to the use of AI systems when sensitive data is involved, including when consent may be necessary, what factors should be considered to ensure that consent has been properly obtained, and whether there is any opt-out opportunity. Finally, this Article will discuss potential mitigating techniques to minimize risk, such as transparency, validation, training and education, the use of de-identified data or a limited data set, and best practices for entities and researchers to promote the responsible use of AI.

Before discussing the use of AI within human subject research, a few important aspects of this topic should be acknowledged. AI has existed for several decades, with various forms, adaptations, uses, and concepts.[7] This Article will predominantly discuss the use of Generative AI, which is an AI system capable of creating original content in response to prompts.[8] This Article will also remark on the use of machine learning and federated learning: AI systems that learn from data without being explicitly programmed.[9] Various forms of AI systems may be used for analyzing source data to develop output; the use of AI may vary, from development of algorithms and models, to creating decision trees for personalized medical treatment.[10] This Article focuses on the generalized risks associated with the use of sensitive data within human subject research and will not identify or cover every potential AI system that is used. This Article will focus on such risks as they apply to users, researchers, developers, participants, and "entities," which may include academic medical centers, research institutions, or hospital systems. This Article focuses specifically on U.S. law and does not address the European Union's General Data Protection Regulations ("GDPR"), which add

7. *Id.* at 6.

8. *Id.*

9. *See id.* at 183, 185; *Responsible Oversight of Artificial Intelligence for Clinical Research Professionals*, ASS'N OF CLINICAL RSCH. PROS. 5 (Jan. 2025), https://acrpnet.org/responsible-oversight-of-artificial-intelligence-for-clinical-research-professionals [https://perma.cc/23RT-CEFH].

10. *See, e.g.*, U.S. DEP'T OF HEALTH & HUM. SERVS., *supra* note 2, at 50–60, 72, 86–87, 115–123, 141–150.

an additional layer of regulations regarding potential data privacy risks, particularly involving data processing.[11] Finally, by the time this Article is published, it is more than likely that supplementary guidance will be issued by applicable federal government agencies and additional considerations will be in place for the use of AI within human subject research.

FEDERAL GOVERNMENT AGENCY REGULATIONS AND GUIDANCE

To date, agencies such as Health and Human Services ("HHS") and the Office of Human Research Protections ("OHRP") have provided minimal guidance on how sensitive data should be used when interacting with AI systems.[12] Given the rapid advancements in AI and the importance of data privacy, there is a need for more guidance to ensure participant data is properly protected.[13] Presently, to understand how sensitive data should be used responsibly within the AI landscape, an entity must rely on existing data privacy and ethical research guidance to establish use parameters.[14] In 1974, the National Research Act[15] was signed into law, which established the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research (the "Commission").[16] The charge of the Commission was to outline "basic ethical principles that should underlie the conduct

11. *Data Protection Under GDPR*, EUROPA (Mar. 3, 2025), https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_en.htm [https://perma.cc/XXU4-Y4PB].

12. *See* Allison Trimble, *Research Involving Artificial Intelligence — Considerations for Academic Medical Centers*, AM. HEALTH L. ASS'N (Nov. 20, 2024), https://www.americanhealthlaw.org/content-library/publications/briefings/299298b9-da2e-4a48-a457-8d0f11e57818/research-involving-artificial-intelligence-conside [on file with the *Stetson Business Law Review*].

13. *See* Sec'y Advisory Comm. on Hum. Rsch. Prots., *IRB Considerations on the Use of Artificial Intelligence in Human Subjects Research,* U.S. DEP'T OF HEALTH AND HUM. SERVS. (Oct. 19, 2022), https://www.hhs.gov/ohrp/sachrp-committee/recommendations/irb-considerations-use-artificial-intelligence-human-subjects-research/index.html [https://perma.cc/TD7Y-2VX5].

14. *See id.*

15. BELMONT REPORT: ETHICAL PRINCIPLES AND GUIDELINES FOR THE PROTECTION OF HUMAN SUBJECTS OF RESEARCH, Report of the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 44 Fed. Reg. 23191, 23192 (Apr. 18, 1979) (to be codified at 45 C.F.R. pt. 46).

16. *Id.*

of biomedical and behavioral research involving human subjects."[17] The Commission was asked to consider

> (i) the boundaries between biomedical and behavioral research and the accepted and routine practice of medicine, (ii) the role of assessment of risk-benefit criteria in the determination of the appropriateness of research involving human subjects, (iii) appropriate guidelines for the selection of human subjects for participation in such research and (iv) the nature and definition of informed consent in various research settings.[18]

This Act has become commonly known as the Belmont Report.[19]

The Commission evaluated the gray areas between medical practice and human subject research, determining that if there is any element of research in a project, that activity should undergo review for the protection of human subjects.[20] The Commission went on to discuss the choices of an individual person, determining that individuals should enter into research voluntarily and with enough information to make such a decision regarding participation.[21] The Commission discussed the patient consent process, which should include a consent form that provides detailed information, is comprehensible, and expresses that participation is voluntary.[22] Finally, there is a risk-benefit analysis that should take place as to whether the risks associated with the proposed research may ultimately produce a larger, long-term benefit.[23]

Following the Belmont Report, the Federal Policy for the Protection of Human Subjects ("Common Rule") was published in 1991, which established ethical standards and procedures for federally funded research involving human participants; specifically, the Common Rule outlines requirements for informed consent and the need for Institutional Review Board ("IRB") review

17. *Id.*
18. *Id.*
19. *Id.*
20. *See id.* at 23193.
21. *See id.* at 23195.
22. *See id.*
23. *See id.* at 23196.

and approval.[24] The Common Rule also has certain exemptions, which are research activities that meet specific requirements and, therefore, may not require informed consent or full IRB oversight.[25] In determining whether the Common Rule applies to research activities, including those involving AI systems, an entity must determine if the research is a "systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge."[26] This system has become a general standard when evaluating if research activities fall under the Common Rule.[27]

In 2022, HHS provided guidance regarding the use of technology within human subject research; the Secretary's Advisory Committee on Human Research Protection ("SACHRP") evaluated the use of human subject data and determined that if the data collection is mentioned within a protocol explicitly, it would fall under the Common Rule's definition of research.[28] However, SACHRP acknowledged that although data may be collected initially for non-research purposes, the secondary use of such data may fall under a Common Rule exemption, specifically 45 C.F.R. 46.104(d)(4), which outlines the exemptions for secondary research using identifiable data or biospecimens.[29] SACHRP acknowledged that because the activity would fall under the Common Rule exemption, participants may not be adequately protected and there may be a lack of transparency surrounding how the data will be used.[30] Participants may not provide the same authorization for subsequent use of their data if they were provided full transparency about the possible uses of their information.[31] As it applies to AI technology, SACHRP determined that such research activities could fall under the Common Rule exemptions, thereby not requiring consent or full IRB approvals; however, there may be circumstances where a research activity, such as AI validation, is not "designed to develop or contribute to the generalizable knowledge", but the underlying intent goes

