



# AI in healthcare: data governance challenges

Jenifer Sunrise Winter

School of Communications, Communication and Information Sciences Interdisciplinary PhD Program, University of Hawaii at Manoa, Honolulu, HI, USA

Correspondence to: Prof. Jenifer Sunrise Winter. School of Communications and Chair, Communication and Information Sciences Interdisciplinary PhD Program, University of Hawaii at Manoa, Honolulu, HI, USA. Email: [jwinter@hawaii.edu](mailto:jwinter@hawaii.edu).

Received: 27 August 2020; Accepted: 08 October 2020; Published: 25 March 2021.

doi: [10.21037/jhmhp-2020-ai-05](https://doi.org/10.21037/jhmhp-2020-ai-05)

View this article at: <http://dx.doi.org/10.21037/jhmhp-2020-ai-05>

## Introduction

AI applications are poised to transform health care, revolutionizing benefits for individuals, communities, and health-care systems (1). As the articles in this special issue aptly illustrate, AI innovations in healthcare are maturing from early success in medical imaging and robotic process automation, promising a broad range of new applications. This is evidenced by the rapid deployment of AI to address critical challenges related to the COVID-19 pandemic, including disease diagnosis and monitoring, drug discovery, and vaccine development (2-4).

At the heart of these innovations is the health data required for deep learning applications. Rapid accumulation of data, along with improved data quality, data sharing, and standardization, enable development of deep learning algorithms in many healthcare applications (5). One of the great challenges for healthcare AI is effective governance of these data—ensuring thoughtful aggregation and appropriate access to fuel innovation and improve patient outcomes and healthcare system efficiency while protecting the privacy and security of data subjects. Yet the literature on data governance has rarely looked beyond important pragmatic issues related to privacy and security. Less consideration has been given to unexpected or undesirable outcomes of healthcare in AI, such as clinician deskilling, algorithmic bias, the “regulatory vacuum”, and lack of public engagement (6). Amidst growing calls for ethical governance of algorithms (7), Reddy *et al.* (8) developed a governance model for AI in healthcare delivery, focusing on principles of fairness, accountability, and transparency (FAT), and trustworthiness, and calling for wider discussion. Winter and Davidson (9) emphasize the need to identify underlying values of healthcare data and use, noting the

many competing interests and goals for use of health data—such as healthcare system efficiency and reform, patient and community health, intellectual property development, and monetization. Beyond the important considerations of privacy and security, governance must consider who will benefit from healthcare AI, and who will not. Whose values drive health AI innovation and use? How can we ensure that innovations are not limited to the wealthiest individuals or nations? As large technology companies begin to partner with health care systems, and as personally generated health data (PGHD) (e.g., fitness trackers, continuous glucose monitors, health information searches on the Internet) proliferate, who has oversight of these complex technical systems, which are essentially a black box? (9,10).

To tackle these complex and important issues, it is important to acknowledge that we have entered a new technical, organizational, and policy environment due to linked data, big data analytics, and AI (11). Data governance is no longer the responsibility of a single organization. Rather, multiple networked entities play a role (12) and responsibilities may be blurred. This also raises many concerns related to data localization and jurisdiction—who is responsible for data governance? In this emerging environment, data may no longer be effectively governed through traditional policy models or instruments. Below, I highlight some key issues to illustrate these challenges.

## The growing scope and variety of health-related data

Personal health data increasingly extend beyond clinical encounters, transactions at pharmacies, and claims data. Many types of data related to a person's health are directly

collected, or can be inferred, based on daily activities (e.g., fitness trackers, web browsing, tracking of household activities via smart devices, supermarket purchases). Sources of these PGHD (13) are rapidly growing and are aggregated, mined for insight, and resold for profit. These data may fall outside of existing health data regulation (e.g., HIPAA in the United States) and are governed by the technology company's own privacy policies (10). Thus, the distinction about what is health data and what is not is increasingly blurred. Predictive health models based on these data can be used to inform a variety of consequential decisions (14,15) that may not be in the best interest of the individual. Additionally, harms such as unjust discrimination may occur in areas not directly related to health care, such as employment or housing discrimination (10).

The scale and scope of data necessary for health AI, and the opacity of how algorithms access and transform these data, challenge existing data protection regimes. Even a comprehensive data protection law such as the EU's GDPR may not be able to manage the tension between desired innovation through AI and protection of personal health data. The GDPR allows data gathered for specific purposes and prohibits reuse, while training deep learning models requires large amounts of data (16,17) and may be strengthened by reuse of data collected for other purposes.

