



Legal Perspective: Data Privacy Considerations Within Medical Information Operations

9th Customer Centric Medical Information Conference
Colin J. Zick, Esq.
Foley Hoag LLP

April 24, 2024

Decoding Current Regional and Global Patient Privacy Trends: Facebook Pixel Cases



- *John Doe, et al., Plaintiff, v. Atrius Health, Inc., Defendant*, Civil Action No. 22-12196-FDS

- **MEMORANDUM AND ORDER ON PLAINTIFFS' MOTION TO REMAND**

- SAYLOR, C.J. This is a putative class action against a non-governmental healthcare provider alleging systematic violation of patients' state-law privacy rights. The complaint was originally filed in the Norfolk County Superior Court before being removed to federal court under 28 U.S.C. §1442(a)(1). Plaintiffs have moved to remand, contending that federal subject-matter jurisdiction is lacking because defendant has failed to meet the requirements of §1442(a)(1). For the reasons set forth below, the motion to remand will be granted.

- **I. Background**

- **A. Factual Background**

- ♦ Atrius Health, Inc. is the parent company for more than 30 medical practices in Massachusetts. (Compl. ¶18). Its principal place of business is in Massachusetts, and it is a Massachusetts corporation. (*Id.*). Atrius operates websites designed for patient communications, scheduling, searching for physicians, paying bills, requesting medical records, learning about medical issues, and joining support groups. (*Id.* ¶¶19-20).
 - ♦ The complaint alleges that plaintiffs visited defendant Atrius's websites in 2022 and entered data, including personal health information. (*Id.* ¶¶88, 91). The complaint alleges that Atrius's websites utilized Facebook's Meta Pixel tool—a computer code that tracks users' activities on a website, allowing that information to be processed and analyzed by Facebook and shared with third-party advertisers. (*Id.* ¶¶54-56, 92).

- *John Doe 1 and John Doe 2 v. Boston Medical Center*

**MEMORANDUM OF DECISION AND ORDER ON
DEFENDANT'S MOTION TO DISMISS**

Plaintiffs John Doe 1 and John Doe 2 commenced this putative class action against defendant Boston Medical Center Corporation (“BMC”), alleging that it used digital marketing tools on its website that illegally redirected website users’ personal information, and the contents of their communications with BMC’s website, to third parties Google and Meta. On the basis of these allegations, the Complaint asserts claims for violations of the Massachusetts Wiretap Statute, G.L. c. 272, § 99, and invasion of privacy under G. L. c. 214, § 1B. Presently before the court is BMC’s motion to dismiss. After a hearing on July 18, 2023, and consideration of the parties’ submissions, the motion is **DENIED**.

Critical Legislation and Their Impact on Medical Information Teams

- The powers of the FTC:
 - FTC's health breach notification rule
 - The proposed American Privacy Rights Act
- California Consumer Privacy Act and HIPAA
- The proposed Massachusetts Information Privacy and Security Act

The Lost World: FTC's Health Breach Notification Rule

- Show of hands: Before today, who has heard of the FTC breach notification rule?
- 16 CFR Part 318: The Rule requires vendors of personal health records and related entities to notify consumers following a breach involving unsecured information. In addition, if a service provider to one of these entities has a breach, it must notify the entity, which in turn must notify consumers. The Final Rule also specifies the timing, method, and content of notification, and in the case of certain breaches involving 500 or more people, requires notice to the media.
<https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/health-breach-notification-rule>.
- Even the FTC seems to have forgotten about it, until recently.
<https://www.ftc.gov/news-events/press-releases/2021/09/ftc-warns-health-apps-connected-device-companies-comply-health>.

The proposed American Privacy Rights Act

- Bipartisan Senate and House lawmakers announced on April 7, 2024, that they had reached a deal on draft Federal privacy legislation – the American Privacy Rights Act (“APRA”).
- APRA would be administered by the Federal Trade Commission, and apply to “covered entities,” which are sizeable businesses that engage in collecting, processing, retaining, or transferring consumer data. “Small businesses” – defined as businesses with \$40 million or less in annual revenues, that process the data of fewer than 200,000 individuals, and that do not earn revenue from the transfer of data to third parties – would be exempt from APRA.
- Covered entities would be required to practice “data minimization” with respect to personal data: collecting or transferring biometric or genetic information or transferring sensitive information – would require affirmative express consent from consumers.
- Covered entities would be required to publish privacy policies detailing their data privacy and security practices, including what data is collected, the categories of third parties to which data is transferred, and how consumers can exercise individual data controls and opt-out rights.
- Consumers would have the right to access their personal data, delete that data, and correct inaccuracies. Consumers would also be able to opt-out of the transfer of personal data and the opt-out of the use of personal data for targeted advertising.

