Key Developments in the Regulation of Software and Digital Health:
New Guidance, Initiatives, and Enforcement

May 2015

Marian J. Lee
202.887.3732
MJLee@gibsondunn.com

GIBSON DUNN

Beijing • Brussels • Century City • Dallas • Denver • Dubai • Hong Kong • London • Los Angeles • Munich
New York • Orange County • Palo Alto • Paris • San Francisco • São Paulo • Singapore • Washington, D.C.

Key Developments

1. **New FDA Guidance Documents**
   - Draft Guidance on Medical Device Accessories
   - Draft Guidance on General Wellness Products
   - Guidance on Medical Device Data Systems (MDDS)
2. **FTC Scrutiny and Enforcement**

FDA's Comments on the Regulation of Software

- "There is no definitive list"
- "The product spectrum is highly diverse and complex"
- "Decision requires a detailed review of the information available"
- **"Can be confusing very quickly"**

(Source: John F. Murray Jr., FDA/CDRH Software Compliance Expert, March 2010 Presentation)

FDA Draft Guidance: *Medical Device Accessories* (January 2015)

Is it an accessory?

1. **Intended for use with one or more parent devices**
   - Examine labeling and promotional materials for the accessory (rather than for parent device)
   - Generally would not include mobile phones used as general platform for mobile medical apps

Medical Device Accessories (cont'd)

2. **Intended to "support," "supplement," and/or "augment" the performance of one or more parent devices**
   - Support = enable or facilitate the parent
   - Supplement = add new function or new way of using parent, without changing the intended use of the parent
   - Augment = enable parent to perform intended use more safely or effectively

Medical Device Accessories (cont'd)

- Historically, FDA classified accessories by either --
  - Grouping them with the parent device, or
  - Creating unique, separate classification

→ *Regulate device accessories* ***based on the risks presented when they are used with parent devices***
  - *Will not impute all parent risks to the accessory*

→ *Encourage use of* ***de novo classification*** *for lower-risk accessories of a new type (FDCA § 513(f)(2))*

FDA Draft Guidance:
General Wellness Products (January 2015)

1. **Intended Use**
   - Maintaining/encouraging a general state of health or healthy activity – no reference to disease/condition
   - Associates role of healthy lifestyle with helping reduce the risk or impact of certain chronic diseases/conditions
2. **Present "very low risk" to user safety**
   - Invasive?
   - Pose risk to user's safety if device controls are not applied?
   - Novel questions of usability?
   - Biocompatibility?

→ ***Does not intend to examine whether these products are devices, or, if they are devices, whether they comply with FDA requirements***

FDA Guidance:
Medical Device Data Systems (February 2015)

- MDDS include hardware and software that permit the transfer, storage, conversion of formats, and display of medical data
- MDDS do not modify data or control the functions of any other medical device
- MDDS are not intended for use in active patient monitoring

→ *"Low risk" products that have an "important" role "in advancing digital health"*