24. Basic HHS Policy for Prot. of Hum. Rsch. Subjects, 45 C.F.R. § 46.101–46.124 (2025); *see* Trimble, *supra* note 12.
25. Exempt Research, 45 C.F.R. § 46.104 (2025).
26. *See* Trimble, *supra* note 12.
27. *Id.*
28. *See* Sec'y Advisory Comm. on Hum. Rsch. Prots., *supra* note 13.
29. *Id.*; Exempt Research, 45 C.F.R. § 46.104(d)(4) (2025).
30. *See* Sec'y Advisory Comm. on Hum. Rsch. Prots., *supra* note 13.
31. *See id.*

beyond just validation and may require full regulatory oversight.[32] Following SACHRP's evaluation, SACHRP provided several recommendations to HHS: reexamination of the meaning of identifiability in response to new technology and research activities; revisions to the Common Rule definition of human subject; and providing formal guidance on the potential harms caused by inherent bias.[33]

An exploratory workshop held by HHS in September 2024, "The Evolving Landscape of Human Research with AI - Putting Ethics in Practice," discussed whether activities involving AI systems utilized under a research project would fall under the Common Rule.[34] The workshop broadly covered the use of AI within human subject research and the potential legal and ethical considerations.[35] Presenters during the workshop discussed the increased likelihood of re-identification; combining high volumes of data with technical advancements creates the opportunity for recognized patterns, as well as AI's ability to connect information from various different sources.[36] The presenters also acknowledged the potential serious privacy, confidentiality, and transparency challenges, as well as the possibility that IRBs may not be equipped to determine whether an activity meets the definition of human subject research.[37] The general consensus of the workshop participants was that the use of AI systems within human subject research is growing rapidly, with minimal guidance from federal government agencies on how to approach concerns and potential risks.[38]

More recently, the National Institute of Standards and Technology ("NIST") updated its Privacy Framework to meet privacy risk management needs and provided information on the

32. *See id.*
33. *See id.*
34. *See* Trimble, *supra* note 12; Eric Mah, Ed.D., M.H.S. & Benjamin C. Silverman, M.D., *The Evolving Landscape of Human Research with AI–Putting Ethics to Practice, 2024 Exploratory Workshop* (Sep. 19, 2024), https://www.hhs.gov/sites/default/files/ohrp-exploratory-workshop-summary-report-2024.pdf [https://perma.cc/9ABB-6ALU].
35. *See* Benjamin M. Zegarelli & Pat G. Ouellette, *OHRP Workshop Highlights Artificial Intelligence Uses, Concerns in Human Research*, MINTZ (Oct. 9, 2024), https://www.mintz.com/insights-center/viewpoints/2791/2024-10-09-ohrp-workshop-highlights-artificial-intelligence-uses [https://perma.cc/68XQ-J3SR].
36. *See id.*
37. *See id.*
38. *See id.*

use of AI.[39] NIST stated that AI systems "are engineered or machine-based systems that can, for a given set of objectives, generate outputs such as predictions, recommendations, or decisions influencing real or virtual environments."[40] NIST acknowledged that "[p]rivacy risks can arise . . . when AI systems are trained on data that was collected without individuals' consent or have missing or inadequate safeguards."[41] NIST also discussed the possibility of re-identification and human-cognitive biases, while recognizing the potential for physical and economic harms associated with the use of AI.[42] Although NIST did not directly reference Protected Health Information ("PHI") or human subject research, the Privacy Framework established by NIST discusses mitigating tactics that could be applied to such use of AI systems and sensitive data, including monitoring and review, being cognizant of privacy risks and concerns, de-identification techniques, data minimization, and implementation of user controls.[43] Entities are recommended to utilize NIST's Privacy Framework as a method to "manage AI risks and promote trustworthy and responsible development and use of AI systems."[44]

Additional federal guidance on AI appears in HHS's Strategic Plan for the Use of Artificial Intelligence in Health, Human Services, and Public Health, released on January 10, 2025.[45] HHS acknowledged the significant presence and development of AI within the healthcare industry and the potential economic opportunities, while also noting the need for responsible use of AI based on the level of risks associated with using sensitive data.[46] Under the current administration, HHS did not move forward with this existing Strategic Plan; on January 23, 2025, the current administration signed Executive Order 14179, titled "Removing Barriers to American Leadership in Artificial Intelligence."[47]

---

39. *See NIST Privacy Framework 1.1*, NAT'L INST. OF STANDARDS & TECH. 1 (Apr. 14, 2025), https://doi.org/10.6028/NIST.CSWP.40.ipd [https://perma.cc/868X-NFW3] [hereinafter NAT'L INST. OF STANDARDS & TECH.].

40. *Id.* at 7.

41. *Id.*

42. *See id.*

43. *See id.* at 8.

44. *Id.*

45. *HHS Releases Strategic Plan on AI*, AM. HOSP. ASS'N. (Jan. 10, 2025, at 15:38 ET), https://www.aha.org/news/headline/2025-01-10-hhs-releases-strategic-plan-ai [https://perma.cc/H5Q2-A27W].

46. *See* U.S. DEP'T OF HEALTH & HUM. SERVS., *supra* note 2, at 6–8.

47. Exec. Order No. 14179, 90 Fed. Reg. 8741 (Jan. 31, 2025).

Although not specific to healthcare, this Executive Order referenced the use of AI to carry out basic research or applied research as being within scope and applies to all federal government agencies, calling for the development of documented AI strategies.[48]

Despite federal government agencies providing some guidance on the utilization of AI within clinical healthcare settings and clinical trials, there remains a gap when it comes to human subject research.[49] It is important to recognize that there have been minimal updates to the research ethical framework since the establishment of the Belmont Report, despite efforts from the healthcare and research communities.[50] Utilization of AI within human subject research remains a complicated area of risk, partially due to the lack of guidance from federal government agencies and a general deficiency of applicable laws and regulations.[51] Some states have turned to implementing their own legislation to address privacy concerns regarding AI; however, these variations in state law may create additional regulatory confusion.[52] Therefore, there likely will be additional calls to action to address the existing gaps in regulation and provide entities with more insight on responsibly using AI within human subject research.[53]

RISKS ASSOCIATED WITH AI WITHIN HUMAN SUBJECT RESEARCH

Before delving into the potential risks associated with AI, it is important to discuss the benefits of using AI within human subject research. AI allows for the advancement of basic research through

48. *See id.*

49. *See* Renée E. Pierre-Louis & Paul F. Franco, *Preparedness of Health Systems for AI Adoption in Research: Are Compliance Officers Ready?,* COMPLIANCE TODAY, Nov. 2024, at 1.

50. *See id.*

51. *See id.* at 4.