Because the movement and use of data is not typically transparent to data subjects or regulatory authorities, damages may be hard to detect, and monitoring and enforcing compliance may be difficult. This has led to a call for FAT in algorithms, as well as growing efforts towards "explainable AI" and algorithmic audits (8,12).

### New data handlers and collaborations

As the volume of digitized health data has grown, many new actors have entered the health data ecosystem. Numerous technology start-ups, as well as information technology giants—such as Google, Apple, and IBM—collect data through apps, their online search platforms, and a growing array of health tech devices (e.g., sleep trackers, EKGs, smart thermometers). For example, in 2019 Google acquired fitness tracker Fitbit and its users' data. These technology firms are also increasingly creating partnerships with health care systems. For tech firms, the potential to monetize personal healthcare data is a strong temptation, and organizations that handle health information may work around, or even disregard, health data regulations in the race towards lucrative AI innovation (10). This is evidenced

by two recent cases. In 2015, Google's DeepMind Health AI venture partnered with a National Health Services (NHS) hospital system in the UK and shared 5 years of identifiable medical data on 1.6 million patients. The intention of this partnership was to develop healthcare AI applications that might also improve NHS patient care (18,19). Although the UK Information Commissioner's Office ruled in 2017 that this data-sharing agreement violated data protection laws, it was nonetheless extended for another 5 years (20). Thus, even in the UK's highly regulated environment, and after public outrage and regulatory censure, Google DeepMind Health continued to use patient data for its AI health venture. In late 2019, Google Health also partnered with Ascension Health to analyze data from millions of people in 21 US states (21).

In a second case, Facebook founder Mark Zuckerberg testified before the US Congress in 2018 that the social media giant deliberately sought out individuals' health data. Journalists soon revealed that Facebook had sought to access anonymized patient data to "*match hospitals' patient data on diagnoses and prescription information with Facebook so the company could combine that data with its own to construct digital profiles of patients [...]*" (22). Disclosure of de-identified data is often permitted for secondary analysis without patient consent, but anonymized information is increasingly being re-identified through big data analytics and data linkages between sets (23). Facebook bypassed federal law in the US that requires a patient's consent to access personal health data. This instance illustrates how AI in healthcare analytics is challenging the principle of informed consent. A patient may authorize sharing of his or her health information to third parties for a particular use, such as coordinating payment by an insurer or obtaining medication from a pharmacy. Some of the organizations who handle this data may re-use it to facilitate internal analytics or as part of a health research project. The Facebook and Google DeepMind Health cases suggest that the lure of AI innovation led the companies to bypass patient consent, and this reveals a growing tension between health research involving big data sets and informed consent. New models of open, broad, and portable consent are emerging, but the question of who will benefit from these research results is important (24).

These cases also highlight how regulations intended to preserve patient privacy and control over personal health data cannot fully address the increased scope and number of data handlers using, and reusing, health data. Partnerships with healthcare organizations operating under

one set of restrictions and large tech firms operating under a more relaxed regulatory regime facilitates AI healthcare innovation and monetization.

## Conclusions

As we advance the many promising applications of healthcare AI, data governance must not be overshadowed by innovation. Building health AI applications that create improvements in patient care and health services administration will require building public trust, institutions, and policies that ensure fair, equitable, and transparent developments. To do so, we need to better understand the motivations, values, and conflicts underlying the use of health data. This will require broad and thoughtful discussion about whose interests will be served and how we can balance individual and community rights with corporate interest in AI health data.

## Acknowledgments

*Funding:* This material is based upon work supported by the National Science Foundation under grant no. 1827952.

## Footnote

*Provenance and Peer Review:* This article was commissioned by the editorial office, *Journal of Hospital Management and Health Policy* for the series “AI in Healthcare - Opportunities and Challenges”. The article did not undergo external peer review.

*Conflicts of Interest:* The author has completed the ICMJE uniform disclosure form (available at <http://dx.doi.org/10.21037/jhmhp-2020-ai-05>). The series “AI in Healthcare - Opportunities and Challenges” was commissioned by the editorial office without any funding or sponsorship. JSW served as the unpaid Guest Editor of the series. The author has no other conflicts of interest to declare.

*Ethical Statement:* The author is accountable for all aspects of the work in ensuring that questions related to the accuracy or integrity of any part of the work are appropriately investigated and resolved.

*Open Access Statement:* This is an Open Access article distributed in accordance with the Creative Commons

Attribution-NonCommercial-NoDerivs 4.0 International License (CC BY-NC-ND 4.0), which permits the non-commercial replication and distribution of the article with the strict proviso that no changes or edits are made and the original work is properly cited (including links to both the formal publication through the relevant DOI and the license). See: <https://creativecommons.org/licenses/by-nc-nd/4.0/>.