→ *Will exercise enforcement discretion --*

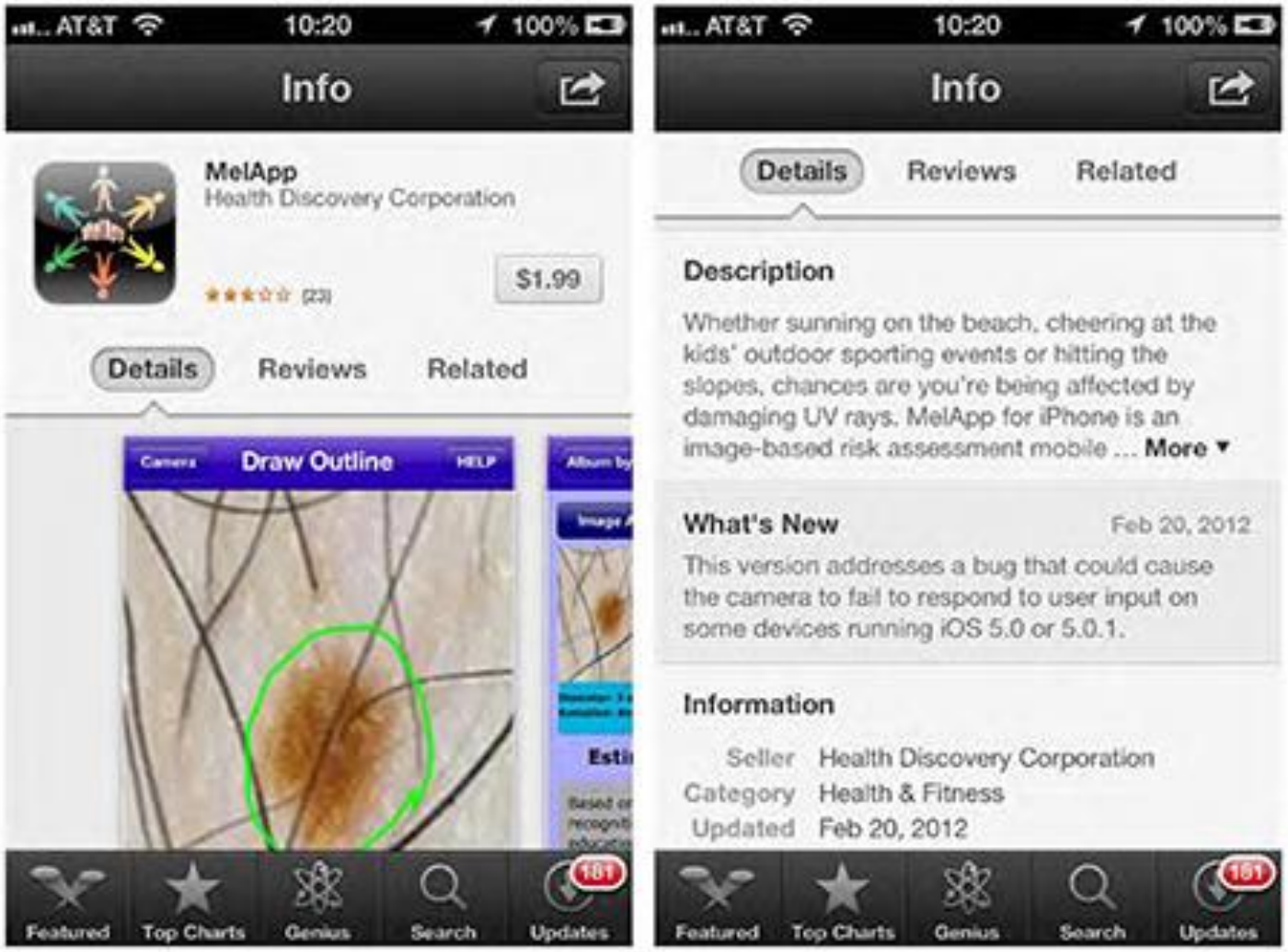
- *MDDS (21 CFR 880.6310),*
- *Medical image storage devices (21 CFR 892.2010)*
- *Medical image communications devices (21 CFR 892.2020)*

FTC Scrutiny and Enforcement

FTC's Broad Reach

- Power to prohibit "unfair or deceptive acts or practices in or affecting commerce" - FTC Act, Section 5
- Advertising for non-restricted medical devices
- Heightened focus on health-related privacy and data security in mobile and software technologies
  - "Mobile Privacy Disclosures: Building Trust Through Transparency: A Federal Trade Commission Staff Report"
  - "Medical Identity Theft: FAQs"
  - Health Breach Notification Rule
  - FTC Staff Report, "Internet of Things" (January 2015)
  - FTC Workshop on cross-device tracking (November 2015)

FTC Enforcement: "MelApp" and "Mole Detective"