52. *See* Katherine Grillaert, Matt Kennedy & Chinasa T. Okolo, *Risks of State-Led AI Governance in a Federal Policy Vacuum*, TECHPOLICY PRESS (Feb. 6, 2025), https://www.techpolicy.press/risks-of-state-led-ai-governance-in-a-federal-policy-vacuum/ [https://perma.cc/D7FS-YCAW]; David Peloquin, Senior Counsel at Cleveland Clinic, Gregory Stein, Partner Ropes & Gray LLP, & Allison Trimble, Associate General Counsel BJC Health System, *Privacy Strategies for AI: Enabling Global Health Innovation in Research and AI*, Am. Health L. Ass'n Conf. (Feb. 5, 2025).

53. *See* Pierre-Louis & Franco*, supra* note 49, at 4.

the processing of significant amounts of data and images in real time, which can result in discovering links between disease and treatment, as well as identifying previously unrecognizable patterns that can assist with clinical treatment.[54] From a business perspective, the development of AI within research is thriving, with the possibility to fund future research initiatives and drive innovation.[55] The widespread availability of AI provides researchers with an additional resource, allowing for the progression of new inventions while lowering general operating costs.[56] Potentially the most important factor about AI is that it accelerates timelines for human subject research, which allows for the possibility of providing greater access to healthcare for individuals.[57] AI may allow for testing, evaluating, and analyzing a population that would otherwise be difficult to study or has limited access to care.[58] Finally, federal government agencies have acknowledged the widespread potential for AI's application with human subject research, recognizing the impact it may have in clinical research and drug development.[59]

Although the use of AI within human subject research is invaluable, leading to increased innovation, discoveries, and future treatment breakthroughs, such use of AI also comes with various risks to entities, researchers, users, developers, and most importantly, the participants.[60] This section will evaluate some of the risks associated with AI and human subject research, including privacy concerns, consent requirements, bias and discrimination, and hallucinations and inaccuracies, with the intent of bringing these considerations to light for parties involved in such research. This section will also highlight potential mitigation strategies, as well as lay the foundation for discussions on best practices.

54. *See id.* at 3.
55. *See* U.S. DEP'T OF HEALTH & HUM. SERVS., *supra* note 2, at 5.
56. *See id.* at 22.
57. *See id.* at 23.
58. *See* Diana Bae & Jooyoung Jeon, *Understanding Artificial Intelligence with the IRB: Impacts in Research*, TCHRS. COLL. IRB BLOG (Apr. 23, 2024), https://www.tc.columbia.edu/institutional-review-board/irb-blog/2024/understanding-artificial-intelligence-with-the-irb-impacts-in-research/ [https://perma.cc/M45R-YH88].
59. *See* Pierre-Louis & Franco, *supra* note 49, at 1.
60. *See id.* at 4, 6–7; U.S. DEP'T OF HEALTH & HUM. SERVS., *supra* note 2, at 173–74.

A. Privacy

Entities subject to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") are held to a high regulatory and compliance standard when it comes to utilizing large amounts of data, specifically sensitive, personal, and identifiable information, such as PHI, within human subject research.[61] If the application of data in an AI system constitutes a use or disclosure of PHI by a covered entity, then the activity must be permitted under HIPAA.[62] These covered entities can only use such data for particular purposes under HIPAA, such as research, which may require that the data be de-identified or in the form of a limited data set.[63] As part of HIPAA's Safe Harbor method, de-identification of data requires that any identifying elements, as defined by HIPAA, be removed from the dataset, which may allow for more flexibility in how the data can be used.[64] Alternatively, the dataset may be considered a limited data set, in which some, but not all, of the identifiable information has been removed as defined by HIPAA.[65]

In addition to the removal of identifiers, an entity may be required to obtain authorization or waiver of authorization following review of the research activity by an IRB or privacy board.[66] If a HIPAA-covered entity intends to use data for purposes of human subject research and the research does not qualify for a waiver, the entity should obtain voluntary and informed consent.[67] This is assuming the data is collected as part of the research itself and is not considered secondary use, thus falling under the

61. *See* Peloquin, Stein & Trimble, *supra* note 52; Trimble, *supra* note 12.

62. *See* Peloquin, Stein & Trimble, *supra* note 52.

63. *See id.*; *How Can Covered Entities Use and Disclose Protected Health Information for Research and Comply with the Privacy Rule?*, U.S. DEP'T OF HEALTH AND HUM. SERVS. NAT'L INST. OF HEALTH (Feb. 2, 2007), https://privacyruleandresearch.nih.gov/pr_08.asp [https://perma.cc/LR5G-324J] [hereinafter U.S. DEP'T OF HEALTH AND HUM. SERVS. NAT'L INST. OF HEALTH].

64. *See* Peloquin, Stein & Trimble, *supra* note 52; Security and Privacy, 45 C.F.R. § 164.514(b)(2) (2025).

65. *See* Peloquin, Stein & Trimble, *supra* note 52.

66. *See id.*; U.S. DEP'T OF HEALTH AND HUM. SERVS. NAT'L INST. OF HEALTH, *supra* note 63.

67. *See* Trimble, *supra* note 12, at 2; Gen. Requirements for Informed Consent, 45 C.F.R. § 46.116 (2025).

Common Rule exemptions.[68] Regarding compliance, entities may consider whether its IRBs or privacy boards have standard operating procedures to facilitate reviewing studies involving AI and providing guidance to study personnel and participants to ensure consent has been properly obtained.[69] IRBs and privacy boards may need to consult with AI experts prior to making certain determinations, similar to ancillary review committees.[70]

Using de-identified data per HIPAA's Safe Harbor reduces potential risks when AI is involved, although entities should still be aware of the likelihood of re-identification.[71] In its guidance on human subject research and technology, SACHRP stated "[r]emoval of identifiers no longer means that individuals cannot be identified, nor does it mean that private and sensitive information will not be disclosed and potentially connected back to the individual in the future. That risk should be explicitly disclosed."[72] Although utilizing de-identified data minimizes potential risk, if the data is aggregated with publicly available information or datasets which contain similar variables, there could be an increased likelihood of re-identification.[73] SACHRP also raised an important distinction in the use of machine learning: the goal of these applications is to "infer novel or undisclosed information about such individuals."[74] This distinction supports the likelihood of potential re-identification, even with traditional forms of AI.[75] AI systems that involve machine learning or federated learning, which allow greater control over how the data is accessed and used within an AI setting, may be considered in lieu of a large language model ("LLM"), open source, or some form of Generative AI.[76] However, it may not always be feasible that the

68. *See* Sec'y Advisory Comm. on Hum. Rsch. Prots., *supra* note 13; Exempt Research, 45 C.F.R. § 46.104 (2025).

69. *See Guidance on the Use of AI in Human Subjects Research*, U. OF TENN., https://research.utk.edu/research-integrity/artificial-intelligence-ai-tools/ [https://perma.cc/C2XP-GSSM] (last visited Oct. 27, 2025).

70. *See id.*

71. *See* Sec'y Advisory Comm. on Hum. Rsch. Prots., *supra* note 13.

