Digital Health Transactions: AI and Big Data

Health Law Webinar

March 13, 2024

Fredrikson

Where Law and Business Meet®

Agenda

- Introductions, Housekeeping
- Overview: Uses of “Big Data” and AI in Healthcare
- Artificial Intelligence Landscape
- Privacy Considerations
- Contracting around IP in Data and AI
- Health Care Regulatory Perspectives

Data: The Fuel that Drives AI

- Data is what powers AI
  - *The AI can be only as good as the data it relies on*
- Data is a critical corporate asset (and liability)
- Controls around data collection, acquisition, security, privacy, accuracy and ethical use are key

How are Big Data and AI Impacting Healthcare?

Big Data and AI are driving Digital Health

“Digital health is the convergence of the digital and genomic revolutions with health, healthcare, living, and society.”

Source:
http://storyofdigitalhealth.com/

Scope and Applications

Health Apps

Connected Devices / IoT

Automation and Robotics

Consumer apps and wearables

Clinical Research

Health IT / Services

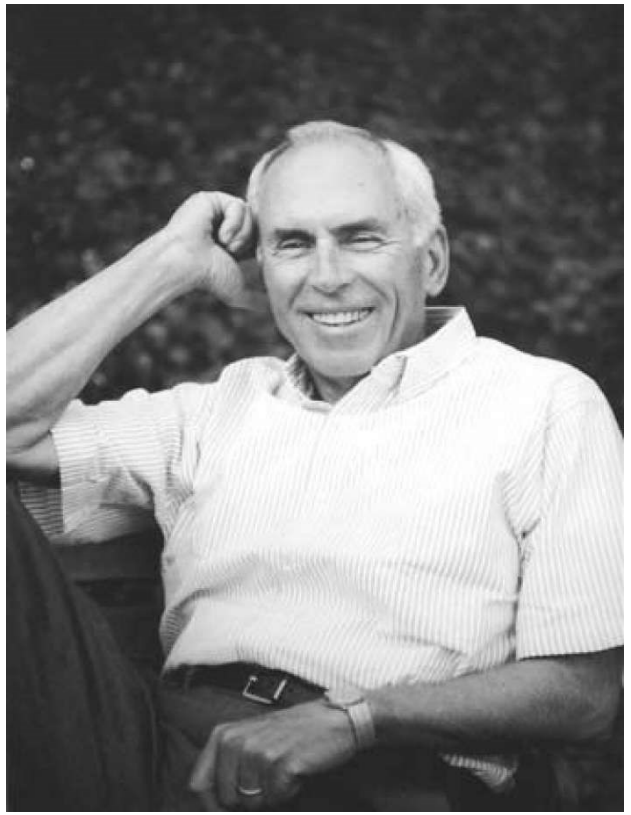
Telemedicine

Medical Algorithms

Amara's Law

"We tend to overestimate the effect of a technology in the short run and underestimate the effect in the long run."

- Roy Amara, Co-founder, Institute for the Future



Multiple Intersecting Issues

Technology and IP Rights Considerations

Regulatory Considerations

Life Sciences Considerations

Health Care Considerations

Advertising Considerations

Ethical Considerations

Additional Considerations

Artificial Intelligence Landscape

Artificial Intelligence – What is it?

An "***artificial intelligence system***" (as defined in the EU AI Act) is software developed using techniques or approaches that permit it "for a given set of human-defined objectives, [to] generate outputs such as content, predictions, recommendations or decisions," which "influenc[e]" the environments with which the software interacts.

- AI leverages "models" – computational, statistical, or machine-learning techniques – to produce outputs from a given set of inputs. (President Biden's *Executive Order on AI* at §3(c).)
- Data and computer scientists build the models using the following types of data sets:
  - *Training data: the data that is used to teach an AI system the appropriate parameters for its data analysis.*
  - *Validation data: the data that is used to evaluate the AI system's outputs and to tune its non-learnable parameters and learning processes.*
  - *Testing data: the data that is used to independently evaluate the trained and validated AI system before placing it in the market or putting into service.*

Many AI Systems are theoretical—meaning they do not currently exist in a tangible or workable form.

