NELSON HARDIMAN
HEALTHCARE LAWYERS

Priority Litigation Update: GoodRx and the FTC's Emergence in Protecting Health Privacy

Priority Litigation Update:

GoodRx and the FTC's Emergence in Protecting Health Privacy

On February 1st, 2023, the Federal Trade Commission (FTC) announced a groundbreaking action against GoodRx, a California-based telehealth company that provides prescription drug resources and telehealth services. The FTC filed a comp alleging that GoodRx had unlawfully shared sensitive health data about its customers with advertisers like Google and Faceb and failed to notify them afterwards. Additionally, on the same day, the FTC announced that it had reached a $1.5 million-doll settlement with GoodRx, subject to the approval of the trial court.

The complaint and settlement deserve attention for several reasons. Firstly, it marked the first time that the Health Breach Notification Rule (HBNR) was used by the Federal Trade Commission for an enforcement action. The HBNR was established 2009 to compel consumer notification in the event of a data breach. The regulation was based on a narrower rule that was on applicable to healthcare providers and special contractors subject to Health Insurance Portability and Accountability Act (HIPA In contrast to HIPAA's breach notification requirement (adopted contemporaneously), the FTC's HBNR applied to a broader category of "vendors of personal health records." This much less restrictive classification enveloped many types of consumer-focused businesses entities outside of the provision of healthcare services that received and used personal health for commercial gain. This included companies such as Ancestry.com, which collects and stores genetic information for its customers, as well as a spate of health and wellness apps and wearable devices that track cardio health, glucose levels, fertil cycles, and other sensitive medical information.

In the past, the domain of enforcement for breach notification was primarily the responsibility of the Department of Health and Human Services Office for Civil Rights (OCR), which is tasked with monitoring HIPAA compliance for covered entities such as healthcare providers and health insurance plans. For instance, when a Chinese hacker stole the personal health information o million Anthem customers in 2018, the OCR reached a $16 million-dollar settlement with Anthem for failing to notify the affect customers of the breach. The GoodRx case, however, signals the rise of FTC enforcement as an independent federal force fo health privacy. This rising role for the FTC can be seen as an outgrowth of the evolving landscape of digital technologies, onli storage, and the overall growth of the online health and wellness sector. Consumers are now routinely sharing personal medi information with exercise and fitness companies, chatbot therapists, and telemedical referral companies that fall outside the s of HIPAA because they are provided voluntarily by consumers to organizations outside the traditional scope of clinical provide HMOs, and health insurers.

In its agreement with GoodRx, the FTC imposed a $1.5 million fine and prohibited the company from sharing user health data third parties for advertising purposes. It also mandated the implementation of privacy programs and better controls to ensure consent with regards to the sharing of sensitive data in the future. Although GoodRx did not admit any wrongdoing, it agreed t distribute a Notice to Covered Users acknowledging that, between July 2017 and April 2020, it shared identifiable information related to users, including health information, without their permission.

The settlement with GoodRx was not without internal agency controversy. FTC Commissioner Christine W. Wilson expressed view that the civil penalty was rather paltry. Wilson noted that the company had an $18 billion valuation when it went public in 2020, and that it "profited significantly from its silence about its scurrilous privacy practices – far in excess of the $1.5 million penalty the Commission levied." While Wilson raises legitimate concerns, the FTC had several incentives to avoid a trial and c for a quick resolution. Trials always come at a cost of time and money, with no guarantee of a better outcome. Unlike an open hacking breach, companies like Google and Facebook keep a tight lid on what they know about consumers, making it difficult assess the extent of harm. Moreover, the FTC has larger concerns related to the proliferation of pixels and other embedded tracking technologies that have become the norm on websites and mobile platforms. In fact, in GoodRx's media release of the settlement, the company complained that it was singled out for a ubiquitous practice: "The FTC complaint revolved around ou inclusion of a Facebook Javascript tracking pixel, which is widely used by many consumer, healthcare and government websi […] insurance companies, hospitals, and others." A recent investigation by TheMarkup and STAT found that 33 of the top 100 American hospitals had an embedded "Meta Pixel" tracker on their public facing websites. These trackers were actively sendi

data packets to Facebook whenever patients logged in to schedule an appointment.

At the same time, the challenge of Americans providing their health data across websites and smartphone apps (as well as be geolocatable by the same devices, allowing for analysis of their real-world healthcare choices) has taken on new significance the reversal of *Roe v. Wade*. A landmark Supreme Court decision finding that the zone of health privacy was narrower than m Americans assumed, coupled with activist states declaring an interest in utilizing health data to enforce laws restricting abortio added fuel to the fire – making protection of health privacy an urgent FTC priority. The FTC's action against GoodRx can be s as part of a broader effort to take a proactive role to preserve medical privacy in light of growing concerns that location trackin data can be used against women seeking abortion or individuals who aid or assist them. Last August, for example, the FCC fi lawsuit against the data broker Kochava, for "selling geolocation data from hundreds of millions of mobile devices that can be [to] reveal people's visits to *reproductive health clinics*, places of worship, homeless and domestic violence shelters, and addi recovery facilities." Currently, Kochava is aggressively litigating the action. But other FCC enforcement activities relating to he privacy enforcement have ended in settlements. In June 2021, for example, the FCC secured a settlement against Flo Health period tracking app, regarding allegations that the company had shared the health information of its users with third-party data analytics providers, despite promising to keep such information confidential.

The clear takeaway for now is that the FTC is prioritizing cybersecurity and health data privacy regarding sensitive medical information. While preserving patient confidentiality may not be new for healthcare providers subject to HIPAA, many of those same organizations need to evaluate a broader set of practices related to their marketing and social media. In addition, health privacy is new ground for consumer brands that are not healthcare organizations, but receive and use health data as part of th business. In the coming months and years, a broader range of organizations collecting health data will need to reckon with the FTC as a health privacy enforcement agency. The FCC's example is being emulated at the state level as well. California, for instance, also mandates data security breach reporting. As the general public becomes increasingly aware of how they can be compromised by companies unscrupulously sharing their medical data, it's not difficult to imagine state attorneys general and regulatory agencies targeting consumer and technology companies for their practices related to health privacy. It's time to reevaluate risks related to health privacy across a far greater range of businesses than are currently addressing the issues.

Authored By:

Harry Nelson, Managing Partner, Nelson Hardiman

Yehuda Hausman, Law Clerk, Nelson Hardiman

Nelson Hardiman LLP

Healthcare Law for Tomorrow

Nelson Hardiman regularly advises clients on new healthcare law and compliance. We offer legal services to businesses at ev point in the commercial stream of medicine, healthcare, and the life sciences. For more information, please contact us.