72. *Id.*

73. *See Guidance: Using Artificial Intelligence During Research Activities,* VA. TECH RSCH. INNOVATION: SCHOLARLY INTEGRITY & RSCH. COMPLIANCE 4 (Feb. 13, 2024), https://www.research.vt.edu/content/dam/research_vt_edu/sirc/files/sirc-guidance-for-ai.pdf [https://perma.cc/KAK5-4ZWM].

74. *See* Sec'y Advisory Comm. on Hum. Rsch. Prots., *supra* note 13.

75. *See id.*

76. *See* Trimble, *supra* note 12, at 2; Francesco Piccialli, et al., *Federated and Edge Learning for Large Language Models,* 117 INFO. FUSION 1, 6 (2025).

research can be accomplished using a more developed, longstanding form of AI and, ultimately, the risks associated with re-identification remain.[77] Other potential mitigating factors include only using de-identified data during model training or encrypting the data during any form of subsequent transfer.[78] Finally, entities should explore whether the AI system allows for parameters or limitations to be placed on the analyzed data, such as eliminating or minimizing demographic information or data that can be easily re-identifiable.[79] Additionally, if the research activity is questionable because of the likelihood of re-identification, a solution to mitigate potential risk is to obtain consent.[80]

To maintain ethical practices, entities may consider maintaining a level of transparency with their data subjects and participants.[81] When considering what steps need to be taken to promote transparency with participants, entities should review the applicable consent forms.[82] The consent form should include, in lay terms, a clear description of the research project, how the participant's data will be used, and what rights the participant is granted when participating in the research activity.[83] The consent should reasonably explain the potential risks associated with participation, such as loss of privacy or confidentiality.[84] Additionally, the consent should highlight who may have access to the data; if it is unclear to the AI user, then information could be provided as to the owner or developer of the AI system.[85] The overall goal is to allow the participants to make individual, informed determinations about whether to participate in the research activity.[86]

---

77. *See* Trimble, *supra* note 12, at 2.

78. *See Responsible Oversight of Artificial Intelligence for Clinical Research ProfessionalsProfessionals*, *supra* note 9, at 11.

79. *See Guidance on the Use of AI in Human Subjects Research, supra* note 69.

80. *See* Sec'y Advisory Comm. on Hum. Rsch. Prots., *supra* note 13.

81. *See WMA Declaration of Helsinki-Ethical Principles for Medical Research Involving Human Participants*, WORLD MED. ASS'N. 2 (2024), https://www.wma.net/policies-post/wma-declaration-of-helsinki-ethical-principles-for-medical-research-involving-human-subjects/ [https://perma.cc/3429-8GBN].

82. *See id.* at 4–5.

83. *See id.*

84. *See Guidance: Using Artificial Intelligence During Research Activities, supra* note 73, at 4.

85. *See id.* at 3.

86. *See Guidance on the Use of AI in Human Subjects Research, supra* note 69.

The consent form should delineate whether the participant's data could be removed from the AI system.[87] If the data can be removed, the consent form may outline a process for requesting the data to be removed and various timelines for removal, in line with applicable laws.[88] The participant should also be informed if the data cannot be removed, how it could be used in the future, and whether the data may be aggregated with other data or output.[89] If the data was used as training data for development of algorithms or models, there is a high likelihood that the data cannot be fully removed, which should be communicated to the participant.[90] If a participant has any questions surrounding how the data will be used, the research organizers may provide additional information to the participant regarding the scope of the study.[91] These considerations also ensure that the entity has a full understanding of how the data will be used, who has access to the data, and how it should be protected.[92]

Privacy concerns surrounding the use of AI with large datasets for research, validation, and quality purposes are not entirely new; rather, they are variations on longstanding issues related to privacy rights.[93] However, the rapid advancement of AI within human subject research has put stress on our privacy laws and practices.[94] Entities should do their best to implement standard compliance practices that align with HIPAA to ensure that the confidentiality and anonymity of its participants in a research activity are protected.

B. Black Box

The concept of the black box creates uncertainty concerning intellectual property, ownership, privacy, and the need to obtain consent.[95] The general concept of the black box is that training data is fed into an AI system that is developed in such a way that makes it difficult to readily identify or explain how the output is

87. *See id.*
88. *See WMA Declaration of Helsinki-Ethical Principles for Medical Research Involving Human Participants, supra* note 81, at 5.
89. *See id.*
90. *See* Zegarelli & Ouellette, *supra* note 35.
91. *See Guidance on the Use of AI in Human Subjects Research, supra* note 69.
92. *See id.*
93. *See* Daniel J. Solove, *Artificial Intelligence and Privacy*, 77. FLA. L. REV. 1, 1 (2025).
94. *Id.* at 26.
95. *See* Trimble, *supra* note 12, at 2.

generated.[96] When applied to human subject research, this causes complications for numerous reasons when there is a lack of understanding as to how the data is being utilized and, ultimately, results in an entity having little to no control over the data.[97] Many entities may find it difficult to obtain a valid and full explanation from the original developer or owner of the AI system as to what exactly is occurring within the black box.[98] This is typically because the developer or owner wants to protect the application and development of the model.[99] To mitigate risk, entities should, to the best of their abilities, ensure that they have an understanding of how the data is being processed or utilized, what is being developed, and what ownership rights exist or can be argued if the entity is providing the source of the data that contributes to the generation, development, or expansion of the model.[100]

Utilization of a black box also creates issues when it comes to obtaining informed consent.[101] Communicating how participants' data is used within the AI system may be difficult if the entity does not have a full understanding or explanation regarding what activities are occurring within the black box.[102] If an entity is not able to obtain all information needed regarding the black box, a good course of action is to be as transparent as possible in the consent form or provide as much information to the participant that is available to the entity.[103] Ongoing debate remains regarding the levels of transparency that should be provided when a black box is used; entities may consider a risk-benefit analysis approach, weighing the benefits of access to the output generated versus the lack of transparency, potential issues with consent, and overall inability to fully control how the data is used.[104]

---

96. *See id.*

97. *See id.*

98. *See* Matthew Kosinski, *What is Black Box Artificial Intelligence (AI)?*, IBM, https://www.ibm.com/think/topics/black-box-ai [https://perma.cc/M3GZ-GJFQ] (last visited Nov. 2, 2025).

99. *See id.*

100. *See Guidance: Using Artificial Intelligence During Research Activities, supra* note 73, at 4.

101. *See* Trimble, *supra* note 12, at 2.

102. *See id.*; Solove, *supra* note 93, at 18–19.

103. *See* Glenn Cohen, *Informed Consent and Medical Artificial Intelligence: What to Tell the Patient?*, 108 GEO. L.J. 1425 (2020).

