HINSHAW

Alerts

Lesson Learned From Recent FTC Settlement: Be Cautious With Compliance "Seals"

February 19, 2021
Hinshaw Privacy & Cyber Bytes

"HIPAA Compliance" seals are not a reliable indicator that a company's website employs reasonable measure to secure personal medical information. That is one lesson from a recently finalized settlement between the Federal Trade Commission (FTC) and SkyMed International, Inc., a Nevada-based travel emergency service provider.

In its 2020 complaint, the FTC alleged that SkyMed failed to take reasonable measures to secure the personal information it collected from consumers who had signed up for its emergency travel membership plan. Consumers were required to provide personal health information, including a list of prescribed medications, medical conditions, and hospitalizations within the past six months. SkyMed's terms and conditions warned consumers that "failure to provide accurate information may be a felony in your area."

The FTC alleged that, as a result of SkyMed's failure to take reasonable measures to secure this personal information, the company left a cloud database containing 130,000 membership records unsecured. The unsecured database was exposed by a security researcher and could be located and accessed by anyone. The database stored, in plain text, customers' personal information including names, birthdates, home addresses, health information, and membership account numbers. The FTC also alleged that SkyMed failed to: (1) assess risks to such data by performing penetration testing and other measures, and (2) monitor its network for unauthorized access.

According to the complaint, SkyMed deceived consumers by displaying a "HIPAA Compliance" seal on every page of its website, giving the false impression that its privacy policies had been reviewed by an unspecified authority and met the security and privacy requirements of the Health Insurance Portability and Accountability Act (HIPAA). The FTC alleged that no government agency or other third party had reviewed SkyMed's information practices for HIPAA compliance.

The settlement prohibits SkyMed from misrepresenting how it secures personal data, the circumstances of and response to a data breach, and whether the company has been endorsed by or participates in any government-sponsored privacy or security program. It also requires SkyMed to send a notice to affected consumers detailing the information exposed by the data breach. The company must implement a comprehensive information security program and obtain biennial assessments of it by a third party. Additionally, a senior corporate

Service Areas

Privacy, Security & Artificial Intelligence

manager for SkyMed must provide the FTC with annual certifications that the company has established, implemented, and maintained this comprehensive information security program, and that any instances of non-compliance or data breaches have been reported.