Federal Trade Commission

Cybersecurity & the Healthcare Industry:
The FTC's Tools for Tackling New Threats

Thomas Pahl
Acting Director, Bureau of Consumer Protection, FTC

University of Maryland Medical Systems
Board Cybersecurity Retreat
March 29, 2017

Good morning. I'm delighted to be here to kick off today's event by discussing the FTC's work on data security and health information. I need to make two disclaimers. First, the views I express here are my own and do not necessarily represent the views of the Federal Trade Commission or any individual Commissioner. Second, although not a Luddite, I definitely am not a techie. My teenage son was recently looking over my shoulder watching me start to go online and asked in an appalled voice, "Are you really using Google to get to Yahoo?" I responded, "Of course not. I am using Google to get to Yahoo to get to AOL." My expertise clearly lies in law, not technology.

Consumers are increasingly taking a more active role in managing their health data. They have available to them an increasing number of new health-related apps, devices,and services. There are apps that allow consumers to track their diet and exercise habits, devices that help

them track their glucose levels, and websites where people with the same medical condition may share information. In addition, consumers may download their medical information into personal health records and use this information to make decisions about their health. Some of these products are doctor-recommended, such as diet and exercise apps that generate and send reports back to physicians. Others products consumers find and use outside of the traditional healthcare context. Many of these products increase consumer engagement in their health and fitness, reduce healthcare costs, and improve outcomes. Yet these products may raise privacy and security concerns too. Most consumers regard their health data as highly sensitive and private. Data breaches and unauthorized disclosures of such information can cause or be likely to cause substantial harm to consumers, including subjecting them to fraud and medical identify theft.

In my remarks today, I would like to do three things. First, for those of you who are not familiar with the Federal Trade Commission, I will begin with a quick FTC 101. Second, I'll outline some security risks affecting hospitals, health apps, and other companies in the health care field. Third, I'll describe what health care companies can do to address these risks and mitigate harms to themselves and their patients.

I. FTC 101

First, what is the FTC? The Federal Trade Commission is a small, independent agency with a large role to play when it comes to data security and health information. The FTC has broad jurisdiction to protect consumers. We issue some regulations, but we are primarily a civil law enforcement agency.

We enforce a number of laws applicable to data security that cover a wide array of entities. Our primary authority is the FTC Act, which prohibits unfair and deceptive acts and

practices.[1] As applied to the data security area, the FTC Act requires that companies refrain from making deceptive security claims. A failure to have taken reasonable security measures also can constitute an unfair practice under the FTC Act.

The FTC recognizes there is no such thing as perfect security. Just because a company experiences a breach does not mean its data security practices were unreasonable. What is reasonable will depend on a number of factors, including the size and complexity of a company's operations, the amount and sensitivity of data it collects, and the availability of low-cost tools to mitigate threats.

In addition, the Commission also enforces a number of sector-specific statutes that include data security requirements, such as the Children's Online Privacy Protection Act, the Fair Credit Reporting Act, and the Gramm-Leach-Bliley Act, known as GLBA. We also enforce the GLBA Safeguards Rule, which imposes data security requirements on non-bank financial institutions.[2] Like the FTC Act, each of these laws require companies to practice reasonable security. In the ancient world, it was said, "all roads lead to Rome." In the data security world, all roads lead to reasonableness.

In addition to enforcing laws, we develop and distribute consumer and business education materials, issue reports, testify before Congress, and host workshops on various business and technological developments, including those relating to data security and privacy. These policy and outreach efforts raise consumer awareness and help prevent consumer harm, which makes them integral to our consumer protection mission.

Now, why should a medical audience care about the FTC? Two reasons. The first reason is that the FTC Act is broad and extends to traditional healthcare businesses even if the Health

[1] 15 U.S.C. § 45(a).
[2] 15 U.S.C. §§ 6801-6809 (GLBA); 15 U.S.C. § 1681 (FCRA); 15 U.S.C. §§ 6501-6506 (COPPA) and 16 C.F.R. Part 312 (COPPA Rule).

Insurance Portability and Accountability Act, or HIPAA, also applies to them. The FTC Act, for example, applies to health care providers, health plans, health care clearinghouses, and their business associates. Note, however, that the FTC Act generally does not reach nonprofit entities or state-regulated insurance practices.[3] Moreover, the Department of Health and Human Services and the FTC have worked together closely because of our common interest in ensuring the privacy and security of health information, regardless of the applicability of our respective legal authority.[4]

The second reason that a medical audience should care about the FTC is that physicians and other HIPAA-covered businesses may recommend that consumers use health apps, devices, and other products that non-HIPAA covered entities have developed. The entities creating these new products often are within the FTC's jurisdiction. Indeed, the FTC Act is currently the primary federal statute applicable to the privacy and security practices of non-HIPAA covered businesses that collect individually identifiable health information.

