

Strategies to Unlock AI's Potential in Healthcare Part 6: Commercialization of AI Tools in Healthcare – the Challenge of Securing Adequate Data Rights

Article By:

Julie E. Korostoff

As noted in previous posts in this [series](#), AI tools hold great promise for applications in healthcare. To date, AI tools in healthcare primarily [leverage machine learning technology](#) – i.e., the machine's ability to keep improving its performance without humans having to explain exactly how accomplish the tasks it's given. Rather than programming the machine to perform specific tasks for specific outcomes, machines are trained using real world, curated medical data; the more quality training data, the better the machine's performance. If access to large amounts of well-labeled data is necessary to perfect an AI tool, how do you ensure that you have adequate data rights to move towards commercialization? This post will address the contractual commitments that a developer of a healthcare AI tool should secure in order to have the data rights necessary for development and commercialization.

At each juncture at which you procure data for your product, whether from a strategic development partner, a customer or a third party data aggregator, it is key to (1) secure express rights to use the data for commercial purposes; (2) obtain contractual commitments from the data source that the data source has the right to provide the data for such purposes; and (3) require the data source to provide the data with the labeling and format necessary for your algorithm to learn the associations between the features and the labels.

Data Rights at the Development Stage

Like many developers of healthcare AI tools, your algorithm may have been initially the fruit of a collaboration with a particular health services system in which you were given the right to use the health system's data for the purpose of developing the tool for the benefit of the health system's patient population. To commercialize the tool, you will need to obtain explicit rights in your written contract with the health system to use the data set for the benefit of other populations for your company's commercial purposes. As a condition to the right to use the data in this manner, the health system likely will require that you protect the privacy of the data by de-identifying the data. Contracts for the sharing of health data for commercial purposes will often stipulate the manner in which the data will be de-identified so that the data is no longer considered "personal health information" or "PHI" as defined and regulated by HIPAA (see our post on

HIPAA considerations [here](#)). It will serve you well to identify proactively the de-identification process before approaching any data source; this will instill confidence that you are a conscientious business partner.

Data Rights from Customers

For an AI tool to be most useful across a customer base, each customer will need to agree that the data processed by the AI tool will become a permanent part of the AI tool's data set. This would be accomplished by including specific contract clauses in the agreement that you sign with your customer that state that your company has the perpetual, irrevocable right to use the data provided by the customer and processed by the AI product. Here too, customers will require that the data be de-identified in order for the data to be used for purposes other than servicing the customer's own patient population.

Data Rights from Commercial Sources

Healthcare data is remarkably silo-ed. Often, healthcare data resides captive in the un-integrated data stores of disparate health services systems. Data from sources other than development partners and customers may be necessary for your product. You may license de-identified data from data aggregators, third parties that aggregate data from healthcare providers and other health services companies. Unlike the data that you obtain directly from your customers, where you and the customer control the manner in which the data is labeled, organized and ingested and subsequently de-identified, you will have to stipulate by contract with the aggregator the characteristics and qualities of the data you will purchase. In addition, you will want the aggregator to ensure (and warrant) that the data has been de-identified in a HIPAA-compliant manner.

Ensuring sufficient data rights at the outset of product development and throughout the trajectory of your product is a necessary component for commercial success.

Read part [one](#), [two](#), [three](#), [four](#), and [five](#) of the series here.

©1994-2025 Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, P.C. All Rights Reserved.

National Law Review, Volume VIII, Number 330

Source URL: <https://natlawreview.com/article/strategies-to-unlock-ai-s-potential-healthcare-part-6-commercialization-ai-tools>