bodman

A Health Care Law Update

Bodman PLC **August 28, 2023**

Legal Restrictions on Health Information – Beyond HIPAA

By: Brandon M. Dalziel, Member, Health Care Practice Group

Appropriately so, providers look first to the Health Insurance Portability and Accountability Act of 1996, as amended (HIPAA), to ensure that they comply with regulations regarding patients' protected health information (PHI). Nonetheless, one must also look beyond. HIPAA is a federal statute, which preempts state law that is contrary to HIPAA. However, state law that is more stringent than the HIPAA privacy standard is not preempted, and there are other federal regulations to be considered.

HIPAA applies to 'covered entities' and their 'business associates.' Covered entities are generally health plans, health care clearinghouses, and health care providers who electronically transmit any health information in connection with transactions for which the Department of Health and Human Services has adopted standards.

Health apps, such as fitness trackers, and other similar technologies which are directed toward individuals and not healthcare providers or other covered entities, may be outside of HIPAA. However, those technologies may fall within the Federal Trade Commission's (FTC) rules with respect to personal health records. The lesser-known FTC Health Breach Notification Rule has been around since 2009. In 2021, the FTC issued a policy statement confirming that health apps and connected devices that collect or use consumers' health information must comply with the FTC Health Breach Notification Rule.

This year, the FTC brought forth its first two enforcement actions for failure to follow the Health Breach Notification Rule, resulting in civil penalties of $100,000 and $1,500,000.

The FTC has recently proposed updates to the Health Breach Notification Rule. The proposed updates include: (a) revising several definitions to clarify the rule's application to health apps and similar technologies not covered by HIPAA; (b) requiring health apps to obtain authorization from consumers to share their information with third parties; and (c) clarifying that a "breach of security" under the rule includes an unauthorized acquisition of identifiable health information that occurs as a result of a data security breach or an unauthorized disclosure. The comment period to the proposed updates ended this month. Thus, there is likely a final rule, with updates, forthcoming in the not-too-distant future.

HIPAA is the foundation of federal regulations that protect health information. However, there are other federal regulations to be considered as well, including the FTC Health Breach Notification Rule. Additionally, state laws can also be applicable. When dealing with health information, one must consider the full regulatory landscape to ensure compliance.

Bodman PLC can provide guidance on this matter and others and provide practical advice to meet your needs. To discuss this or any other legal issue affecting your organization, please contact your Bodman attorney or Brandon Dalziel at (313) 393-7507 or bdalziel@bodmanlaw.com. Bodman cannot respond to your questions or receive information from you without first clearing potential conflicts with other clients. Thank you for your patience and understanding.