- Most businesses currently leverage "predictive AI"—software that relies on predictive analytics models "designed to assess historical data, discover trends, and use that information to predict future trends." (IBM, *"What is Predictive Analytics?"*)
- "Generative AI" is a machine-learning model that essentially predicts patterns and blocks of text to create new data (rather than just simple predictions based upon an analysis of a structured data set).

What Rights Exist in AI Systems?

Traditional intellectual property rights:

- Patent rights – Ability to prevent someone else from practicing your invention.
- Copyrights – Exclusive right that the author of a work has to reproduce, distribute, prepare derivative works based upon, perform, and display such work.
- Trade secret rights – Provides owners of valuable and secret information a remedy for the misappropriation of such information.

What IP rights arise in AI Systems?

- The underlying models, to the extent they mechanize a process, could be patentable inventions. The details could also constitute trade secret information.
- The software code that executes the model could be copyrightable as an original work of authorship, or be a trade secret, to the extent its confidentiality is preserved.
- Data, in and of itself, as a set of facts, is not protected by U.S. copyright law. But a data compilation may be protected if the arrangement or selection of data is sufficiently creative/original. (*See Feist Publications, Inc. v. Rural Telephone Service Co.*, 499 U. S. 340 (1991).) Note: an AI System's "methods," "procedures," and "processes" are not copyrightable.
- Data, as information, could constitute a trade secret if it is commercially valuable and steps are taken to preserve its confidentiality.

Components of an AI System where IP rights may exist: (1) input data; (2) algorithms/models; (3) validation data/training data; (4) the inventions arising from the application; (5) output data; and (6) the code that allows the system to execute.

Contract Terms are Key…

- Google's Terms of Service: "You provide Google with [a license to] . . . host, reproduce, distribute, communicate, and use your content . . . publish, publicly perform, or publicly display your content . . . modify and create derivative works based on your content . . .. This license lasts for as long as your content is protected by intellectual property rights."
- OpenAI's Terms of Use: "We may use [your input to the Services] to provide, maintain, develop, and improve our Services."
- Meta's AIs Terms of Service: "When information is shared with AIs, the AIs may retain and use that information to provide more personalized Outputs. Do not share information that you don't want the AIs to retain and use. . . . Meta may share information that you provide with third parties who help us provide you with more relevant or useful responses. For example, we may share questions contained in a Prompt with a third-party search engine, and include the search results in the response to your Prompt. The information we share with third parties may contain personal information if your Prompt contains personal information about any person. By using AIs, you are instructing us to share your information with third parties when it may provide you with more relevant or useful responses."
- Microsoft's AI Services Terms: "[B]y using the Online Services, posting, uploading, inputting, providing or submitting content you are granting Microsoft, its affiliated companies and third party partners permission to use the . . . [p]rompts . . . in connection with the operation of its businesses (including, without limitation, all Microsoft Services), including, without limitation, the license rights to: copy, distribute, transmit, publicly display, publicly perform, reproduce, edit, translate and reformat the . . . [p]rompts . . . and other content you provide."

What are Some Current Enforcement Trends?

Intellectual Property Enforcement:

- *The New York Times Company v. Microsoft Corporation, OpenAI, Inc., et al.*, Case No. 1:23-cv11195 (S.D. New York), filed Dec. 27, 2023 – The NY Times alleges that OpenAI (which Microsoft has invested in and will be a part-owner of) trained its large-language models ("LLMs") on NY Times content, which the NY Times demonstrates in its complaint with examples of prompts causing ChatGPT and Bing Chat to produce verbatim NY Times' content. The NY Times argues these outputs are reproductions and derivatives of NY Times' works infringing on the NY Times' copyrights and seeks statutory and actual damages and the destruction of all models and training sets that incorporate the NY Times' works.
- *The Authors Guild, et al. v. Microsoft Corporation, OpenAI, Inc. et al., Case No. 1:23-cv-8282-SHS (S.D. New York), filed Sept. 20, 2023* – Plaintiffs allege that OpenAI pirated very large sources of ebooks and digested such books in their entirety to train Chat GPT-4 and, as a result, even summaries of copyrighted books are derivative works that are "inherently based on the original unlawfully copied work." Plaintiffs argue OpenAI and Microsoft's conduct constitutes willful infringement of Plaintiffs' copyrights and seeks statutory damages, actual damages, and an award of profits attributable to the infringement.

