The FTC's Action Against LabMD: Why Physicians Should Care

LinkedIn Post 8/16/16
Donna Vanderpool, MBA JD
Vice President of Risk Management, PRMS

The Federal Trade Commission (FTC) has asserted jurisdiction and, after some back and forth, found liability on the part of a laboratory for failure to protect data on its computer networks, resulting in breach of patient confidentiality. The lab's data security practices were found to be unfair, in violation of the Federal Trade Commission Act. Here's how the case unfolded:

August 2013: The FTC filed a complaint against LabMD based on two incidents where the lab allegedly failed to protect the security of personal information. In the first incident, a third party was able to access information on approximately 9,300 patients, including names, dates of birth, Social Security numbers, procedure codes, etc. This alleged breach was through a file-sharing application. The second breach involved personal information, including Social Security numbers, found in the possession of individuals who subsequently pleaded "no contest" to identity theft charges. LabMD moved to dismiss the complaint arguing that the FTC cannot enforce HIPAA's Security Rule. That argument was rejected by the FTC and the case continued, with the FTC arguing that among other things, the company failed to:

- Have a comprehensive security program to protect consumers' personal information
- Use readily available measures to identify commonly known or reasonably foreseeable security risks and vulnerabilities on its computer networks
- Use adequate measures to prevent employees from accessing personal information not needed to perform their jobs
- Adequately train employees to safeguard personal information
- Require employees or other users with remote access to the networks to use common authentication-related security measures
- Maintain and update operating systems of computers and other devices on its networks
- Employ readily available measures to prevent or detect unauthorized access to person information on its computer networks

November 2015: An Administrative Law Judge (ALJ) within the FTC ruled that LabMD's alleged failure to institute reasonable data security measures was not likely to cause substantial injury to consumers. The FTC disagreed with the ruling.

July 2016: After another hearing, the FTC Commissioners disagreed with the ALJ and determined that a showing of tangible injury was not necessary for a company's acts and practices to be unfair, in violation of the FTC Act. The Commissioners specifically noted that the company failed to provide reasonable and appropriate security for stored information and corrections could have been made at relatively low cost.

So breaches involving patient information can result in an investigation by the FTC (for all entities) as well as by OCR (for covered entities under HIPAA).

PRMS
Manager of The Psychiatrists' Program
Medical Professional Liability Insurance for Psychiatrists
1-800-245-3333
Email: TheProgram@prms.com
Visit: PsychProgram.com
Twitter: @PsychProgram