wiley

NEWSLETTER

Safeguarding Health Information in the Apps Ecosystem: A Reminder from the California AG

November 2020

Privacy in Focus®

California Attorney General Xavier Becerra charged Glow, Inc. (Glow), a fertility health app, with privacy and basic security failures that allegedly put women's "deeply-sensitive" personal and medical information at risk. The AG and Glow agreed to settle the charges.

In the settlement, which remains subject to court approval, app developers for Glow agreed to pay a $250,000 civil penalty. The settlement also imposes injunctive terms that require Glow to comply with state consumer protection and privacy laws, and a novel injunctive term that requires Glow to consider how privacy or security lapses may uniquely impact women. This settlement signals to "every app maker that handles sensitive private data" the significant legal and regulatory risk that arises from its collection and storage.

Settlement Background

Although health care and other wellness apps have existed for many years, these apps have seen increasingly widespread adoption, particularly during the COVID-19 pandemic. Consumers frequently use health apps in lieu of or in conjunction with other in-person interactions with their doctors, fitness professionals, and employers, and this collection and transmission of personal data presents unique privacy and data security risks. While sensitive data in medical records held by a doctor's office – or other health care providers and affiliates – are protected under the federal Health Information Portability and Accountability Act (HIPAA), highly sensitive information shared by consumers in mobile apps to manage their health without the involvement of a health care provider may be subject to various

Authors

Antonio J. Reynolds
Partner
202.719.4603
areynolds@wiley.law

Tawanna D. Lee
Consulting Counsel
202.719.4574
tdlee@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

state privacy laws, even if not subject to HIPAA. (Wiley's data protection team has a handy primer on the scope and applicability of HIPAA.)

Mobile application developer Glow markets an ovulation and fertility tracker that recently caught the attention of the California AG because of its alleged failure to protect sensitive personal information. Glow collects and stores highly sensitive personal and medical information related to a user's menstruation, sexual activity, and fertility. According to the complaint, the Glow app is designed to track personal and medical information, including medications, fertility test results, past and upcoming medical appointments, ovulation-cycle calculations and complete medical records. Users can track intimate details of their sexual experiences, efforts to become pregnant, and pregnancy histories, including miscarriages, abortions, and stillbirths. The app also allows users to import and export medical records.

The complaint alleges that between 2013 and 2016, Glow "had serious basic security failures that put its users' data at risk." First, the app offered a "Partner Connect" feature, which allowed two users to link to each other and share information. According to the complaint, the app automatically granted the linking requests without authorization from the user whose information was shared. Second, the Glow app's password change function could have allowed third parties to reset user account passwords and access information in those accounts without user consent. The health app's Privacy Policy and Terms of Use made representations about how Glow maintains user privacy and personal data. According to the AG's complaint, Glow's representations that it "use[s] industry standard security measures to protect [user] information so that it is not made available to unauthorized parties" were undercut by Glow's security flaws.

Injunction Requirements

In addition to the civil penalty levied, the AG's order requires Glow to institute a series of injunctive terms to resolve failings in its privacy and data security practices. The settlement outlines specific safeguards and controls to which Glow must adhere, including:

- Implementing, maintaining, regularly reviewing and revising, and complying with a documented information security program designed to protect the security, integrity, availability, and confidentiality of users' information;
- Designating one or more individuals to manage Glow's compliance with applicable state and federal privacy laws, and ensure those individuals have the authority and autonomy to perform their responsibilities and to report "any significant privacy or security concerns" to the CEO or other executives;
- Obtaining affirmative authorization from consumers before sharing personal information with any third party other than service providers unless required by law, or using personal information for any materially different purpose, and giving consumers the right to revoke;
- Developing, implementing, and maintaining a process to incorporate privacy-by-design principles and security-by-design principles when creating new applications or online services, and specifically considering how privacy or security lapses may affect women;

- Providing employee training concerning awareness and prevention of online threats affecting women, including cyberstalking and online harassment, as well as privacy issues related to reproduction and reproductive rights; and
- Completing an annual privacy risk assessment that addresses Glow's efforts to comply with applicable privacy laws, and considers online risks that women face as a result of privacy or security lapses while using Glow's mobile apps or online services – and delivering a copy of the report of that assessment to the AG's office.

The Glow settlement highlights increased scrutiny of consumer-directed health app developers' privacy and data security practices and the regulatory tools available to ensure that highly sensitive data are being safeguarded. Notably, the AG's "first-ever" injunctive term focused on the unique impacts that online privacy and security lapses can have on women. This novel injunctive term demonstrates the AG's willingness to target its privacy and data security efforts to protect particular groups from the disparate harms that may arise from app developers' failure to protect user privacy. Companies that collect and manage sensitive personal information should pay close attention to developments in this area.