Biden *Executive Order* – Upcoming Deadlines

- The *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* ("EO") was released on October 30, 2023
- More than 50 federal entities are directed to take more than 100 specific actions to implement the EO from 2024 – 2025
- The EO has eight policy focuses: (1) Safety and Security; (2) Innovation and Competition; (3) Worker Support; (4) Consideration of Bias and Civil Rights; (5) Consumer Protection; (5) Privacy; (6) Federal Use of AI; (7) International Leadership
- Office of Science and Technology Policy (and other agencies) to establish guidelines for companies that manipulate biologic genetic material – Due April 27, 2024
- Health and Human Services to:
  - Develop a strategy to assess AI quality – Due April 27, 2024
  - Consider actions to advance compliance with nondiscrimination laws as they relate to AI for health and human services providers receiving federal funding. – Due April 27, 2024
  - Develop a strategy for the use of AI and AI-enabled tools in drug development – Due October 29, 2024
  - Establish a safety program to monitor and improve AI development in healthcare through a common framework to identify errors and avoid harms – Due October 29, 2024

What are Some Current Regulatory Trends?

Regulatory Scrutiny:

- **Human Resources:** Illinois' AI Video Interview Act prohibits the use of "artificial intelligence to evaluate applicants who have not consented to the use of artificial intelligence analysis" and requires notice and consent before analyzing applicant-submitted videos with AI Systems. New York City's Local Law 144 regulates the use of automated employment decision tools ("AEDTs") in hiring and promotion decisions. Employers are prohibited from using AEDTs unless the tool has been subject to a bias audit and the results of the audit have been made publicly available to candidates.
- **Biometric Information:** In December 2023, the FTC filed a complaint against Rite Aid Corporation alleging Rite Aid used facial recognition technology for surveillance purposes but failed to implement reasonable procedures to test the technology's accuracy and oversee its use by employees to prevent foreseeable harm to consumers (particularly, "Black, Asian, Latino, and women consumers"). The stipulated settlement imposes extremely specific requirements for the use of such technology in the future.

What are We Seeing From a Security Risk Perspective?

Professional researches and hackers are undertaking studies to identify vulnerabilities of generative AI Systems.

- *Compromise of Microsoft's Repository:* Third-party researchers were able to leverage Microsoft's publicly available GitHub libraries for its open-source AI learning models to expose 3TB of internal Microsoft data, including backup copies of two Microsoft employee workstations

- *Custom GPTs:* In November 2023, a group of researchers at Northwestern University studied AI Systems that leverage OpenAI's GPT models to design "custom" GPTs that are tailored by users for specific applications. The researchers were able to prompt the AI Systems to provide files that had been uploaded to the system by a previous user 100% of the times attempted and were able to extract previous-user-submitted system prompts 97% of the times attempted.