104. *See id.*

C. Bias and Discrimination

A primary concern when inputting data in an AI system is whether the output will accurately reflect the true data population.[105] An AI system may include bias or discrimination into its decision-making process, thereby creating inaccuracies within the output.[106] Further, if a research activity involves data specific to health inequities or social outcomes, the likelihood that bias may impact the output is significantly higher.[107] There are also inherent biases to consider, such as historical and representation biases.[108] Historical or systemic biases that exist in a society may be integrated into data historically, and when that data is fed to AI models, the AI outputs reflect and perpetrate those human biases.[109] Representation bias, also known as statistical computational bias, exists because of an over-representation of certain groups, with an under-representation of the true population.[110] Finally, there is a potential for human bias, either intentional or unintentional.[111] Additionally, because AI systems identify patterns that may not be readily apparent, they may reproduce bias unrecognized within the source data and inadvertently affect the resulting output.[112] Given these potential biases, the human subject research community has extensively discussed this issue and, subsequently, turned to federal government agencies for guidance to ensure responsible use of AI.[113]

In 2022, HHS tasked SACHRP with responding to questions and concerns regarding potential bias and flaws in the use of AI in research, in addition to addressing how IRBs should consider these risks during their review process.[114] SACHRP recognized two important factors: First, that there may be unrecognized bias within a dataset, which is the result of systemic bias and

105. *See Datasets, Bias, and Discrimination*, UNIV. OF TORO. LIBRS. (Aug. 21, 2025), https://guides.library.utoronto.ca/c.php?g=735513&p=5297043 [https://perma.cc/9LE7-EALY].
106. *See id.*
107. *See id.*
108. *See id.*
109. *See id.*; NAT'L INST. OF STANDARDS & TECH., *supra* note 39, at 7.
110. *See Datasets, Bias, and Discrimination*, *supra* note 105.
111. *See id.*
112. *See* Solove, *supra* note 93, at 49.
113. *See* Andrew Tutt, *An FDA for Algorithms,* 69 ADMIN. L. REV. 83, 83 (2017).
114. *See* Sec'y Advisory Comm. on Hum. Rsch. Prots., *supra* note 13.

discrimination, and, therefore, the end result would not accurately represent the population to which scientific conclusions are drawn;[115] Second, that the preparation of the initial dataset may have been done separately from the research activity and, therefore, researchers may be unaware of potential biases in the source data.[116] SACHRP recommended HHS establish mechanisms to facilitate conversations about how the "interests of groups predictably affected by AI research might be considered and protected, consistent with maintaining scientific integrity."[117] SACHRP also recommended that HHS adopt regulations and provide guidance to address the matter.[118] These recommendations resulted in the 2024 Final Rule implementing Section 1557 of the Patient Protection and Affordable Care Act, which protects against bias in health care algorithms and requires users to employ reasonable efforts to mitigate the risk of discrimination.[119]

Many resources discuss potential ways to mitigate the risk of bias and discrimination, acknowledging the difficulty or potential impossibility of eliminating it entirely; the determination then becomes based on a risk-benefit analysis.[120] Regarding concerns about the accuracy of the source data due to biases, one potential practice for entities is to encourage researchers to be involved in the initial collection of the source data.[121] Alternatively, a summary of the data could be provided to the researcher prior to being put into an AI system, allowing for greater familiarity with the data points and elements.[122] Entities may encourage researchers to document their efforts to understand the data, especially if they were not the original data collector, for purposes of validating the data and identifying potential biases.[123] Several ways to validate the data may exist, such as verifying that the

115. *See id.*
116. *See id.*
117. *Id.*
118. *See id.*
119. Nondiscrimination in Health Programs or Activities, 45 C.F.R. § 92.1(a)-210 (2024).
120. *See* Sec'y Advisory Comm. on Hum. Research Prots., *supra* note 13; Bae & Jeon, *supra* note 58.
121. *See* Sec'y Advisory Comm. on Hum. Research Prots., *supra* note 13; *Guidance: Using Artificial Intelligence During Research Activities, supra* note 73, at 4.
122. *See* Sec'y Advisory Comm. on Hum. Research Prots., *supra* note 13; *Guidance: Using Artificial Intelligence During Research Activities, supra* note 73, at 4.
123. *See Guidance: Using Artificial Intelligence During Research Activities, supra* note 73, at 4.

output aligns with the source data and accurately reflects the proposed or expected outcome.[124] Efforts to validate the data and document the process mitigate potential risk of bias and discrimination and protect outcomes for future research.[125]

Another method to mitigate risk and deter potential biases within the source data and output is regular evaluation and audit of an AI system.[126] For example, in developing protocols, researchers may include or outline a process in which they intend to monitor for potential biases while using the AI system.[127] Another possible form of mitigation is to diversify the training data to limit the likelihood of bias.[128] If there is any bias or discrimination identified, the users should consider replicating the analysis or removing some of the initial data elements to increase the quality of the output.[129] This process would also avoid an inherent risk of future users relying on the output for research purposes without recognizing or having any knowledge of the potential quality concerns.[130] Finally, it is the responsibility of the researcher to review the source data and output to validate the quality of the data and eliminate any potential risks of bias and discrimination.[131]

D. Inaccuracy of the Data

While AI systems can greatly enhance human subject research through increased efficiency and automation, they can also raise concerns about the accuracy of generated data, as there is currently no established standard to ensure precise results.[132] However, it is commonly known that if the initial source data is inaccurate, the output will also be inaccurate.[133] This is because AI output "is only as accurate as its training data."[134] The result of

124. *See id.*
125. *See id.* at 3–5.
126. *See Guidance on the Use of AI in Human Subjects Research, supra* note 69.
127. *See id.*
128. *See Responsible Oversight of Artificial Intelligence for Clinical Research Professionals*, *supra* note 9, at 11.
129. *See Guidance on the Use of AI in Human Subjects Research, supra* note 69.
130. *See Guidance: Using Artificial Intelligence During Research Activities*, *supra* note 73, at 4.
131. *See id.* at 6.
132. *See id.* at 4.
133. *See* Solove, *supra* note 93, at 52.
134. *Guidance: Using Artificial Intelligence During Research Activities, supra* note 73, at 4.

relying on data from an inaccurate source or subsequent inaccurate output, is that individuals may be directly harmed through denial of treatment, misuse of resources, and an increase of safety concerns.[135] Since there is no guarantee that the output from an AI system is wholly accurate, entities and researchers must be mindful of the potential risk in heavily relying on output from an AI system to establish their research, especially when the system has not been properly or fully evaluated.[136]

Entities and researchers should acknowledge that the result of using AI systems within human subject research may lead to important discoveries or uses in clinical treatment and, therefore, accuracy of the data is paramount.[137] As discussed earlier in this Article, researchers may take certain steps to validate the quality of the data. Researchers may manually review the results or output to verify accuracy, which provides the opportunity to evaluate and identify whether there is any bias, discrimination, or hallucinations present in the source data or results. [138] This also allows for a human element in the research, which some argue is produced even by AI systems, to be verified and reinforced.[139] Researchers may consider using AI systems as an adjunct to the analysis, using AI as a method to review the manually developed output, rather than relying on AI to complete the work itself.[140] This may also minimize the potential of developing low quality output, as AI would be used in conjunction with the human review process.[141] Researchers may prepare predictions prior to reviewing the output, and compare their hypothesis to assist in determining the accuracy of the data before further use.[142] Researchers may document their efforts, and although human error could occur in reviewing the results, researchers performing an additional review

