WEBINAR

TOP TAKEAWAYS

Protecting the Telehealth Consumer: FTC and State-Based Considerations

As the COVID-19 pandemic in the United States eases, telemedicine faces an important crossroads. While telehealth services have demonstrated their value as an integral part of care delivery, federal and state waivers instituted during the crisis are likely to expire soon. As lawmakers and agency officials consider updated or expanded digital health rules, regulators are expected to intensify their scrutiny of providers. In this webinar, McDermott lawyers Brian Boyle and Jiayan Chen explored an important issue for post-COVID-19 healthcare: consumer protections for telehealth consumers.

1. The Federal Trade Commission (FTC) routinely challenges data privacy and security practices as unfair or deceptive acts or practices. Key FTC expectations for digital health providers include minimizing data, limiting access and permissions, implementing authentication and strong password protections, ensuring that third-party providers follow good data security practices, implementing "security by design," taking advantage of data privacy and security resources from NIST and other sources, communicating effectively and transparently with consumers, and complying with all relevant laws.

2. The FTC's Health Breach Notification Rule may apply to web-based businesses that collect consumer health data (such as health tracking services and apps) and are not governed by HIPAA. Under the Health Breach Notification Rule, a company that experiences a breach of unsecured personal health information may be required to notify the FTC, consumers, and others within specified time periods. In addition to FTC rules, companies should pay close attention to state privacy laws, which are expanding and proliferating.

3. Advertising claims (including social media endorsements) related to health and safety face intense regulatory scrutiny and require a high level of substantiation. Health and safety claims must be based on competent and reliable scientific evidence, not anecdotal evidence from patients. Claims cannot be false or misleading (for example, by omitting appropriate context or by suggesting that non-clinical data has clinical significance).

4

Many health stakeholders are exploring innovative digital ways to engage with their patients and should therefore familiarize themselves with the various federal and state laws that may apply to these communications. For example, the Telephone Consumer Protection Act governs telephone and text message communications, and imposes specific consent requirements, among other provisions. The Controlling the Assault of Non-Solicited Pornography and Marketing Act establishes requirements for commercial emails, including header and subject line rules and recipient opt-out rights. For recorded voice calls, the federal wiretap standard and wiretap laws in many states require the consent of at least one party to the call. Several states require the consent of all parties to the call.

5

Healthcare organizations contracting with consumers should give careful consideration to how they bind users to terms of service and privacy policies. A browse-wrap mechanism secures only passive consent, and most courts consider this an insufficient means of binding a user to the terms. In contrast, a click-wrap mechanism provides a manifestation of a user's assent (by clicking a checkbox, for example). Organizations should also consider whether to incorporate their privacy policy into the terms of service (*i.e.*, making it part of the user contract) or keep it separate (as a compliance document only).

VISIT **MWE.COM/HEALTH**

McDermott Will & Emery