II. Data Security Risks

Let me now outline some data security risks that currently affect hospitals, health apps, and other health care companies. The first is the risk of a data breach. One recent report has suggested that in 2016, there was on average one health care sector breach per day, resulting in the breach of 27 million patient records.[5] These types of breaches can result in unauthorized access to and misuse of personal information. The business of buying and selling personal information can be a lucrative one. Indeed, one study showed that hackers could sell health

[3] 15 U.S.C. §§ 44 & 45(a).
[4] For example, FTC staff collaborated with OCR to bring a set of cases involving faulty data security practices that implicated both HIPAA and the FTC Act. *See Rite Aid Corporation*, No. C-4308 (F.T.C. Nov. 12, 2010) (decision and order), *available at:* https://www.ftc.gov/enforcement/cases-proceedings/072-3121/rite-aid-corporation-matter; *see also CVS Caremark Corporation*, No. C-4259 (F.T.C. June 18, 2009) (decision and order), *available at:* https://www.ftc.gov/enforcement/cases-proceedings/072-3119/cvs-caremark-corporation-matter.
[5] http://www.healthcare-informatics.com/news-item/cybersecurity/healthcare-data-breaches-year-review.

insurance credentials on the black market for $20. And hackers could sell a complete medical record for $1200 or more.[6]

Second, the threat of ransomware continues to plague the health care industry. In the fall, the FTC hosted a workshop examining the threat of ransomware.[7] Ransomware is software that a malicious actor uses to hold data hostage to extort payment. The FTC's workshop highlighted a string of high profile ransomware attacks on health care organizations. For example, the 2016 attack on Hollywood Presbyterian Medical Center in Southern California took out the hospital's entire network for more than a week, leaving staff without access to email and some patient data. The malware crippled the hospital's emergency room systems and other computer systems necessary for patient care. It forced hospital staff to log medical records with pen and paper. In response, the hospital paid a ransom of 40 Bitcoins, or $17,000, to restore its operations.[8] Another ransomware attack crippled MedStar Health's computer systems, disabling access to email and patient records at ten hospitals in the Washington, D.C. region for nearly two weeks. Given these kinds of high profile attacks, it is not surprising that ransomware is a cyber threat that greatly worries many health care professionals.[9]

A third risk involves Internet of Things botnets. The IoT is the phenomenon where everyday objects connect to the Internet to send and receive data. It, for example, includes bracelets that allow a consumer to share with friends how far he has biked or run during the day.

---

[6] *See* Dell SecureWorks, *Hackers Sell Health Insurance Credentials, Bank Accounts, SSNs and Counterfeit Documents*, *available at* https://www.secureworks.com/blog/general-hackers-sell-health-insurance-credentials-bank-accounts-ssns-and-counterfeit-documents.

[7] *Fall Technology Series: Ransomware* (Sept. 7, 2016), *available at* https://www.ftc.gov/news-events/events-calendar/2016/09/fall-technology-series-ransomware.

[8] *Hollywood Hospital Pays $17,000 in Bitcoin to Hackers; FBI Investigating*, LOS ANGELES TIMES (Feb. 18, 2016) *available at* http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html.

[9] Ponemon Institute, *Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data* (May 2016), *available at* http://www.ponemon.org/blog/sixth-annual-benchmark-study-on-privacy-security-of-healthcare-data. [10] Krebs on Security, *DDoS on Dyn Impacts Twitter, Spotify, Reddit*, Oct. 21, 2016, *at* https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify-reddit/.

The IoT also includes insulin pumps and blood-pressure cuffs that connect to a mobile app to enable consumers to record, track, and monitor their vital signs without having to go to a doctor's office. The IoT holds great promise for consumers who are concerned about their health.

Yet the lack of adequate security relating to the IoT can cause or be likely to cause substantial harm to consumers. Botnets can exploit security vulnerabilities in IoT medical devices to send transmissions to other computers on the Internet resulting in denial of service attacks. Take, for example, the DDoS attack against Dyn on Oct. 21. That attack relied on infecting IoT devices such as cameras, monitors, and routers. It led to consumers' inability to load major websites such as Etsy, AirBnB, Netflix and Twitter.[10] Imagine if hospital patients likewise were denied access to critical medical services over the Internet.

A final risk relating to the IoT involves threats to health and safety from inadequate data security. As the IoT continues to flourish, a lack of reasonable security around connected health devices can have serious consequences for consumers. If hackers can hack an insulin pump – and there has been evidence that they can in some instances[11] – consumers' physical safety is at risk.

III. Data Security Best Practices

In light of these and other evolving threats, what's a company to do? We offer a number of resources for businesses looking to improve their privacy and data security practices. Let me highlight a few key suggestions here.

---

[10] Krebs on Security, *DDoS on Dyn Impacts Twitter, Spotify, Reddit*, Oct. 21, 2016, *at* https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify-reddit/.