135. *See* U.S. DEP'T OF HEALTH & HUM. SERVS., *supra* note 2, at 85.
136. *See* Bae & Jeon, *supra* note 58.
137. *See id.*
138. *See* U.S. DEP'T OF HEALTH & HUM. SERVS., *supra* note 2, at 28–30.
139. *See* Bae & Jeon, *supra* note 58.
140. *See* U.S. DEP'T OF HEALTH & HUM. SERVS., *supra* note 2, at 7.
141. *See id.*
142. *See* Riccardo Fogliato et al., *Who Goes First? Influences of Human-AI Workflow on Decision Making in Clinical Imaging*, 2022 ACM CONF. ON FAIRNESS, ACCOUNTABILITY, AND TRANSPARENCY 2 (May 2022), https://arxiv.org/pdf/2205.09696 [https://perma.cc/XU34-E3GY].

of the output, rather than solely relying on the AI's technology, will likely reduce potential inaccuracies.[143]

Entities may encourage researchers to be transparent about how the source data was obtained, how the output was developed, the authenticity of the output, and the overall quality of the data.[144] As discussed earlier in this Article, research activities may use existing data, which could be considered secondary use.[145] If an entity or researcher decides to utilize existing, retrospective data to input into an AI system, the researcher may attempt to validate the source of the data to ensure transparency and accuracy.[146] If the data is coming from a publicly available source or even a third-party, the researcher should verify that all required permissions have been obtained to utilize the data with AI and confirm it is from a reputable source.[147] Finally, the likelihood of inaccuracy with the use of sensitive data with AI in human subject research is inevitable; however, best practices for responsible use of AI mitigate this risk.[148]

STRATEGIES TO MITIGATE RISK AND ENSURE COMPLIANT PRACTICES

There are many ongoing conversations between legal, compliance, and regulatory communities about how entities can reduce risk when utilizing AI systems in healthcare and human subject research, especially when using sensitive data. This section further explores strategies to reduce risk while also ensuring compliance with applicable state and federal laws. Additionally, this section discusses practices recommended by several federal government agencies to ensure the responsible use of AI by stakeholders.

143. *See Guidance: Using Artificial Intelligence During Research Activities, supra* note 73, at 5–6.
144. *See id.* at 5.
145. *See id.* at 4.
146. *See id.*
147. *See id.*
148. *See id.*

A. Transparency

Transparency is a critical mitigating factor when utilizing AI systems within human subject research.[149] Entities, researchers, and users can implement transparency throughout the research activity in various ways. One example is developing patient consent forms which clearly indicate how the participant's data will be used for purposes of the research activity and how it may be used subsequently in future research.[150] Another example is to indicate to future users of the source data and output where the data originated, how it was developed, and for purposes of the output, what specific AI system, model, or algorithm was utilized.[151] And finally, authors can promote transparency in publications by acknowledging AI use, specifying how AI interacted with the data, and disclosing the source data and development method of the subsequent output.[152]

For purposes of developing transparency within consent forms, entities should be knowledgeable about what reviews their IRBs or privacy boards are performing, and whether there are any additional considerations or screenings that should take place if AI is being used within the research.[153] As discussed earlier in this Article, IRBs or privacy boards may be able to provide a framework or guidance for researchers looking to utilize AI within their research activities, specifically when developing protocols or patient consent documents.[154] IRBs or privacy boards may be able to assess the use of multiple datasets and determine the likelihood of re-identification, allowing entities and researchers the opportunity to more effectively evaluate the use of the AI system within the research activity, and potentially disclose this risk to the participant.[155] Entities may consider implementing a separate AI review body that focuses on risk-benefit analysis, minimization of risk to participants, and transparency considerations within the

149. *See id.* at 5.
150. *See id.* at 4.
151. *See Guidance: Using Artificial Intelligence During Research Activities*, *supra* note 73, at 5.
152. *See id.*
153. *See* Pierre-Louis & Franco, *supra* note 49, at 2.
154. *See id.* at 7.
155. *See id.* at 4.

consent forms.[156] An AI review body would not necessarily replace an IRB or privacy board, but instead work collaboratively to ensure compliance while also streamlining review processes.[157]

When developing the source data, if a researcher is not transparent about where the data originated, the conclusions and scientific findings associated with the research activity could be called into question.[158] Researchers may consider maintaining transparency about where the source data originated, how it is being used, how the AI system is processing the source data, and whether this activity has been validated through human review.[159] If a researcher using data cannot validate its legitimacy because there is limited information regarding its origin, the researcher is then taking on a risk; even with human review, it is possible that the output may be inaccurate.[160] Remaining transparent about the origin of the data and development of the output allows for ethical and responsible collaboration with other users of the data, and allows future users to evaluate any potential risks associated with the data and take necessary precautions.[161]

Transparency regarding the use of AI within the research activity also reduces the potential for publication concerns.[162] If source data is utilized with an AI system and the output is similar to previous studies, there may be concerns about the legitimacy of the results.[163] Including a thorough explanation in a publication about the use of AI, the particular AI system used, how AI interacted with the data (either through algorithms or models, for example), and a general disclaimer about the validation practices may reduce potential risks and promote the responsible use of AI within human subject research.[164] Finally, entities and researchers should be cognizant of terms and conditions within contractual agreements, or partnership discussions with AI developers, which

156. *See Responsible Oversight of Artificial Intelligence for Clinical Research Professionals*, *supra* note 9, at 10.
157. *See id.*
158. *See* Pierre-Louis & Franco, *supra* note 49, at 5, 7.
159. *See id.* at 9.
160. *See Guidance: Using Artificial Intelligence During Research Activities*, *supra* note 73, at 6.
161. *See id.* at 5.
162. *See id.*
163. *See id.* at 4.
164. *See id.* at 5.

require a general disclaimer or scientific acknowledgement in a publication.[165]

B. Validation of Data

As discussed earlier in this Article, output data generated from the use of an AI system can be inaccurate, biased, discriminatory, or the result of a hallucination.[166] Therefore, validation of the output is an important method to reduce risk and confirm that the output being utilized and relied upon is accurate.[167] Researchers should not rely solely on the AI system, assuming the results are accurate, but should instead consider validation through a human reviewer.[168] The "human-in-the-loop" concept is critical, especially if there are indications that there may be issues with the source data or concerns about inaccuracies.[169] Entities may develop guidance and processes for researchers, emphasizing best practices to validate the source data and output, to determine the quality of the results.[170] Examples of potential best practices include evaluating the data, monitoring and auditing the AI systems, and identifying the potential risk level based on the type of AI being utilized. [171] For example, Generative AI may be considered higher risk, so entities may require validation practices; whereas entities using more traditional models, such as machine learning or federated learning, may only encourage validation practices, but not necessarily require such actions.[172]