The proposed American Privacy Rights Act (cont.)

- There would be an additional category of “large data holders” under APRA, defined as entities with \$250,000,000 or more in annual revenue, that process the data of more than 5,000,000 individuals (or 15,000,000 portable devices, or 35,000,000 connected devices that can be associated with an individual), or that process the “sensitive data” of more than 200,000 individuals.
 - “Sensitive data” would include data such as health information, biometrics, genetic information, and similar information.
 - Large data holders, would be required to retain and publish 10 years’ worth of prior privacy policies, report metrics on addressing data requests from consumers, designate both a privacy and security officer, file annual certifications related to internal controls with the FTC, and both share with the FTC and publicly disclose impact assessments related to the use of algorithms that may reasonably create disparate impacts in terms of race, color, religion, national origin, gender, or disability.
- APRA could be enforced not only by the FTC but also state attorneys general, and create a private right of action for consumers to recover damages, obtain injunctive or declaratory relief, and recover attorneys’
 - In the case of actions related to biometric and genetic information, consumers would also be able to recover damages consistent with what is currently available under Illinois’ Biometric Information Privacy Act and Genetic Information Privacy Act; similarly, California residents would be able to recover damages consistent with what the California Privacy Rights Act currently provides in relation to data breaches.
- Much state data privacy legislation would be pre-empted by APRA.
 - Entities subject to Federal laws that contain data security requirements (e.g., HIPAA) would be deemed to be in compliance with the data security requirements of APRA, although would not necessarily be deemed to be in compliance with respect to all provisions of APRA.

California Consumer Privacy Act and HIPAA

- CCPA went into effect January 1, 2020; it regulates the privacy of health information of California residents, but exempts:
 - Protected Health Information (PHI)
 - Personal information that HIPAA-covered entities handle like PHI
- Most likely to benefit from this exemption:
 - Health care providers
 - Health insurers
- These companies collect personal information that is not exempt:
 - Employment information
 - Electronic network activity information (e.g., cookies)
 - Labs doing return to work COVID screening (not diagnostic testing)
- More laws like this have followed and will continue to follow

The Proposed Massachusetts Information Privacy and Security Act

■ Key elements of the proposed MIPSAs:

- Applies to non-HIPAA “personal information”
- Similar in many respects to newish laws in California, Washington, Colorado, Virginia, and Connecticut
- Would apply to entities with revenues exceeding \$25M per year; determines the processing of at least 100,000 individuals; or is a data broker

■ What would change?

- Far broader scope of information covered than HIPAA or existing Massachusetts law
- Risk assessments
- Private right of action

Is It Customer Services or a HIPAA Violation?

■ From Modern Healthcare:

- A patient publicly criticized CVS Health, its executives and Caremark, its pharmacy benefit manager, for requiring her and other commercial enrollees to [switch from Bristol-Myers Squibb's Eliquis to Janssen Pharmaceuticals' Xarelto](#), both anticoagulants that experts say have not been proven interchangeable through randomized control trials. Observational studies have concluded the two are not the same.
- The patient tagged the company and several of its executives, including its CEO, in multiple Twitter posts. She called out the business during public testimony before the Federal Trade Commission.
- Then she received an unexpected call from a CVS employee, who said he wanted to talk about her health history. It raises the question: by using information from her private Caremark account to perform customer service, were the federal laws on the disclosure of patient information violated?

