The Right to Erasure: How to Delete Your Data from AI Health Platforms

Rasit Dinc

Rasit Dinc Digital Health & AI Research

Published: January 26, 2023 | AI Diagnostics

DOI: 10.5281/zenodo.17997636

Abstract

The Right to Erasure: How to Delete Your Data from AI Health Platforms The integration of Artificial Intelligence (AI) into healthcare has ushered in an...

The Right to Erasure: How to Delete Your Data from AI Health Platforms

The integration of Artificial Intelligence (AI) into healthcare has ushered in an era of unprecedented diagnostic and therapeutic potential. From predictive analytics to personalized medicine, AI health platforms are rapidly becoming central to modern healthcare delivery. However, this progress is predicated on the collection and processing of vast quantities of sensitive Personal Health Information (PHI). As the digital footprint of health data expands, a critical question for professionals and the general public alike is: **How do I delete my data from AI health platforms?** Understanding the legal landscape and the practical steps for data deletion is paramount to maintaining digital autonomy and privacy in the age of algorithmic health.

The Legal Frameworks Governing Health Data Deletion

The ability to request the deletion of personal data is not a mere courtesy; it is a legally enshrined right in many jurisdictions. The complexity arises because AI health platforms often operate across multiple regulatory environments, primarily governed by the European Union's **General Data Protection Regulation (GDPR)** and the United States' **Health Insurance Portability and Accountability Act (HIPAA)**.

1. The GDPR's Right to Erasure

For individuals within the European Economic Area (EEA), the GDPR provides the most robust mechanism for data deletion, known as the "right to be forgotten" (Article 17) [1]. This right mandates that a data controller (the AI health platform) must erase personal data without undue delay under several conditions, including:

The data is no longer necessary for the purpose for which it was collected. The individual withdraws consent, and there is no other legal ground for processing. *The individual objects to the processing, and there are no overriding legitimate grounds.*

The challenge for AI systems is that personal data, once used to train a model, becomes intrinsically linked to the model's functionality. The European Data Protection Board (EDPB) has acknowledged this, noting that the exercise of the right to erasure can be difficult in the context of AI models, especially concerning the concept of "unlearning" data from the model's parameters [2]. Nevertheless, the obligation to delete the original data source and any derived personal identifiers remains clear.

2. HIPAA and the Right to Amendment

In the United States, HIPAA provides a different, though related, set of rights. HIPAA grants individuals the right to request an amendment to their Protected Health Information (PHI) held by Covered Entities (CEs) and Business Associates (BAs), which often include AI health platforms [3]. While HIPAA does not explicitly grant a "right to erasure" equivalent to the GDPR, it mandates strict rules for data disposal and security.

Specifically, HIPAA requires CEs and BAs to have policies for the secure disposal of PHI, ensuring that data is rendered essentially unreadable, undecipherable, and irrecoverable [4]. For the user, the practical route to data deletion often involves requesting the platform to terminate the account and confirm the secure disposal of all associated PHI, a process that must adhere to the platform's established HIPAA-compliant data retention and destruction policies.

Practical Steps to Delete Your Data

For an individual seeking to exercise their right to delete data from an AI health platform, a structured approach is necessary:

Step	*Action Required*	*Key Consideration*
1. Identify the Data Controller	*Determine the specific entity (the app, the service provider, or the underlying data processor) that holds your data.*	*Check the platform's Privacy Policy and Terms of Service.*
2. Locate the Privacy Request Mechanism	*Find the platform's designated channel for privacy requests (e.g., a dedicated privacy portal, a specific email address, or a form).*	*Do not rely on general customer support; look for "Data Subject Access Request" (DSAR) or "Privacy Request."*
3. Submit a Formal Request	*Clearly state your request for the* ***erasure*** *or* ***secure disposal*** *of all your personal data and PHI, citing the relevant regulation (GDPR Article 17 or state-specific privacy laws like CCPA).*	*Be specific about the data you want deleted (e.g., account, usage logs, health metrics).*
4. Follow Up and Confirm	*Request written confirmation that the data has been securely and permanently deleted from all active systems and backups.*	*Platforms must respond to these requests within a legally defined timeframe (e.g., 30 days under GDPR).*

The Challenge of Data Unlearning in AI

*The most significant technical hurdle to data deletion is the concept of **data unlearning**. When an AI model is trained on a dataset, the information is encoded into the model's weights and parameters. Simply deleting the original source data does not remove its influence on the model's behavior.*

*While research into machine unlearning is advancing, it remains a complex and computationally intensive task [5]. Platforms may argue that complete removal of data influence is technically infeasible or would compromise the model's integrity. However, legal interpretations increasingly suggest that the **right to erasure** requires a meaningful effort to mitigate the influence of the deleted data, or at minimum, to cease all future processing and ensure the data is not used for future model retraining.*

For more in-depth analysis on the technical and ethical implications of data unlearning and the future of digital health privacy, the resources at www.rasitdinc.com provide expert commentary.

Conclusion

The power of AI in healthcare must be balanced by a commitment to individual data rights. While the process of deleting data from AI health platforms is complex, driven by a patchwork of global regulations, the legal obligation on data controllers is clear. By understanding the rights afforded by frameworks like GDPR and HIPAA, and by following a formal request process, individuals can take proactive steps to control their digital health data and ensure their right to privacy is respected.

*

References

[1] Art. 17 GDPR – Right to erasure ('right to be forgotten'). GDPR.eu*. https://gdpr-info.eu/art-17-gdpr/ [2] Opinion 28/2024 on certain data protection aspects related to the development and deployment of AI models.* European Data Protection Board (EDPB)*. https://www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-models_en.pdf [3] Integrating artificial intelligence into health care through data governance.* PMC - NCBI*. https://pmc.ncbi.nlm.nih.gov/articles/PMC6813940/ [4] Data Disposal – a Key to HIPAA Security.* AI Robotics Law*. https://www.airoboticslaw.com/blog/data-disposal-hipaa-security [5] Beware Privacy Risks In Training AI Models With Health Data.* Frost Brown Todd*. https://frostbrowntodd.com/beware-privacy-risks-in-training-ai-models-with-health-data-3/

Rasit Dinc Digital Health & AI Research

https://rasitdinc.com