THOMSON REUTERS
Westlaw®

MedTech update 2020 — Legal and regulatory issues to watch for in the medical technology industry in the new year: Health information privacy and data protection

By Jo-Ellyn Sakowitz Klein, Esq., CIPP/US; Mallory Jones, Esq., CIPP/US; Rachel Kurzweil, Esq.; Caroline Kessler, Esq.; and Taylor Daly, *Akin Gump Strauss Hauer & Feld

FEBRUARY 14, 2020

Medical device and diagnostics companies and laboratories should anticipate significant legal, regulatory and market changes in 2020 that will have a lasting impact on the industry. From revisions to how the government regulates value-based care, to shifts in the marketplace for medtech mergers and acquisitions (M&A), 2020 will prove to be another year of evolution.

Based on recent trends and developments, Akin Gump attorneys have prepared several articles to provide the medtech industry with a landscape overview of the following issues in the year ahead: Food and Drug Administration regulatory developments; federal health care programs; international trade; intellectual property (IP) litigation; False Claims Act enforcement and health information and privacy and data protection.

We plan to monitor and report on these developments and potential updates as the year unfolds.

HEALTH INFORMATION PRIVACY AND DATA PROTECTION

The past two decades marked a time of unprecedented change and development in the health information privacy and data protection landscape in the U.S.

As we move into 2020, here are a few key issues to watch in the health information privacy and data protection space, which are likely to have a substantial impact on medtech operations (including research and development), compliance activities and transactions:

Potential updates to the HIPAA regulations

The Health Insurance Portability and Accountability Act (HIPAA) regulations, which have been the dominant force in the health information privacy and data protection landscape since the interim final HIPAA privacy rule was promulgated in 2000, evolved significantly over the past two decades.

These changes were driven by statutory action, formal and informal regulatory action and increasingly steady enforcement, as well as by market forces and the new value proposition presented by big data and related tools.

The HIPAA privacy, security, enforcement and breach notification regulations were last overhauled by the omnibus rulemaking promulgated in 2013.

At the end of 2018, CMS issued a broad request for information[1] to help the agency identify and address aspects of HIPAA that hinder information sharing among health care providers, payers, patients and caregivers.

The HIPAA privacy, security, enforcement and breach notification regulations were last overhauled by the omnibus rulemaking promulgated in 2013.

The Fall 2019 Unified Agenda published November 20, 2019 (Unified Agenda), indicated that the HHS Office of Civil Rights (OCR) would release a notice of proposed rulemaking (NPRM) regarding updates to HIPAA by the end of 2019.

That did not happen, but we expect that NPRM will be released in early to mid-2020. Notably, OCR could propose changes to promote new or expanded disclosures related to value-based care, coordinated care and the opioid crisis, potentially including material changes to existing HIPAA access requirements.

Continued emphasis on interoperability

In March 2019, the HHS Office of National Coordinator for Health Information Technology (ONC) published a proposed rule aimed largely at improving access to health information. The Unified Agenda projected publication of the final rule in November of 2019.

The rule remains pending and is highly anticipated. Medtech companies should be prepared to evaluate their information sharing practices to ensure processes currently in place to protect

data privacy do not run afoul of anticipated provisions regarding information blocking.

Challenges may also arise in reconciling potentially competing privacy and security requirements under shifting federal and state regimes.

Targeted — and increasing — HIPAA enforcement activity

HIPAA enforcement activity has been building rather steadily since 2008. Last year, HHS OCR announced an initiative to focus on the rights of patients to access their medical information under HIPAA.

In September, OCR announced an $85,000 settlement with a hospital over the hospital's alleged failure to timely provide a patient with fetal heart monitor records from her pregnancy.

In December, OCR settled an enforcement action against a health care provider for allegedly failing to promptly provide a patient's health records to a third party upon the patient's request, as required by HIPAA.

We anticipate that more health care providers, as well as other entities that create, receive, maintain or transmit HIPAA-protected information, may face enforcement action in 2020 regarding patient access rights.

Overall, dollar amounts captured by regulators through settlements and penalties continue to climb, making HIPAA compliance an increasingly high-stakes endeavor at a time when the regulatory landscape is changing.