[11] Elizabeth Weise, *Johnson & Johnson Warns of Insulin Pump Hack Risk*, USATODAY (Oct. 4, 2016), *available at* http://www.usatoday.com/story/tech/news/2016/10/04/johnson-johnson-warns-insulin-pump-hack-risk-animas/91542522/.

First, don't misrepresent the level of security you provide. We've brought several cases that challenged deceptive privacy and security claims made by businesses. For example, last year, we brought a case against a dental software company. According to our complaint, the company deceptively told its clients that it encrypted consumer data, when in fact, it did not use industry-standard encryption.[12] Furthermore, fine-print disclosures won't cure a misleading impression. In another case, we alleged that a company deceptively failed to disclose that patient reviews of doctors would be made public, when the disclosure of that fact was not clear and conspicuous.[13]

Second, protect against well-known, foreseeable threats. As I mentioned earlier, we recognize that there is no such thing as perfect security. Even if a company implements reasonable security measures, it may suffer a breach. Our law requires, not that security be perfect, but that companies reasonably protect against well-known threats. Again, our cases are instructive. For example, our complaint against GMR Transcription Services alleges that the company used independent typists to transcribe medical notes, but did not encrypt data in transmission. Nor did it reasonably oversee its service providers. Because of GMR's lax practices, according to our complaint, at least 15,000 files containing sensitive personal information – including consumers' names, birthdates, and medical histories – were available to anyone on the Internet.[14]

Third, take advantage of the numerous education resources that the FTC has distributed, often in conjunction with HHS. Last year, for example, we worked with HHS and the FDA to

[12] *See Henry Schein Practice Solutions, Inc.*, No. C-4575 (May 23, 2016), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3161/henry-schein-practice-solutions-inc-matter.
[13] *See Practice Fusion, Inc.*, C-4591 (Aug. 16, 2016), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3039/practice-fusion-inc-matter.
[14] *GMR Transcription Servs., Inc.*, No. C-4482 (F.T.C. Aug. 14, 2014) (decision and order), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3095/gmr-transcription-services-inc-matter.

develop an interactive tool to help health app developers. Developers can use this tool to determine which data security laws– including HIPAA, the Federal Food, Drug, and Cosmetic Act, the FTC Act, and the FTC's Health Breach Notification Rule – apply to them.[15] The FTC also released guidance to help health app developers build privacy and security into their apps.[16]

More generally, in 2015, the FTC launched its *Start with Security* initiative, which includes a guide for businesses that summarizes the lessons learned from the FTC's data security cases,[17] as well as 11 short videos.[18] These materials discuss ten important security topics, such as authentication, access controls, and network segmentation, and give advice about specific security practices for each. We recently distributed copies of the guide to members of a House subcommittee hearing about the data security obligations of small businesses and the challenges they face in meeting those obligations. After reviewing the guide, the subcommittee chair was so impressed he posted them on the subcommittee's website.

These business guidance materials are good but we are trying to make them even better. Many of our business education efforts relating to data security have emphasized reviewing FTC complaints and orders to understand what businesses should not do. Businesses would benefit from even more information from the FTC's closed data security cases. We therefore are undertaking a project to disclose more information when possible about the data security investigations we close. This will help illustrate how the FTC staff has applied the principles in its long-standing data security guidance materials to decide not to take enforcement action.

---

[15] *See* Mobile Health Apps Interactive Tool (Apr. 2016), *at* https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool.
[16] *See Mobile Health App Developers: FTC Best Practices* (Apr. 2016), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-app-developers-ftc-best-practices.
[17] *Start with Security: A Guide for Business* (June 2015), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business.
[18] *Start with Security: Free Resources for Any Business* (Feb. 19, 2016), *available at* https://www.ftc.gov/news-events/audio-video/business.

In addition to our more general guidance materials about data security, we have publications to assist businesses address specific threats, or to help particular industries. For example, the FTC has issued a publication describing the nature of the ransomware threat, how to defend against ransomware, and essential steps to take if businesses become victims of ransomware.[19] The FTC also developed guidance about ways to provide data security for connected devices, which includes tips such as designing products with authentication in mind and protecting the interfaces between an IoT product and other devices or services.[20]

Finally, we are stepping up efforts to educate small businesses on data security and privacy issues. We are creating a one-stop shop on our website with data security and privacy materials specifically for small businesses. And, in the coming months, we will expand our business outreach on data security issues, with a focus on helping businesses identify risks and develop data security plans.

IV. Conclusion

The FTC is committed to protecting the privacy and security of information, including health information. We want to find ways to get this done without imposing unnecessary or undue costs on businesses. I hope we can work together to get this done. Thank you.

[19] FTC Business Blog, *Ransomware – A Closer Look* (Nov. 10, 2016), *available at* https://www.ftc.gov/news-events/blogs/business-blog/2016/11/ransomware-closer-look.
[20] https://www.ftc.gov/tips-advice/business-center/guidance/careful-connections-building-security-internet-things