AI Litigation Risks for the Medical Technology Industry

August 29, 2023

Presented by:

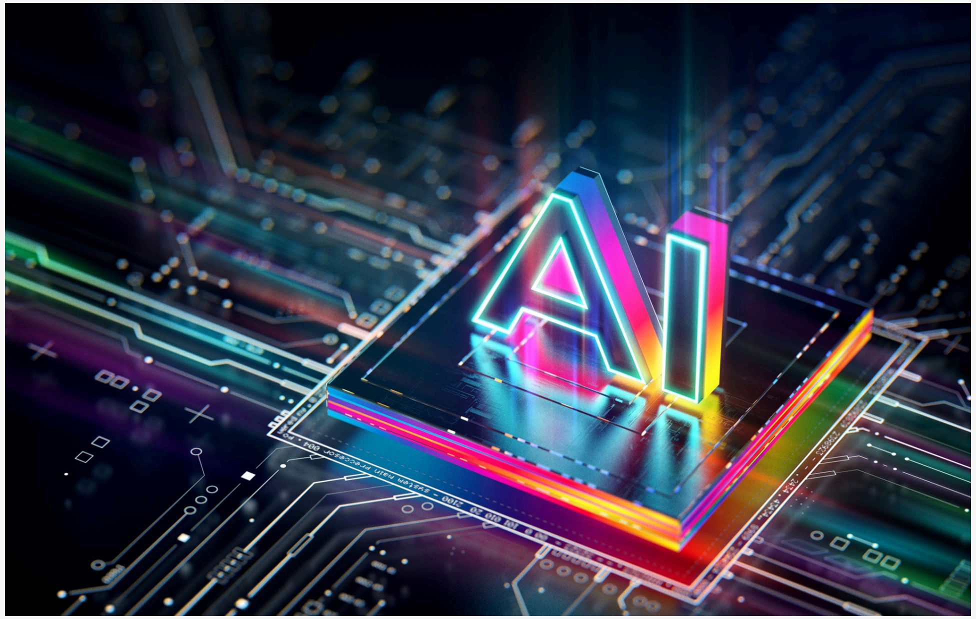
Jenny Colgate, Partner

Jennifer Maisel, Partner

ROTHWELL FIGG

What is artificial intelligence (AI)?

Artificial Intelligence (AI) and Machine Learning (ML) can be described as a branch of computer science, statistics, and engineering that uses algorithms or models to perform tasks and exhibit behaviors such as learning, making decisions, and making predictions. ML is considered a subset of AI that allows models to be developed by training algorithms through analysis of data, without models being explicitly programmed.