State law developments

State legislatures were active on privacy issues in 2019, and we anticipate that robust legislative activity will continue throughout the rest of 2020. States jumping into the privacy law space will add to the existing patchwork of state law requirements for health care entities, including medical device companies.

Notably, the expansive CCPA[2] took effect January 1, 2020. The CCPA includes exemptions based on HIPAA, but these exemptions do not cover the field. In particular, non-covered entities relying on HIPAA standards as a best practice may need to adjust their practices to satisfy differing CCPA requirements.

Further, questions remain regarding the extent to which standards for de-identification of personal information under the CCPA align with HIPAA's well-established de-identification provisions.

Additionally, the narrowness of the CCPA's exception for use of personal information in clinical research could create obstacles for the medtech sector.

Change is possible — for example, relevant amendments are pending — and 2020 is certain to be a critical year. Beyond California, states across the country have adopted or considered privacy laws that could have implications for the medtech industry, and this trend is expected to continue.

Congressional focus on privacy and data protection

As the second session of the 116th Congress takes off, Members of the Senate Commerce, Science, and Transportation Committee have continued negotiations on a bipartisan federal privacy bill, and the House Energy and Commerce Committee has begun to incorporate stakeholder feedback on its staff-level privacy draft released in December.

Critical issues debated have included whether legislation protecting online consumer privacy rights should include a private right of action and preempt state privacy law. We expect to see continued debate over these issues, and increasing Congressional interest in privacy matters, this year.

Continued privacy regulation and enforcement in Europe

The EU's GDPR entered its second year of enforcement this past May, and EU regulators have maintained an interest in health data.

In the past year, the EU Member State data protection authorities (DPAs) have issued fines for GDPR violations committed by hospitals and research organizations for issues related to health data, such as data breaches, insufficient data security practices and non-compliant processing activities.

Additionally, in January 2019, the European Data Protection Board (EDPB) — the EU body in charge of the application of the GDPR — issued an opinion on the interaction between the GDPR and the EU's Clinical Trials Regulation (CTR), which addressed, among other things, requirements regarding the legal basis for processing personal data in the course of a clinical trial (as required under GDPR Art. 6) and the ability to further use clinical trial data for other scientific purposes.

Further, there is an increasing awareness among the European population of their rights under the GDPR, including the right to complain to a DPA about an entity's data processing practices and activities.

The European Commission has noted that the DPAs have collectively received over 140,000 queries and complaints from data subjects since May 2018.

Medical device companies should be prepared for continued guidance and enforcement in Europe, particularly as regulators seek to harmonize the different regulatory frameworks, including, potentially, the European Medical Device Regulation (MDR).

Notes

[1] https://bit.ly/37m5CeB

[2] https://bit.ly/2OPcfjm

This article first appeared on the Westlaw Practitioner Insights Commentaries webpage on February 14, 2020.

ABOUT THE AUTHORS




(L-R) **Jo-Ellyn Sakowitz Klein** is a senior counsel at **Akin Gump Strauss Hauer & Feld**. Her practice focuses on assisting clients with issues arising under state and federal privacy, security and data breach notification laws and regulations, including HIPAA, the HITECH Act and Section 5 of the Federal Trade Commission Act. She can be reached at jsklein@akingump.com. **Mallory Jones** is an associate at the firm, representing a variety of health care entities including hospitals and health systems, academic medical centers, and pharmaceutical companies. She focuses on regulatory, transactional and advocacy matters related to privacy, food and drug law, and Medicare and Medicaid reimbursement. She can be reached at jonesm@akingump.com. Akin Gump associate **Rachel Kurzweil** advises entities in the health care industry and assists in matters related to the EU General Data Protection Regulation and state and federal privacy laws. She can be reached at rkurzweil@akingump.com. **Caroline Kessler** is an associate at the firm, where she advises companies in the U.S. health care industry. She assists in matters related to regulatory compliance, reimbursement, advocacy and transactional matters. She can be reached at ckessler@akingump.com. **Taylor M. Daly** (not pictured) is a public policy specialist at Akin Gump. She can be reached at tdaly@akingump.com. The authors are all located in the firm's Washington office. A version of this client alert was first published Jan. 7, 2020, on the Akin Gump website. Republished with permission.