Privacy Considerations

Laws Regulating Non-PHI Health Data

Washington My Health My Data Act – effective March 31, 2024

- Purpose: "[To] close an egregious legal loophole that allows non-health care organizations to collect, share or sell private health information."
- Applicability: Entities that (a) conduct business in Washington or produces or provides products or services that are targeted to consumers in Washington and (b) control the purposes and means of processing consumer health data
- Information Regulated: "Consumer health data" is "personal information that is linked or reasonably linkable to a consumer and that identifies a consumer's past, present, or future physical or mental health."
- Key Requirements
  - *Extensive requirements re: disclosures in privacy policy*
  - *Consent before collecting or sharing consumer health data, except as necessary to provide a product or services requested by consumer. Note: separate consent required for collecting and sharing.*
  - *Afford consumers right to (a) confirm whether entity is collecting, sharing, or selling consumer health data, (b) withdraw consent from collection and sharing of consumer health data, and (c) delete consumer health data*
  - *Must flow-down requirements to 3P processors*
  - *Restrict access to those for whom access is necessary to further the purposes for which the consumer consented*

Other Privacy Compliance Considerations

Updating notices at collection

Evaluating whether there is processing of “sensitive” personal information (i.e., inferences)

Operationalizing the right to (1) receive details regarding how their personal information is used and to whom it is disclosed, (2) request the business delete their personal information, and (3) withdraw consent or opt-out of certain processing of their personal information

Meeting data minimization standards

Justifying the retention of data for long periods of time

Determining whether risk assessments are required

FTC Case Study #1: Everalbum, Inc.

Complaint brought in January 2021 - Settled

Allegation: Everalbum misled users of mobile app that facial recognition technology would not be activated with respect to users' content unless they affirmatively chose to activate the feature. Everalbum activated the feature, which could not be turned off, for almost all users. Everalbum also failed to honor promise to delete data and instead retained data indefinitely.

Settlement Included:

1. Deletion or destruction of all affected data derived from an image of an individual's face
2. Deletion or destruction of all affected models or algorithms developed using biometric information collected from users

FTC Case Study #2: Korchava Inc.

Complaint brought in August 2022 - Pending

Allegation: Korchava acquired consumers' precise geolocation data and sold the data in a format that allowed others to track consumers' movements to and from sensitive locations, such as locations associated with medical care, reproductive health, mental health. The data feeds are sold via marketplaces that are publicly accessible.

Legal Claim: Identification of sensitive and private characteristics of consumers injures or is likely to injure consumers through exposure to stigma, discrimination, or other harms. Constitutes an unfair sale of sensitive data in violation of FTC Act.

FTC Case Study #3: GoodRx Holdings, Inc.

Complaint brought in February 2023 (amended June 2023) – Pending

Allegation: GoodRx ran campaigns on ad platforms such as Facebook, Google, Criteo, etc. using information about users' prescription medications and personal health conditions, as well as contact information and persistent identifiers. No notice was provided regarding such disclosures.

Legal Claim: GoodRx disseminated false and deceptive statements re its use and disclosure of health and personal information. Such conduct was in violation of the FTC Act and Health Breach Notification Rule

Privacy Issues

Complying with HIPAA

Complying with evolving state-specific laws

Complying with 3rd party terms

Addressing the Unique IP Issues of Data and AI in Transactions

Reminder- Important Proprietary Rights Should be Addressed in Multiple Areas When Using AI and Data:

(1) Input data, including training data and validation data
(2) Algorithms/models applied to the data
(3) Output data (derived data)
(4) Updates to the algorithms/models (code) created by the application to the data
(5) The “learnings” –separate from the updates to the algorithms-arising from application of the code to the data

When contracting around use of AI and use of data, the contract needs to address the scope of each party’s rights to own and/or to use data, code, improvements and results, the economic rights that flow from the use of any developments, and the allocation of risks of use

Ownership or License – Do you Care?

Input data (including training and validation data)-RETAIN OWNERSHIP

Grant a license, don't assign the data

License terms to consider-

- Where does the data sit?
- Duration of the license
- Rights to de-identify the data
- Rights to combine the data with data from others
- Sublicense rights- will you allow the licensee to provide access to others, and if so, how will you protect your data?

