US REGULATORY CONSIDERATIONS APPLICABLE TO DIGITAL HEALTH PROVIDERS AND SUPPLIERS – PART IV: OTHER POTENTIAL APPLICABLE LAWS

PRIMARY REGULATORY REGIMES RELEVANT TO MHEALTH

Date: 18 October 2021

By: Aiko Yamada

This final article in our four-part series examines other relevant laws digital health providers and suppliers should know.

If you missed our earlier articles, you can read about HIPAA in Part I and Part II, and the FDCA and other privacy considerations in Part III.

FEDERAL TRADE COMMISSION ACT (FTCA)

When companies tell consumers they will safeguard their personal information, the Federal Trade Commission (FTC) can and does act to ensure companies live up to their promises. The FTC has brought legal actions against organizations that have violated consumers' privacy rights, misled them by failing to maintain security of sensitive consumer information or caused substantial consumer injury. In many cases, the FTC has charged the defendants with violating laws related to unfair and deceptive trade practices.

As a recent example, a developer of a popular women's fertility-tracking app settled FTC allegations that it misled consumers about the disclosure of consumers' health data. As part of the proposed settlement, the developer is prohibited from misrepresenting: 1) the purposes for which it or entities to whom it discloses data collect, maintain, use or disclose the data; 2) how much consumers can control these data uses; 3) its compliance with any privacy, security or compliance program; and 4) how it collects, maintains, uses, discloses, deletes or protects users' personal information. Additionally, the developer must notify affected users about the disclosure of their personal information and instruct any third-party that received users' health information to destroy that data.[1]

In addition, FTC also enforces federal laws relating to consumers' privacy and security.[2] Specifically, the FTC's Health Breach Notification Rule requires a provider of a personal health record (PHR) or PHR-related entity to notify affected consumers, the FTC and, in some cases, the media following a breach of unsecured personal health information. Service providers and PHR-related entities must also notify these PHR providers in the event of a breach. FTC defines PHR as an electronic record of identifiable health information on an individual drawn from multiple sources that is managed, shared and controlled by or primarily for the individual.[3] A business is a PHR vendor if it offers or maintains a PHR. An example of a PHR vendor is a business with an online service allowing consumers to store or organize medical information from many sources in one online location.[4]

A PHR vendor that is not a HIPAA Covered Entity is not required to be HIPAA-compliant. Thus, PHR vendors are not subject to the HIPAA Breach Notification Rule but are governed by the FTC Health Breach Notification

©2005-2026 K&L Gates LLP. All Rights Reserved.

Rule.[5] FTC recognizes scenarios in which an entity is a HIPAA Business Associate and subsequently offers PHR services to the public. Such an entity would be subject to both the HIPAA and FTC Breach Notification Rules. The fact pattern is limited, and it does not address a situation where the customers of the PHR vendor and the Covered Entity are the same group of people. However, in the event a PHR vendor has a direct relationship with all the individuals affected by a HIPAA breach, one entity could contract with the other to provide one notification to affected individuals.[6]

TELEMEDICINE LAWS

The delivery of healthcare services in the US through telemedicine or telehealth is generally governed by State medical boards on a State-by-State basis. Licensure requirements can vary based on where the patient or the healthcare provider is located. Prior to the Covid-19 pandemic, most States, plus the District of Columbia, Puerto Rico and the Virgin Islands, required that physicians engaging in telemedicine must be licensed in the State in which the patient is located. In relation to the Covid-19 Public Health Emergency, twelve State boards issued a special purpose license, telemedicine license or certificate, or license to practice medicine across State lines in relation to the practice of telemedicine and six States required physicians to register, as opposed to obtain a license, if they wanted to practice across State lines.[7]

Many of these requirements were modified during the pandemic to rapidly scale vast telehealth platforms to provide remote care during periods of quarantine and in response to other pandemic-related exigencies. As a result, more States are allowing physicians providing healthcare services to residents of the State to be licensed in neighboring or other States. Some have taken the approach of providing expedited licensure, or foregoing licensure for a temporary, special needs permit. What is unclear, however, is how these States will pivot after the Public Health Emergency no longer is in effect, and if Federal regulators might consider a Federal approach to avoid the patchwork of State laws and licensure regulations from impacting how telemedicine and telehealth services are implemented and scaled.