Forecasting the Upcoming Changes to and Evolution of the Privacy Law Landscape: Use of AI for Medical Information Applications



- UMass Memorial Health:
 - partnership with Google Cloud
 - to use artificial intelligence to identify good candidates for advanced drug therapies
 - for heart disease and diabetes, including GLP-1 agonists like Ozempic and Mounjaro
[Boston Business Journal](https://www.bizjournals.com/boston/news/2024/03/07/umass-memorial-google-cloud-partner-on-new-tool.html?utm_source=st&utm_medium=en&utm_campaign=ae&utm_content=BO&j=34604218&senddate=2024-03-07&empos=p7), March 7, 2024, available at https://www.bizjournals.com/boston/news/2024/03/07/umass-memorial-google-cloud-partner-on-new-tool.html?utm_source=st&utm_medium=en&utm_campaign=ae&utm_content=BO&j=34604218&senddate=2024-03-07&empos=p7.
- Amazon:
 - training an AI chatbot
 - to handle incoming patient messages, and
 - address administrative queries for One Medical
[Becker's Health IT](https://www.beckershospitalreview.com/disruptors/amazon-training-chatbot-for-healthcare-report.html?origin=CIOE&utm_source=CIOE&utm_medium=email&utm_content=newsletter&oly_enc_id=1905F7435578H3V), March 1, 2024, available at https://www.beckershospitalreview.com/disruptors/amazon-training-chatbot-for-healthcare-report.html?origin=CIOE&utm_source=CIOE&utm_medium=email&utm_content=newsletter&oly_enc_id=1905F7435578H3V.
- Nebraska Medicine:
 - using AI at two of its primary care clinics
 - to detect diabetic retinopathy in patients
[Modern Healthcare](https://www.modernhealthcare.com/digital-health/nebraska-medicine-ai-artificial-intelligence-diabetic-retinopathy?utm_source=modern-healthcare-alert&utm_medium=email&utm_campaign=20240304&utm_content=hero-headline), March 4, 2024, available at https://www.modernhealthcare.com/digital-health/nebraska-medicine-ai-artificial-intelligence-diabetic-retinopathy?utm_source=modern-healthcare-alert&utm_medium=email&utm_campaign=20240304&utm_content=hero-headline.

How Is AI Being Used for Healthcare Applications? (cont.)



- GE HealthCare 'actively pursuing' AI for all products:
 - GE HealthCare is among a growing number of radiology companies embracing AI. The company is developing its App Orchestrator, a technology that it said would help providers manage imaging software from different technology vendors. The company said it plans to invest in AI technologies tied to physical devices and others that are cloud-based software. Last month, the company announced plans to acquire medical imaging AI company MIM Software for an undisclosed amount. It intends to fold MIM's imaging analytics and digital workflow capabilities into its precision medicine offerings. In February 2023, it acquired Caption Health, a software company focused on AI-assisted ultrasound scans. The company plans to use Caption Health's AI to integrate real-time guidance into ultrasound systems for clinicians and non-expert users to capture better quality images of the heart.
- Hims & Hers says AI can help retain customers:
 - Telehealth company Hims & Hers announced in November it was testing an AI and machine learning clinical decision support feature that could suggest treatments for some mental health conditions. The company's AI-driven MedMatch technology can recommend clinicians prescribe certain medications and doses, could contribute to customer retention.
- Insurers using AI to improve customer service:
 - Insurers are removing repetitive tasks from workflows by using AI to help with responses to consumer inquiries, updating provider directories and summarizing interactions with customers and patients.
 - An insurer has used AI and machine learning to improve the rate in which member questions are resolved when someone reaches out to their customer service team.
 - UnitedHealth and Cigna have been separately accused of using automated tools to deny some claims.
- R1 RCM examines AI for denials and eligibility:
 - R1 RCM, a tech company that handles providers' billing and claims management services, has developed AI models that can help clinicians identify a patient's insurance eligibility more efficiently. They also help health systems streamline writing an appeal for a complex clinical denial.
 - R1 RCM sees autonomous coding as an opportunity for generative AI use cases.

Modern Healthcare, March 1, 2024, available at https://www.modernhealthcare.com/digital-health/ge-healthcare-unitedhealth-hims-hers-ai-uses?utm_source=modern-healthcare-alert&utm_medium=email&utm_campaign=20240301&utm_content=hero-readmore.