Ownership or License –

Algorithms/code applied to the data- RECEIVE A LICENSE

Will assume are proprietary to the third party, and you would not expect to receive ownership

Even for suggestions you make, and "developments" that arise (unless you could use the developments without access to the underlying code or algorithm)

Expect to receive a license for your use

License terms to consider-

- Who is hosting the algorithm/code (and what does that mean about where your data is being accessed?)
- Standard topics of a technology license- scope of rights, term, renewal rights, price protections, understanding use limits, support/uptime commitments, security and privacy considerations (is the third-party tool built/hosted using good security practices in mind).
- Even if you don't receive ownership, can you receive VALUE for your contributions?

Ownership or License –

Output data-OPEN FOR DEBATE

Approach may vary depending on the level of ‘modification’ to the data, and whether it has been combined with other data sources

Is the resulting database a derivative work? Maybe.

Focus on rights less than on ownership, including upon termination.

- Do you want a copy of any resulting data?
- How long can you use it, and how? How long can the vendor use it, and how?
- Can the resulting data be ‘stripped’ from the underlying algorithm/code?
- Do you want VALUE from subsequent use of resulting data?
- Do you need to protect privacy considerations in resulting data? (no re-identification if it was de-identified)

Ownership or License –

Improvements to the algorithm/code- RECEIVE A LICENSE

Is it possible you have some claim to ownership of improvements to an algorithm made by applying it to your data? Maybe, if there is enough data included in the improved code… but likely not.

Focus again on rights to use (yours and theirs), VALUE, and risk allocation.

- Do you expect to receive a benefit b/c the third-party product has been improved through the mere application to your data? Maybe
- Do you need to understand how much of your data is ‘embedded’ in the improved code- yes- and consider whether by allowing that, and allowing the vendor to continue to use, you are in effect selling data. Where will the data sit?
- Protect yourself from downstream risk- no liability to you if the updated code/algorithm infringes, fails to perform, etc.

Ownership or License –

Insights gained from application of the algorithm/code to the data- OPEN

Which humans are involved, if any?

(are you using the AI tool, e.g. deciding what problem to tackle and applying it to discover something/verify something?—OWN THE RESULTING IP

(is someone else using the tool as applied to your data, as a service?- ADDRESS VALUE TO YOU, BUT NO OWNERSHIP AND LIKELY NO LICENSE)

Allocation of Risks-if you DO Share the IP Ownership of Resulting Data, Resulting Code/Algorithm, Resulting Inventions

- Allocation of IP Risks/Costs Arising from Use
  - *Prosecution of patents/protection of trade secrets*
    - *Understand who is in charge, who bears the cost*
  - *Defense of Infringement claims – will the provider of AI tools/user of AI tools accessing your data defend you from third party IP claims*
    - *arising from the use of the AI engines*
    - *arising from the use of resulting/developed data base*
    - *arising from the use of developed products*
  - *Will you defend the provider for the decisions YOU make based on your use of the tool?*

Health Law and Other Regulatory Considerations

Key Legal Issues

- FDA
- Reimbursement
- Fraud and Abuse
- Licensure and Corporate Practice of Medicine
- Information Blocking and Interoperability
- Liability Issues
- Privacy and Security
- Ethics-avoiding bias

FDA

- FDA's jurisdiction over "devices"
  - When should software be considered an FDA regulated "device"?
- FDA's approach to regulating digital health
  - "Encourage innovation"

Reimbursement

- Payor reimbursement questions
- False Claims Act exposure?