Another reason to implement best practices, such as validation, is to avoid potential research misconduct claims, which include falsified, fabricated, and plagiarized content.[173] If a

165. *See id.*
166. *See id.* at 4.
167. *See id.*
168. *See id.*
169. *See Responsible Oversight of Artificial Intelligence for Clinical Research Professionals*, *supra* note 9, at 12.
170. *See Guidance: Using Artificial Intelligence During Research Activities, supra* note 73, at 4; U.S. DEP'T OF HEALTH AND HUM. SERVS., *supra* note 2, at 17, 42.
171. *See Responsible Oversight of Artificial Intelligence for Clinical Research Professionals*, *supra* note 9, at 11.
172. *See* U.S. DEP'T OF HEALTH & HUM. SERVS., *supra* note 2, at 6, 97.
173. *See Guidance: Using Artificial Intelligence During Research Activities, supra* note 73, at 6.

researcher is using an AI system, it is possible that the output may contain previously falsified, fabricated, or plagiarized source data, thereby widening the possibility of potential research misconduct claims.[174] Additionally, AI systems themselves can result in inaccuracies, such as AI-manipulated images, which lead to questions regarding falsification, or even fabrication.[175] Fabrication may also become more prevalent, as AI systems can generate content which may in fact be inaccurate.[176] And finally, AI allows for a plethora of potential plagiarism scenarios as a result of content generation; even simple functions such as "reword" or "make this sound better" may call into question the legitimacy of the publication.[177] Researchers who rely solely on the output generated without verifying the results may find themselves open to such claims; therefore, validation is a best practice to consider to determine the accuracy of the results before submitting a publication.[178]

C. Risk-Benefit Analysis

A significant component of the use of AI within human subject research is the ongoing risk-benefit analysis that is necessary for entities, researchers, and participants to consider during the research activity.[179] As part of the risk analysis, there are certain factors to consider, which may lessen the potential risks associated with the research activity. One factor to consider is the classification of the data being used.[180] For example, an entity may determine that the use of PHI with AI systems is prohibited because of the inherent risks and participant privacy concerns.[181] Other entities may evaluate the research activity and use of PHI, consult with privacy boards regarding the risk-benefit analysis,

174. *See* Pierre-Louis & Franco*, supra* note 49, at 7.

175. *See Responsible Oversight of Artificial Intelligence for Clinical Research Professionals*, *supra* note 9, at 32.

176. *See id.* at 33.

177. *See id.*

178. *See Guidance: Using Artificial Intelligence During Research Activities, supra* note 73, at 6; U.S. DEP'T OF HEALTH & HUM. SERVS.*, supra* note 2, at 24.

179. *See Guidance: Using Artificial Intelligence During Research Activities*, *supra* note 73, at 4–6.

180. *See Responsible Oversight of Artificial Intelligence for Clinical Research Professionals*, *supra* note 9, at 7–10.

181. *See* U.S. DEP'T OF HEALTH & HUM. SERVS., *supra* note 2, at 28.

and obtain participant consent to minimize risk.[182] In making such governance determinations, entities may consider leveraging existing data classification systems to determine the risk level and evaluate whether there are other ways to mitigate such risk, such as de-identification of the data or only using the minimum amount of data necessary for the purposes of the research activity.[183]

Another component to consider is the type of AI system being utilized.[184] For platforms involving Generative AI or LLMs, there are increased risks, such as re-identification, inaccuracies, patient consent considerations (including transparency), and ownership concerns.[185] Entities may consider using only low-risk data, which likely has already been made public or de-identified, in which there is a minimal possibility for loss of confidentiality or proprietary value.[186] This would allow for the use of platforms such as ChatGPT, DeepSeek, and other open-source solutions, which do not negotiate or enter into substantive contractual terms to protect privacy rights or ownership.[187] Entities may consider developing or facilitating the use of an internal Generative AI system, which would further reduce risks if the data remains on a local server.[188] Another option is to consider other more traditional forms of AI, such as machine or federated learning, which may eliminate the need to share raw data.[189] Federated learning models, for example, avoid data sharing from one organization to another, instead allowing organizations to utilize decentralized data systems in the recipient's own environment.[190] This may allow for the training of an AI model in a more secure environment with greater control over the data.[191]

Other factors to consider during a risk analysis include the possibility of loss of confidentiality, privacy, and potential security

182. *Id.*
183. *See id.*; *Responsible Oversight of Artificial Intelligence for Clinical Research Professionals*, *supra* note 9, at 17–18.
184. *See Responsible Oversight of Artificial Intelligence for Clinical Research Professionals*, *supra* note 9, at 6.
185. *See id.* at 10.
186. *See* U.S. DEP'T OF HEALTH & HUM. SERVS., *supra* note 2, at 28.
187. *See Guidance: Using Artificial Intelligence During Research Activities*, *supra* note 73, at 4; Trimble, *supra* note 12.
188. *See* Trimble, *supra* note 12.
189. *See id.*; Peloquin, Stein & Trimble, *supra* note 52.
190. *See* Peloquin, Stein & Trimble, *supra* note 52.
191. *See id.*

concerns, such as cyberattacks and data breaches.[192] One way to mitigate these concerns may be to negotiate contractual terms and conditions to better protect participants when using an external AI system.[193] Entities may also consider asking vendors to certify their security practices on a regular basis, and report if any unknown parties may have access to any data or output, especially if there is a high likelihood of re-identification.[194] Finally, although not addressed in depth in this Article, entities should be aware of any contractual terms and conditions or activities which may bring them within scope of GDPR, which has a risk-based data classification system for the use of data and AI systems.[195] GDPR has mechanisms for redressing harmed individuals which entities may need to consider as part of their risk-benefit analysis.[196]

Assessing the risk of utilizing AI systems within human subject research should be ongoing.[197] With the fast-pace changing AI landscape, entities should monitor ongoing research activities, while also continuously considering the risks associated with the use of AI.[198] Entities may consider developing not only guidelines for AI use, but also a risk assessment process, which would allow for ongoing monitoring of existing and future research projects involving human subjects.[199]

D. Training and Education

Recently, there has been a call for HHS and other federal government agencies to explore resources for developing education initiatives to support healthcare professionals, entities, researchers, participants, and industry partners in effectively and responsibly using AI systems while also driving innovation.[200] Although there are many general resources available regarding AI, a gap remains in the guidance, training, and education provided

192. *See* NAT'L INST. OF STANDARDS & TECH.*, supra* note 39, at 6.
193. *See* Trimble, *supra* note 12.
194. *See Responsible Oversight of Artificial Intelligence for Clinical Research Professionals*, *supra* note 9, at 21.
195. *See* Solove, *supra* note 93, at 20.
196. *See id.* at 24–25.
197. *See Responsible Oversight of Artificial Intelligence for Clinical Research Professionals*, *supra* note 9, at 2.
198. *See id.*
199. *See Responsible Oversight of Artificial Intelligence for Clinical Research Professionals*, *supra* note 9, at 11; U.S. DEP'T OF HEALTH & HUM. SERVS., *supra* note 2, at 9.
200. *See* U.S. DEP'T OF HEALTH & HUM. SERVS.*, supra* note 2, at 108.