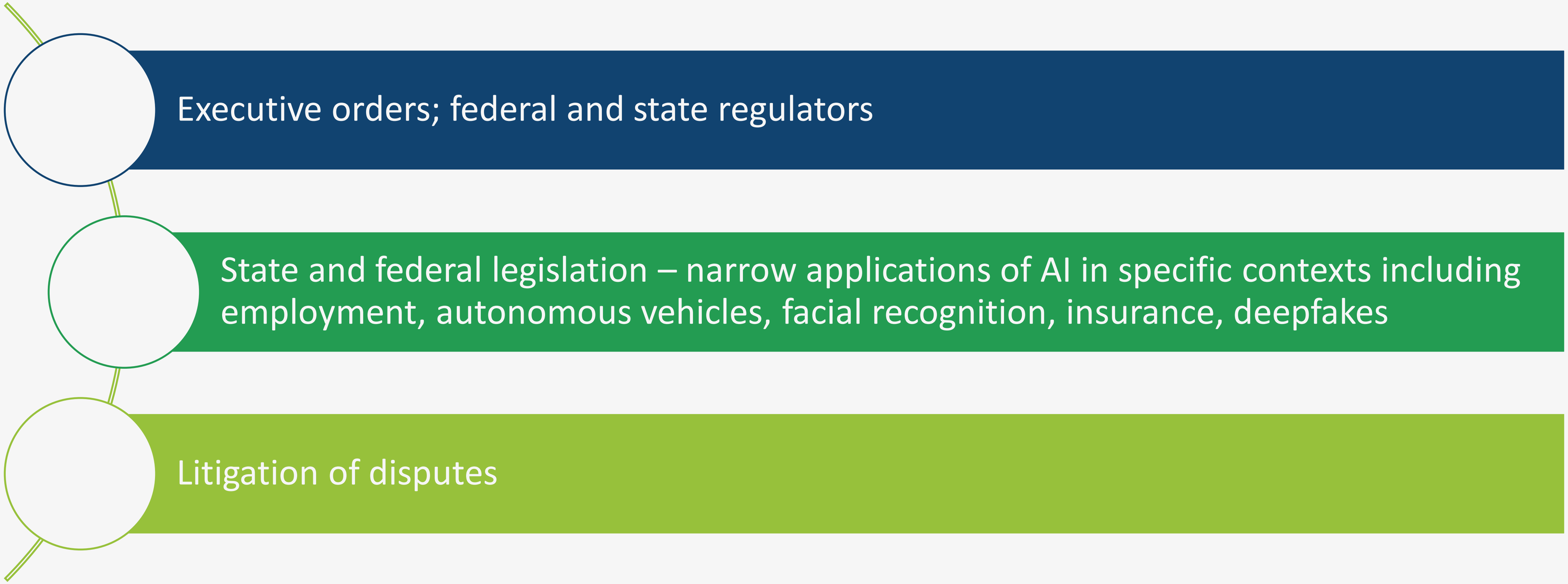


Source: https://www.fda.gov/science-research/science-and-research-special-topics/artificial-intelligence-and-machine-learning-aiml-drug-development

How is AI used in the MedTech industry?

- Drug development
- Software in a medical device
- Software as a medical device
- Software used to manufacture a medical device
- Speeding up medical discoveries

Regulation of AI



- Executive orders; federal and state regulators
- State and federal legislation – narrow applications of AI in specific contexts including employment, autonomous vehicles, facial recognition, insurance, deepfakes
- Litigation of disputes

Regulation of AI - Federal

2019 Executive Order 13859, "Maintaining American Leadership in Artificial Intelligence," jump-started significant, coordinated federal activity focused on balancing the need for regulation of AI with the demands of innovation

January 26, 2023 – NIST’s AI Risk Management Framework

April 3, 2023 – FDA’s "Marketing Submission Recommendations for a Predetermined Change Control Plan for Artificial Intelligence/Machine Learning (AI/ML)-Enabled Device Software Functions”

NIST Risk Management Framework

- Govern
- Map
- Measure
- Manage

Overview of AI Litigation Risks

Activities that could pose risk

- Training data
- Deployment of AI systems
- Use of AI systems

Examples of specific claims

Litigation Risks: “Radioactive” Training Data

- Personal and sensitive data – Notice? Authorization?
- Third-party intellectual property rights
- Contractual limitations / scraping and terms of use
- Training data purchased from others – Reps & Warranties?

Litigation Risks: Deployment of AI Systems

- NIST – AI Risk Management Framework
- Human in the loop / "gut check" on automated decision making
- Warnings and disclaimers
- Labeling and watermarking of AI-synthesized content
- Edge cases and product liability concerns

Litigation Risks: Use of AI Systems

Beware of open/public AI systems (as opposed to enterprise AI systems) because any data you enter can be used to “train” the system (which can breach contracts, affect trade secret protection, violate corporate policies).

- For example, using AI chatbot to diagnose medical condition

Samsung employees made headlines several months ago after they leaked sensitive code to ChatGPT.

Examples of Claims for AI-Related MedTech Litigation

- Breach of contract
- Copyright infringement
- Patent infringement
- Unfair competition
- Data privacy and security
- Trade secret misappropriation
- Torts

Breach of Contract

Failure to abide by third party agreements, including website terms of service

- *hiQ Labs, Inc. v. LinkedIn Corp.*, No. 17-CV-03301-EMC (N.D. Cal. Nov. 4, 2022). LinkedIn's User Agreement forbidding "scraping, crawling, or spidering the Server" unambiguously prohibited hiQ's scraping and unauthorized use of the scraped data.

Copyright Infringement – "Radioactive" Data!

- Andersen et al v. Stability Ai Ltd. - unauthorized use of copyrighted artwork to train AI system
- Doe 1 et al v. GitHub, Inc. et al. - unauthorized use of open source software to train AI system
- Getty Images (US), Inc. v. Stability Ai, Inc. – unauthorized use of photos to train AI system
- Kadrey et al. v. Meta Platforms – unauthorized use of books to train AI system
- Silverman et al. v. OpenAI, Inc. – unauthorized use of books to train AI system
- Tremblay et al. v. OpenAI, Inc. – unauthorized use of books to train AI system

Patent Infringement

Medical technology is an active area of patent enforcement

Recent examples from the software/MedTech industry reflect importance of patent eligibility

- *MED-EL Elektromedizinische Gerate GES.M.B.H. v. Advanced Bionics, LLC*, No. 1:18-CV-01530-JDW, 2023 WL 2186443, at *3-5 (D. Del. Feb. 23, 2023) – cochlear implants
- *Murj, Inc. v. Rhythm Mgmt. Grp., LLC*, 622 F. Supp. 3d 109, 118 (D. Md. 2022) – data management software for implantable cardiac devices