In addition to State licensure laws, there are also State-based consent, medical record, pharmacy, physician ordering and privacy considerations related to telemedicine services. Moreover, reimbursement for telehealth services for Federal healthcare program beneficiaries, such as Medicare, is governed by the Centers for Medicare and Medicaid Services, which have historically reimbursed only for limited visits in remote settings where one or both of the parties was physically located at an acute care facility. Commercial payors, such as private and employer-sponsored health plans, govern reimbursement for private pay patients, and each has their own set of requirements and reimbursement schedules.

Accordingly, any company seeking to develop or expand its telemedicine presence in the United States will need to conduct a State-by-State analysis of specific regulatory requirements and will require reimbursement expertise at the Federal level and an understanding of how commercial payor contracts impact reimbursement for private pay patients. Most importantly, such a company may need a crystal ball, as it is difficult to know how State and Federal regulators will approach these issues after the Covid-19 Public Health Emergency no longer is in effect.

©2005-2026 K&L Gates LLP. All Rights Reserved.

FRAUD AND ABUSE LAWS

Federal and State anti-kickback statutes (e.g., the federal Anti-Kickback Statute[8]) regulate business relationships in the healthcare, pharmaceutical and medical device sectors, prohibiting individuals or entities from asking for or receiving any remuneration in exchange for referrals of healthcare program business. Federal and State physician self-referral laws (e.g., the Stark Law[9]) generally prohibit healthcare providers from referring designated health services (DHS) to entities with which individuals or entities have a direct or indirect financial relationship, unless an exception applies.

The False Claims Act[10] imposes criminal penalties on any person or organization that knowingly makes a false record or files a false claim regarding any Federal healthcare program, whether directly or indirectly. Additionally, the Social Security Act at the Federal level imposes CMPs or excludes from the Medicare and Medicaid programs those physicians and other healthcare providers who commit various forms of fraud and abuse involving Medicare and Medicaid.

Under these Federal and State laws, certain practices that incentivize utilization and profitability and otherwise pay for referrals are impermissible and could subject knowing actors to civil or criminal sanctions. Accordingly, the types of business arrangements and negotiations that are commonplace in other industries may be unlawful within the healthcare industry, where goods or services are reimbursed by the Federal government or third-party payors. To the extent companies aspire to provide goods or services to healthcare providers or directly to patients, where healthcare is reimbursed by Federal healthcare programs and commercial payors, such companies and their contracts and business arrangements will need a full understanding of applicable healthcare fraud and abuse guardrails prior to doing business.

CONCLUSION

Digital Health in the United States, like traditional healthcare, is governed by various regulations that are complicated and continuously changing, especially during and after the Covid-19 Public Health Emergency. Non-US-based companies need to understand how to navigate these complex regulations at every stage of their business development, and legal representation that is nuanced and skilled at understanding the practical application of these regulations is critical to achieving success in the US marketplace.

Should you have any questions about anything in this series, please reach out to the authors.

FOOTNOTES

[1] https://www.ftc.gov/news-events/press-releases/2021/01/developer-popular-womens-fertility-tracking-app-settles-ftc.

[2] https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement.

[3] See https://www.ftc.gov/tips-advice/business-center/guidance/complying-ftcs-health-breach-notification-rule.

[4] Id.

[5] Id.

©2005-2026 K&L Gates LLP. All Rights Reserved.

[6] Id.

[7] https://www.fsmb.org/siteassets/advocacy/key-issues/telemedicine_policies_by_state.pdf

[8] 42 U.S.C. § 1320a-7b.

[9] 42 U.S.C. § 1395nn.

[10] 31 U.S.C. §§ 3729-3733.

* This article was first published by *In-House Community*.

KEY CONTACTS



AIKO YAMADA
COUNSEL

TOKYO
+81.3.6205.3630
AIKO.YAMADA@KLGATES.COM

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author(s) and not necessarily those of the law firm's clients.

©2005-2026 K&L Gates LLP. All Rights Reserved.