by applicable regulatory bodies specific to this industry.[201] Providing training and education to AI users is essential to ensure that they are up to date not only on potential opportunities and new uses, but also possible challenges that may require additional considerations from a regulatory and compliance perspective.[202] Training and education are ways to mitigate the potential misuse of AI systems utilizing sensitive data, and are crucial for ensuring overall responsible use of AI systems within human subject research.[203]

Entities utilizing AI systems with human subject research may consider developing institutional policies and governance to promote safety, risk mitigation, and responsible use of AI.[204] These policies may include the ongoing need for training and education of its workforce, including anticipating changes in regulatory requirements and effectively communicating such changes to these individuals.[205] Governance efforts may also establish an AI ethics committee or review board with clear roles and responsibilities for AI oversight, which might include ongoing monitoring and auditing of AI systems.[206] Although an entity's AI governance may serve as a general guideline for AI system usage, legal and ethical concerns may still need to be evaluated on a case-by-case basis.[207]

Another component to consider during training and education is sharing lessons learned. Examples include confirming that data being used by an AI system is truly de-identified, documenting potential unintended deviations from the protocol, and evaluating successful or unsuccessful validation practices.[208] This allows entities, researchers, and future users to improve upon past

201. *See Responsible Oversight of Artificial Intelligence for Clinical Research Professionals*, *supra* note 9, at 11; U.S. DEP'T OF HEALTH & HUM. SERVS.*, supra* note 2, at 46.

202. *See* Pierre-Louis & Franco*, supra* note 49, at 2.

203. *See Responsible Oversight of Artificial Intelligence for Clinical Research Professionals*, *supra* note 9, at 2.

204. *See* Pierre-Louis & Franco*, supra* note 49, at 2; NAT'L INST. OF STANDARDS & TECH.*, supra* note 39, at 14.

205. *See Responsible Oversight of Artificial Intelligence for Clinical Research Professionals*, *supra* note 9, at 6; NAT'L INST. OF STANDARDS AND TECH.*, supra* note 39, at 12.

206. *Responsible Oversight of Artificial Intelligence for Clinical Research Professionals*, *supra* note 9, at 11.

207. *See* Zagarelli & Ouellette, *supra* note 35.

208. *See Responsible Oversight of Artificial Intelligence for Clinical Research Professionals*, *supra* note 9, at 17.

failures and enforce consistent, ethical practices moving forward.[209] Sharing lessons learned also allows for the minimization of potential risks through responsible research practices, while building trust in the future use of AI.[210] Finally, sharing past failures may allow entities, researchers, industry partners, and others to assess the viability of using AI within particular human subject research activities, and the potential need or want to further invest in such systems.[211]

CONCLUSION

With the fast-paced changes in technology and the increased use of AI within human subject research, entities must rapidly adopt new procedures and processes to ensure active compliance with regulatory requirements, responsible and ethical use of AI, and proper protection of the data and participants.[212] Although implementing new procedures and processes may be challenging and even burdensome, the overall benefits of using AI are undeniable and invaluable from an innovation and entrepreneurial perspective.[213] AI has enabled users to explore new business opportunities and enhance the efficiency of research practices.[214] The AI landscape has shown no signs of slowing down, as new AI platforms continue to emerge and reshape the future of human subject research.[215]

Federal government agencies have also noted the many positives associated with the use of AI and the growing economic market associated with such technologies.[216] As discussed throughout this Article, federal government agencies have provided limited guidance on the use of AI within human subject research, but the need for additional guidance remains.[217] Many

209. *See id.* at 18.
210. *See id.*
211. *See* U.S. DEP'T OF HEALTH & HUM. SERVS.*, supra* note 2, at 125.
212. *See Responsible Oversight of Artificial Intelligence for Clinical Research Professionals*, *supra* note 9, at 6.
213. *See* Trimble, *supra* note 12.
214. *See id.*
215. *See* Solove, *supra* note 93, at 7–8.
216. *See Artificial Intelligence and Its Potential Effects on the Economy and the Federal Budget*, CONG. BUDGET OFF. (Dec. 20, 2024), https://www.cbo.gov/publication/60774 [https://perma.cc/K3HE-BJUB]; U.S. DEP'T OF HEALTH & HUM. SERVS.*, supra* note 2, at 6–7.
217. *See Responsible Oversight of Artificial Intelligence for Clinical Research Professionals*, *supra* note 9, at 6.

stakeholders anticipate that additional guidance will be provided by the federal government in the near future, but this need for further guidance shines a light on the outdated policies, procedures, and regulatory requirements within healthcare and human subject research, which need revising to properly reflect the role that technology plays within these industries.[218] Additionally, uniform guidance is needed to ensure that individual entities are not adopting policies and procedures which create a "patchwork of inconsistent protections" because of lack of guidance. [219] Ideally, future regulatory guidance would include methods for adaptive AI technologies, promoting safe and responsible use of AI, fostering opportunities for quality assurance, transparency, validation, and elimination of bias and discrimination.

Overall, the risks associated with AI and human subject research are known and, as discussed throughout this Article, these conversations and concerns have been ongoing for decades.[220] Entities should focus on mitigating risk by developing policies, processes, and procedures which can be easily adapted and modified, as well as implementing a framework that ensures the research activities being conducted create a benefit that ultimately outweighs the risks associated with the use of sensitive data.[221] Although new challenges may arise as the AI landscape continues to develop, there will likely be other ways to mitigate risk, knowing that the overall benefits of using AI are immeasurable and an important investment in future research methods.[222]

Finally, there are many risks and variables associated with the use of AI and human subject research, which creates uncertainty and hesitation in future use.[223] The human subject research community must continue to foster discussions about the use of AI, push for additional regulatory guidance, and promote the opportunities that AI can provide for advancing research, treatment, and innovation.[224] Entities, researchers, users, and

218. *See* Solove, *supra* note 93, at 16.
219. *See* Sec'y Advisory Comm. on Hum. Rsch Prots., *supra* note 13.
220. *See* Solove, *supra* note 93, at 15-24.
221. *See* NAT'L INST. OF STANDARDS & TECH., *supra* note 39, at 9.
222. *See* Solove, *supra* note 93, at 6, 15, 23–24.
223. *See id.* at 22–28.
224. *See id.* at 5–24.

even participants should accept that AI will become a regular practice within human subject research and be prepared for these changes and adaptations in this technology, while also embracing the endless possibilities associated with AI.[225]

Disclaimer: the content herein is drawn from the Author's research and expertise. This Article in no way reflects the views or perspectives of the Author's employer. This Article is not designed to offer any legal, regulatory, compliance, or professional advice.

225. *See id.*