Fraud and Abuse

Federal Laws

Anti-Kickback

Stark Self-Referral Prohibition

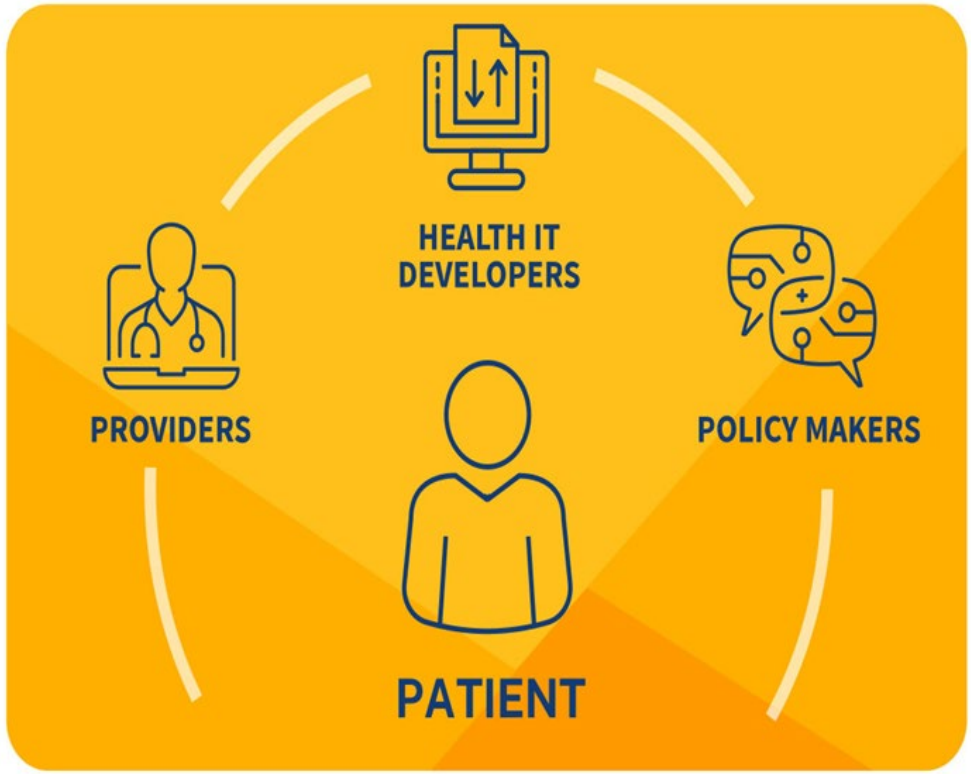
State Laws

State anti-kickback and self-referral prohibitions

Fee-splitting prohibitions

Information Blocking and Interoperability

Goal of seamless and secure access, exchange, and use of electronic health information



Liability Issues

- Providers
- Malpractice Liability
  - *When should providers override algorithms?*
- Informed Consent
  - *What about AI-based, automated telemedicine?*
  - *Need for post-hoc explanations to fulfill duty to obtain informed consent?*
- Developers
  - *Learned intermediary doctrine*

Liability Issues

- Remember duties to patients
- Evaluate AI software capabilities
- due diligence; continual process
- Contractual protections
  - *Representations/warranties, indemnification, insurance, etc.*
- Pay attention to legal/regulatory developments
- The future of AI in clinical-decision making?

Ethical Use of AI

- Concerns:
  - *Data Bias and Algorithmic Fairness*
  - *Reliability and Safety*
  - *Informed Consent*
  - *Accountability, **Transparency**, and Consent*
  - *Privacy*

Ethical Use of AI

- Voluntary and involuntary regulation:
  - *FTC Guidance, Blog Posts*
  - *Industry/Other Guidelines (World Health Organization, Assoc. of British Pharma Industry, AI Councils)*
  - *Regulations (EU)*
  - *Internal policies (AstraZeneca, Novartis, Sanofi)*
  - ***Coalition for Health AI***

Coalition for Health AI- “Guidelines and Guardrails”

- “The Coalition for Health AI (CHAI™) will build a consensus-driven framework to:
- Define core principles and criteria for health AI developers, end-users, and health care organizations to evaluate, monitor and report health AI systems throughout their lifecycle.
- Generate and promote a standard labeling schema for providing transparency to health AI end-users / consumers aiming to increase credibility of health AI systems.”

Presenters

Megan Bowman
Attorney
612.492.7216
mbowman@fredlaw.com

Ryan Johnson
Attorney
612.492.7160
rjohnson@fredlaw.com

Ann Ladd
Attorney
612.492.7124
aladd@fredlaw.com

Thank you!

Fredrikson

Where Law and Business Meet®