Unfair Competition Litigation

Reverse engineering and investigation of competitors’ products

- *Philips North America v. Image Technology Consulting* – use of fake and/or unauthorized certificates to hack Philips’ access control mechanisms on Philips systems to gain unlicensed and unauthorized access to Philips systems, including software to modify medical devices

Data Privacy Litigation

Beware of “radioactive” data containing personal information

- Is the use in AI-use disclosed? Is it authorized?
- What regulations apply?
- *P.M. et al v. OpenAI LP et al* – unauthorized use of personal data in connection with development and training of AI systems

The more data is aggregated and analyzed, the more it will expose identifying information. Information that was not “personal” may become personally identifying.

Data Privacy – Biometric Information

Heightened sensitivities around collection and use of biometric information.

Class action litigation, e.g., Illinois Biometric Information Privacy Act (“BIPA”) and exclusions/carve outs

FTC recently issue a Biometric Information Policy Statement warning that the increasing use of consumers’ biometric information and related technologies, including those powered by machine learning, raises significant consumer privacy and data security concerns and the potential for bias and discrimination.

Data Privacy – Other Private Rights of Action – "My Health, My Data"

Aims to regulate processing of health-related data outside of HIPAA; very broad – includes information *inferred* or *derived*

Provides a number of consumer rights (access, confirm if collecting/selling/sharing, withdraw consent to collect/share, have data deleted)

Provides a private right of action to enforce (effective in 2024)

- Given broad definitions and rights, and PRA, expect litigation against AI-related non-HIPAA med-tech

Data Privacy – FTC Enforcement – Unauthorized Sharing of Consumer Data for Advertising

GoodRx - failure to notify consumers and others of its unauthorized disclosures of consumers' personal health information to Facebook, Google, and other companies

Easy Healthcare Premom fertility app - deceiving users by sharing their sensitive personal information with third parties, including two China-based firms, disclosed users' sensitive health data to AppsFlyer and Google, and failure to notify consumers of these unauthorized disclosures

BetterHealth - On July 14, 2023 FTC finalized an order requiring BetterHealth to pay $7.8M and banning the service from sharing sensitive health data to third parties (including Facebook and Snapchat) for advertising

Data Privacy – FTC Enforcement – Failure to Protect Privacy and Security of PHI

1Health/Vitagene – June 16, 2023 – FTC charged genetic testing firm which left genetic and health data unsecured, deceived customers about the ability to get the data deleted, and changed its privacy policy retroactively without notifying and obtaining customer consent.

Effects of security issues: misdiagnoses, mistakes during surgery, malfunctioning devices, shut down hospital systems, etc.

HIPAA violations / data security violations

Computer Fraud and Abuse Act

Trade Secret Litigation

Trade secrets

- Commercially valuable because it is secret
- Known only to a limited group of people
- Subject to reasonable steps to keep the information secret (e.g., confidentiality agreements with business partners and employees)

Trade secrets examples: data sets, manufacturing processes, software algorithms, takeaways (positive or negative)

Trade secret misappropriate claims often arise when employees move between companies, or when business deals go bad.

Tort Litigation – “Bad” Training Data

If an AI-based medical device is trained using data from a different population than it is being used on in practice, it could produce recommendations and output that is no longer proper?

- For example, imagine if the AI-enabled surgery visualization model was trained using data from young health population, and had issues when applied to older population with heath issues.

Obligation to update data? If an AI-tool is trained using “old” data, recommendations may be flawed.

- For example, AI-system trained before AlphaFold predicted the structure of more than 200 million proteins vs. system trained after, with the benefit of that data

Tort Litigation - Mistakes

What happens when an AI-tool makes a mistake (just like when ChatGPT gives a wrong answer)? For example, the AI-enabled surgery visualization model fails to clearly show the tissue, and the surgeon makes a mistake? Does the surgeon have a responsibility to “double check” the AI model?

What happens if a prosthetic arm suddenly moves on its own and pushes someone onto a train track? How does the user prove he did not do it/ have control over it?

What if an AI-assisted detection tool fails to draw a green box around an area that ends up being cancer? Who is responsible – the doctor or the AI tool?

Should older, traditional screening tools continue to be used as back-up, and if so, how often? What are the limits? What if the traditional tool is more expensive, labor intensive, and intrusive?

Thank you!

Jenny Colgate
Partner
jcolgate@rothwellfigg.com

Jennifer Maisel
Partner
jmaisel@rothwellfigg.com