

# Direct-to-Consumer Neurotechnology: Privacy Implications

Deven McGraw, JD, MPH, LLM  
Partner  
Manatt, Phelps & Phillips, LLP

August 20, 2014

- Without privacy protections, people will engage in “privacy-protective behaviors” to avoid having their information used inappropriately.
  - Survey data show that 1 in 8 do not seek treatment, or lie about conditions, or seek care out of area, due to privacy concerns.
- Public trust in digital health depends on keeping data confidential & protected from unauthorized access, use and disclosure.
- NSA revelations, recent Facebook research controversy, and digital health data breaches may have increased the public’s sensitivity on privacy issues.

- Data part of the “traditional health care system” is regulated by HIPAA’s Privacy & Security Regulations
  - HIPAA applies only to “covered entities” and their “business associates” (contractors).
  - Covered entities include most hospitals, physicians, labs, pharmacies, health plans.
  - Entities/organizations that receive health information in order to perform services for the above = business associates
- Health data (and data with health implications) collected, used and disclosed by consumer-facing and non-health care system entities is not.
  - Most mobile apps and social networking sites marketed directly to consumers.
  - Medical devices also typically not covered.

# When is a Direct-to-Consumer Health Technology a Business Associate?

- Mere connectivity between a device or an app and a health care provider (or health plan) does not render the manufacturer a business associate of that provider (or plan),
- More of a “facts and circumstances” test. Relevant considerations:
  - Who provides the technology to the patient?
  - Who benefits from the technology being offered?
  - Who is responsible for the day-to-day operation or repair of the technology?
  - Who controls the information generated by the technology?
- Something that is “Direct-to-Consumer” is unlikely to trigger business associate coverage.

- Federal Trade Commission

- Authority under the FTC Act to prevent, and seek redress for, unfair or deceptive acts or practices.
- FTC has used this authority to penalize consumer-facing, for-profit companies for failing to abide by commitments regarding data use made in privacy policies.
- Less frequently, FTC has used this authority to stop unfair practices involving data use and collection.
- FTC also expects companies to implement reasonable security safeguards, and has acted in cases of unfair design, unfair default settings, and unfair data security practices that cause substantial injury to consumers and are not offset by other benefits.
- Congress enacted data breach notification requirements for non-HIPAA covered “personal health records” and related apps; overseen by FTC.
- Hosted “Internet of Things” workshop last May focusing on consumer-facing health tools. <http://www.ftc.gov/news-events/events-calendar/2014/05/spring-privacy-series-consumer-generated-controlled-health-data>

- Food and Drug Administration –
  - FDA’s medical device authority extends to apps and other software.
  - In guidance, FDA has established it will focus on apps that act as a medical device and whose functionality could cause a risk to patient safety if it were to not function as intended.  
<http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf>
  - FDA doesn’t regulate “privacy” but does focus on security to the extent it affects device performance and safety.
- States
  - In 2013, California extended the coverage of its state medical privacy law – the Confidentiality of Medical Information Act – to mobile apps and other hardware of software designed to “maintain medical information...in order to make the information available to an individual or a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage his or her information, or for the diagnosis, treatment, or management of a medical condition of the individual.”

- “Here’s Looking at You: How Personal Health Information is Being Tracked and Used,” California Healthcare Foundation Brief, July 2014.  
<http://www.chcf.org/~media/MEDIA%20LIBRARY%20Files/PDF/H/PDF%20HeresLookingPersonalHealthInfo.pdf>
  - Lack of awareness and recourse
  - Third parties’ use of data
  - Scoring/discrimination
  - Re-identification
- Privacy Rights Clearinghouse study of mobile health and fitness apps -  
<https://www.privacyrights.org/mobile-medical-apps-privacy-alert>
  - Many apps connect to third-party sites without user knowledge
  - Unencrypted connections potentially expose sensitive and embarrassing data
- Privacy and Security Risks in Connected Health, Hall, J. & McGraw, D. Health Affairs, vol. 33, No. 2 (February 2014).
- Best Practices for Mobile Application Developers, Center for Democracy & Technology and Future of Privacy Forum, <https://www.cdt.org/files/pdfs/Best-Practices-Mobile-App-Developers.pdf>



**Deven McGraw**

Partner

Manatt, Phelps & Phillips LLP

[dmcgraw@manatt.com](mailto:dmcgraw@manatt.com)