JAMA, April 15, 2024



Original Investigation | Health Informatics

AI-Generated Draft Replies Integrated Into Health Records and Physicians' Electronic Communication

Ming Tai-Seale, PhD, MPH; Sally L. Baxter, MD, MSc; Florin Vaida, PhD; Amanda Walker, MS; Amy M. Sitapati, MD; Chad Osborne, MD; Joseph Diaz, MD; Nimit Desai, BS; Sophie Webb, MS; Gregory Polston, MD; Teresa Helsten, MD; Erin Gross, MD; Jessica Thackaberry, MD; Ammar Mandvi, MD; Dustin Lillie, MD; Steve Li, MD; Geneen Gin, DO; Suraj Achar, MD; Heather Hofflich, DO; Christopher Sharp, MD; Marlene Millen, MD; Christopher A. Longhurst, MD, MS

Abstract

IMPORTANCE Timely tests are warranted to assess the association between generative artificial intelligence (GenAI) use and physicians' work efforts.

OBJECTIVE To investigate the association between GenAI-drafted replies for patient messages and physician time spent on answering messages and the length of replies.

DESIGN, SETTING, AND PARTICIPANTS Randomized waiting list quality improvement (QI) study from June to August 2023 in an academic health system. Primary care physicians were randomized to an immediate activation group and a delayed activation group. Data were analyzed from August to November 2023.

EXPOSURE Access to GenAI-drafted replies for patient messages.

MAIN OUTCOMES AND MEASURES Time spent (1) reading messages, (2) replying to messages, (3) length of replies, and (4) physician likelihood to recommend GenAI drafts. The a priori hypothesis was that GenAI drafts would be associated with less physician time spent reading and replying to messages. A mixed-effects model was used.

RESULTS Fifty-two physicians participated in this QI study, with 25 randomized to the immediate activation group and 27 randomized to the delayed activation group. A contemporary control group included 70 physicians. There were 18 female participants (72.0%) in the immediate group and 17 female participants (63.0%) in the delayed group; the median age range was 35–44 years in the

Key Points

Question Would access to generative artificial intelligence–drafted replies correlate with decreased physician time on reading and replying to patient messages, alongside an increase in reply length?

Findings In this quality improvement study including 122 physicians, generative AI-drafted replies correlated with increased message read time, no change in reply time, and significantly longer replies. Physicians valued AI-generated drafts as a compassionate starting point for their replies and also noted areas for improvement.

Meaning These findings suggest generative AI was not associated with reduced time on writing a reply but was associated with longer read time, longer replies, and perceived value in making a more compassionate reply.

What Laws Apply to the Intersection of Healthcare and AI?

■ Privacy and Data Security:

- Health Insurance Portability and Accountability Act (HIPAA): HIPAA sets standards for the protection of sensitive patient health information, known as protected health information (PHI). Any AI applications or systems used in healthcare must comply with HIPAA regulations to ensure the privacy and security of patient data.
- FTC on non-HIPAA health information and separately regulating AI.
- State laws on non-HIPAA health information and separately regulating AI.
- General Data Protection Regulation (GDPR): In regions covered by GDPR, such as the European Union, strict regulations govern the collection, processing, and storage of personal data, including health data. AI applications in healthcare must comply with GDPR requirements to protect patient privacy and obtain appropriate consent for data usage.

■ Medical Device Regulation:

- President Biden signed an executive order on October 30, 2023, and invoked the Defense Production Act to establish the first set of standards on the use of artificial intelligence in healthcare and other industries.
- FDA: In the United States, the Food and Drug Administration (FDA) regulates medical devices and software used in healthcare, including AI-based technologies. Depending on the intended use and risk level, AI applications may need to undergo FDA approval or clearance processes to ensure safety and effectiveness.
 - ✦ The process involves the FDA reviewing clinical data to ensure the AI-enabled device or software product is safe, effective and only does what it's marketed to do.
 - ✦ Between 1995 and October, the FDA approved, designated or cleared 692 AI-enabled devices.
- Other Medical Device Regulations: AI-based medical devices may be subject to specific regulations governing their design, development, manufacturing, and post-market surveillance. Compliance with medical device regulations, such as ISO 13485 and IEC 62304, is essential to ensure the quality and safety of AI-enabled healthcare products.
- Health AI companies that do business in Europe have to comply with the European Union's Artificial Intelligence Act, which took effect in February. The law categorizes AI into different categories of risk. It requires certain health AI developers to register their models into a database and be transparent with the data that informs their models.

What Laws Apply to the Intersection of Healthcare and AI? (cont.)

