PUBLICATION

A New Sheriff in Town: Federal Trade Commission Enforcement of Medical Information Security [Ober|Kaler]

2014: Issue 19 - Focus on HIPAA/Privacy

A recent court decision found that the Federal Trade Commission (FTC) has authority to enforce the requirements for security of Protected Health Information, or PHI, as defined under the Health Information Portability and Accountability Act (HIPAA), against a defense asserted that the FTC has no authority under that statute. *LabMD, Inc. v. Federal Trade Commission*, 2014-1 Trade Cas. (CCH) ¶ 78,766 (N.D. Ga. May 12, 2014) and *LabMD*, 2014 Trade Cas. (CCH) ¶ 78,785 (F.T.C. May 19, 2014). This is, of course, just one controversy, and one that is being played out in a series of related administrative and judicial actions. However, when that opinion is read against the background of prior FTC enforcement actions and current concern about the security of personal information, it represents a development worth noting.

The procedural history of the case is complex and likely only of interest to lawyers. What is significant is the following:

1. The FTC, in areas in which it does not have specific regulations, regulates by enforcement action under Section 5 of the FTC Act, based on “unfair . . .acts or practices.” 15 U.S.C. § 4 (a). The FTC does not always publish detailed guidance as to its standards and requirements.

2. In general, in the area of data security, the FTC has not been challenged in court and actions have been settled by consent decree. This is the kind of guidance that, even in the absence of regulations, judicial opinions can provide.

For example, in a matter involving transcription services, the FTC complaint stated that the transcription service company failed to implement reasonable and appropriate security measures or to ensure its service providers also implemented reasonable and appropriate security measures. *GMR Transcription Services., Inc*., Matter No. 112-3120 (F.T.C. Dec. 16, 2013) (proposed consent order), At least 15,000 files containing sensitive personal information – including consumers' names, birthdates, and medical histories – were alleged to have been available to anyone on the Internet. The FTC's proposed order resolving the case prohibits GMR from making misrepresentations about privacy and security, and requires the company to implement a comprehensive information security program and undergo independent audits for the next 20 years.

The *LabMD* case has a long procedural history, which is not finished yet. While the case has gone forward on procedural grounds, in essence LabMD, a Covered Entity under HIPAA, challenged an FTC complaint concerning its data security practices for PHI. The FTC administrative complaint alleged that LabMD, through a commercially available peer-to-peer file application, had disclosed the personal information of approximately 9600 people to any other user of that peer-to-peer system. The administrative complaint also stated that the police department in the area had arrested alleged identity thieves and found LabMD documents containing sensitive personal information in the alleged thieves' possession.

LabMD filed an action in the United States District Court for the Northern District of Georgia, seeking to dismiss the FTC's administrative complaint. The federal District Court declined to do so. Among other things, the court stated that LabMd “claims that PHI is regulated by HIPPA and the Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009, which discredits that the FTC has the authority to regulate data

security under Section 5. LabMD further alleges that the FTC has not published any requirements for the protection of patient information, and thus LabMD is not on notice of what protections the FTC now claims were required." *LabMD, Inc. vs. F.T.C.*, 2014-1 Trade Cas. (CCH) ¶ 78,766 slip op. (N.D. Ga. 2014),. This, however, was not enough to dismiss the matter.

In fact, in a footnote, the court also stated that, "[t]he Court believes that the likelihood of a favorable jurisdictional or merits outcome for LabMD is slight, but that belief cannot govern the legal issues addressed in this Order. As the court noted at the May 7, 2014 hearing, the authority of the FTC to enlarge its regulatory activity in the data security area presents an interesting and likely important jurisdictional issue that needs to be resolved promptly."

While this article is just an overview of a complex case that is ongoing, the FTC may emerge as an important enforcer of the security of PHI, without the requirement of regulations to guide the health care community. Certainly, at the very least, statements by health care providers to patients that assure them that their personal medical information is secure (e.g., "We are 100 percent HIPAA compliant" or "Privacy and security of your medical records is our highest priority"), if followed by a data breach, may attract FTC enforcement actions as falling within an allegation of an unfair action or practice, i.e., misleading consumers, one of the core areas of FTC jurisdiction.