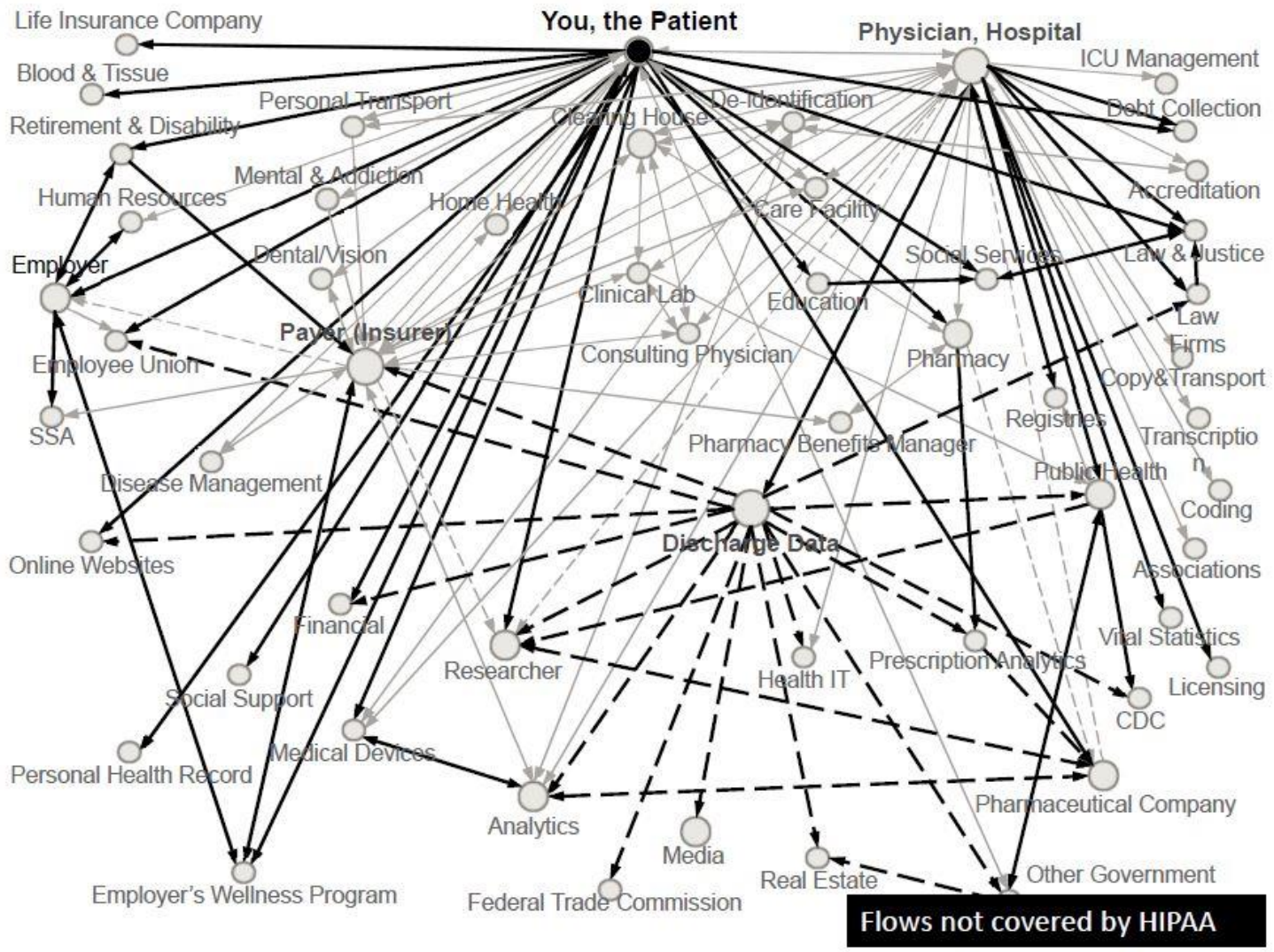


"MelApp" and "Mole Detective" (cont'd)

- Users submitted pictures and information about suspect moles and apps analyzed risk of melanoma (low, medium, high)
- Product claims
  - "patent protected state-of-the-art mathematical algorithms and image-based pattern recognition technology to analyze the uploaded image"
  - "first and only app to calculate symptoms of melanoma right on the phone"
  - "analyzes your mole using the dermatologist ABCDE method and gives you a risk factor based on the symptoms your mole may or may not be showing"
  - "increase the chance of detecting skin cancer in early stages"
  - "saves lives through the early detection of potentially fatal melanoma" using "shape recognition software"

"MelApp" and "Mole Detective" (cont'd)

- FTC's allegation: Deceptive claims that app accurately analyzed melanoma risk and could assess such risk in early stages, and that its accuracy was scientifically proven
- Final consent orders (April 2015)
  - Prohibit making claims that device can detect or diagnose melanoma, unless the representation is truthful, not misleading, and supported by competent and reliable scientific evidence in the form of human clinical testing of the device
  - Prohibit making any other deceptive claims about a device's health benefits or efficacy, or about the scientific support for any product or service
- Companies to pay over $20,000 total as part of settlements



FTC, Consumer Generated and Controlled Health Data, May 2014

FTC Meeting (2014): Digital Health Privacy Studies

- **2014 FTC study of 12 health and fitness apps and 2 wearables**
  - Focus on app traffic
  - Apps transmitted personal and identifying information to 76 different 3rd parties
- **2013 study of 43 free and paid health and fitness apps**
  - Focus on app traffic and privacy policies
  - 26% free apps and 40% paid apps had no privacy policy
  - 39% free apps and 30% paid apps sent data to someone not disclosed by developer
  - 13% free apps and 10% paid apps encrypted all data connections between apps and developer's website

FTC Enforcement: *LabMD*

- FTC complaint against LabMD, alleging that the medical testing lab failed to reasonably protect the security of the personal data (including medical information) of approximately 10,000 consumers
  - Billing information (SSN, dates of birth, health insurance providers, medical treatment codes) for over 9,000 consumers was found on a P2P file-sharing network
  - Documents containing sensitive personal information (SSN, bank accounts) of at least 500 consumers were in the possession of identity thieves
- FTC proposed order
  - Creation of comprehensive information security program
  - Evaluation of program every 2 years for next 20 years by independent expert
  - Require company to notify consumers whose information was or could have been accessible to unauthorized persons

FTC's Perspective

- "LabMD and other companies may well be obligated to ensure their data security practices comply with both HIPAA and the FTC Act. But so long as the requirements of those statutes do not conflict with one another, a party cannot plausibly assert that, because it complies with one of these laws, it is free to violate the other."
- "There are significant privacy implications where health routines, dietary habits, and symptom searches are capable of being aggregated using identifiers unique to that consumer."
- "Although the Commission currently has authority to take action against some IoT [Internet of Things] related practices, it cannot mandate certain basic privacy protections such as privacy disclosures or consumer choice absent a specific showing of deception or unfairness. Commission staff thus again recommends that Congress enact broad based (as opposed to IoT specific) privacy legislation…. In the meantime, we will continue to use our existing tools to ensure that IoT companies continue to consider security and privacy issues as they develop new devices."

Thank You