■ Reimbursement/Fraud and Abuse:

- Some regulatory guidance from the Centers for Medicare and Medicaid Services has come in response to the alleged use of AI for prior authorization and claim denials.
- Major insurers UnitedHealth Group, Humana and Cigna are fighting lawsuits alleging they use AI and other automated tools to routinely decline coverage for post-acute care and other services. The insurers have denied the allegations and Humana filed a motion to dismiss the lawsuit.
- In February, CMS issued guidance to clarify how Medicare Advantage insurers could use AI to assess coverage decisions. CMS said insurers can't use AI tools to override benefits rules and medical necessity standards.
- The Department of Justice has begun subpoenaing pharmaceuticals and digital health companies to learn more about the role artificial intelligence may play in facilitating anti-kickback and false claims violations.

■ Quality of Care and Transparency:

- A White House executive order instructed the Department of Health and Human Services to develop new AI-specific regulatory strategies addressing equity, safety, privacy, and quality for AI in health care before April 27, 2024.
- The Office of the National Coordinator for Health Information Technology finalized a rule in December that set transparency standards for the development of AI in health IT software.
- Republican Utah Gov. Spencer Cox signed the Artificial Intelligence Policy Act earlier this month. Under the law, regulated occupations, which the state says include many professions within healthcare, must disclose any time they have generative AI, such as a chatbot, interact with a consumer.
- Republican Georgia Gov. Brian Kemp signed a law in May that permits the use of AI for eye assessments to generate a prescription for contact lenses or glasses. Some state legislators in Georgia proposed a bill in January that would limit how clinicians could use of AI within healthcare.

What New Laws Under Consideration Might Apply to the Intersection of Healthcare and AI?



- The EU already has a draft law, the EU AI Act: <https://artificialintelligenceact.eu/the-act/>.
- Congress is circling healthcare and AI warily:
 - On February 1, 2024, Reps. Troy Balderson (R-Ohio) and Robin Kelly (D-Ill.) launched the bipartisan Congressional Digital Health Caucus at a Capitol Hill event focused on AI.
 - ◆ Representatives from Amazon, Google, Microsoft, Hippocratic AI and the Consumer Technology Association participated in the briefing.
- There are 14 bills pending in Congress that include the terms “health” and “artificial intelligence.”
- Sen. Mike Rounds (R-S.D.) proposed that the Senate Finance Committee look at using Medicare and Medicaid programs to fund AI innovations in health care, as part of a new framework that Senate leaders on AI are creating for Congress.
- The FDA and ONC have backed the idea of AI assurance labs, which could validate and monitor AI in healthcare.

What Activities at the Intersection of Healthcare and AI Are *Not* Being Regulated?

- Large language models (LLMs) that summarize clinical notes, medications, and other forms of patient data are in advanced development and could soon reach patients without FDA oversight or approval.
 - Summarization is a complex activity, and variation in LLM-generated summaries could exert as yet unknown effects on clinician decision-making.
- Liability: Who should be held responsible when things go wrong?
 - An HHS proposal from 2022 would largely leave health care providers on the hook for verifying that AI tools work and don't lead to discriminatory outcomes.
 - Physicians vehemently oppose the proposal, and would like Congress to step in.
- Insurance:
 - It's not required.



Colin Zick

Partner
Chair, Healthcare Compliance Practice
Co-Chair, Privacy and Data Security Practice
Boston

+1.617.832.1275

czick@foleyhoag.com

- Practice focused on health care and compliance issues, often involving intersection of those two subjects in investigations, administrative proceedings, or litigation.
- Work has particular emphasis on compliance issues related to life sciences, pharmaceutical and medical device companies, laboratories, hospitals, health care providers, and provider organizations.
- Compliance work includes helping clients establish and maintain effective compliance programs.
- Defends clients in disputes alleging kickbacks, overpayments, and billing and coding problems, and represents clients before state health care licensing and regulatory entities.
- Counsels health care, life science, technology and consumer-facing clients on issues involving information privacy and security (including HIPAA and other federal and state data privacy and security laws, EU/GDPR privacy and security issues, AI, and data breach response).
- Co-founded firm's Data Security and Privacy Practice Group and regularly contributes to "Security, Privacy and the Law" blog.
- Practice covers work on health care transactional matters, including data licensing, M&A, joint ventures, creation of new entities, drafting and negotiation of management service and employment contracts, creation of patient assistance programs, and negotiating data use and clinical trial agreements.