## References

1. Flores M, Glusman G, Brogaard K, et al. P4 medicine: how systems medicine will transform the healthcare sector and society. *Per Med* 2013;10:565-76.
2. National Institutes of Health. NIH harnesses AI for COVID-19 diagnosis, treatment, and monitoring. 2020. Available online: <https://www.nih.gov/news-events/news-releases/nih-harnesses-ai-covid-19-diagnosis-treatment-monitoring>
3. Arshadi AK, Webb J, Salem M, et al. Artificial Intelligence for COVID-19 Drug Discovery and Vaccine Development. *Front Artif Intell* 2020;3:65.
4. Harmon SA, Sanford TH, Xu S, et al. Artificial intelligence for the detection of COVID-19 pneumonia on chest CT using multinational datasets. *Nat Commun* 2020;11:4080.
5. Miotto R, Wang F, Wang S, et al. Deep learning for healthcare: review, opportunities and challenges. *Brief Bioinform* 2018;19:1236-46.
6. Carter SM, Rogers W, Win KT, et al. The ethical, legal and social implications of using artificial intelligence systems in breast cancer care. *Breast* 2020;49:25-32.
7. Ahmad MA, Patel A, Eckert C, et al. Fairness in machine learning for healthcare. In: *Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*, 2020:3529-30.
8. Reddy S, Allan S, Coghlan S, et al. A governance model for the application of AI in health care. *J Am Med Inform Assoc* 2020;27:491-7.
9. Winter JS, Davidson E. Governance of artificial intelligence and personal health information. *Digital Policy, Regulation and Governance* 2019;21:280-90.
10. Pasquale F. *The black box society: the secret algorithms that control money and information*. Cambridge: Harvard University Press, 2015.
11. Taylor RD. The next stage of US communications policy: the emerging embedded infosphere. *Telecommunications Policy* 2017;41:1039-55.
12. Janssen M, Brous P, Estevez E, et al. Data governance: organizing data for trustworthy artificial intelligence. *Gov*

- Inf Q 2020;37:101493.
13. Deering MJ, Siminerio E, Weinstein S. Patient-generated health data and health IT. Office of the National Coordinator for Health Information Technology. 2013.
  14. Bates DW, Saria S, Ohno-Machado L, et al. Big data in health care: using analytics to identify and manage high-risk and high-cost patients. *Health Aff (Millwood)* 2014;33:1123-31.
  15. Cohen IG, Amarasingham R, Shah A, et al. The legal and ethical concerns that arise from using complex predictive analytics in health care. *Health Aff (Millwood)* 2014;33:1139-47.
  16. Chen XW, Lin X. Big data deep learning: Challenges and perspectives. *IEEE Access* 2014;2:514-25.
  17. Xiao C, Choi E, Sun J. Opportunities and challenges in developing deep learning models using electronic health records data: a systematic review. *J Am Med Inform Assoc* 2018;25:1419-28.
  18. Hawkes N. NHS data sharing deal with Google prompts concern. *BMJ* 2016;353:i2573.
  19. Winter JS, Davidson E. Big data governance of personal health information and challenges to contextual integrity. *The Information Society* 2019;35:36-51.
  20. Lomas N. DeepMind health inks another 5-year NHS app deal in face of ongoing controversy. *TechCrunch*. 2017. Available online: <https://techcrunch.com/2017/06/22/deepmind-health-inks-another-5-year-nhs-app-deal-in-face-of-ongoing-controversy/>
  21. Singer N, Wakabayashi D. Google to store and analyze millions of health records. *The New York Times*. 2019. Available online: <https://www.nytimes.com/2019/11/11/business/google-ascension-health-data.html>
  22. Ostherr K. Facebook knows a ton about your health. Now they want to make money off it. *Washington Post*. 2018. Available online: <https://www.washingtonpost.com/news/posteverything/wp/2018/04/18/facebook-knows-a-ton-about-your-health-now-they-want-to-make-money-off-it/> (accessed 5 May 2018).
  23. Simon GE, Shortreed SM, Coley RY, et al. Assessing and minimizing re-identification risk in research data derived from health care records. *EGEMS (Wash DC)* 2019;7:6.
  24. Sharon T. The Googlization of health research: from disruptive innovation to disruptive ethics. *Per Med* 2016;13:563-74.

doi: 10.21037/jhmhp-2020-ai-05

**Cite this article as:** Winter JS. AI in healthcare: data governance challenges. *J Hosp Manag Health Policy* 2021;5:8.