AHLA

N. When Health Care Meets Technology: What Lawyers Need to Know in the Era of Health IT and Digital Health

Jackie Olson (Moderator)
Global Health and Wellness Counsel
Apple
Sunnyvale, CA

Afia Asamoah
Senior Counsel and Trust and Compliance Officer
Verily Life Sciences
San Francisco, CA

Cora T. Han
Senior Attorney, Division of Privacy and Identity Protection
Federal Trade Commission
Washington, DC

Lucia C. Savage
Chief Privacy and Regulatory Officer
Omada Health
San Francisco, CA

When Healthcare Meets Technology:

What Lawyers Need to Know in the Era of Health IT and Digital Health

Jackie Olson, facilitator
Global Health and Wellness Counsel
Apple Inc.

Afia Asamoah
Senior Counsel & Trust and Compliance Officer
Verily Life Sciences LLC, an Alphabet Company

Cora Han
Senior Counsel
Division of Privacy and Identity Protection
Federal Trade Commission

Lucia Savage
Chief Privacy & Regulatory Officer
Omada Health, Inc.

What is Digital Health?

- Digital health: Convergence of software, mobile and digital technologies that may influence the way healthcare is delivered and treated and the way consumers and patients manage disease in conjunction with their physicians, nurses and healthcare professionals
- Includes (per FDA)
  - mobile health (mHealth), health information technology (IT), wearable devices, telehealth and telemedicine, and personalized medicine

Digital Health: Opportunities and Challenges

Opportunities

- Continuous, detailed health information informing healthcare and payment decision-making
- Increased patient engagement in care
- Increased flexibility for patients in managing care
- Increased efficiencies and improved outcomes in healthcare delivery

Digital Health: Opportunities and Challenges

Challenges

- What do you do with so much data? Is it just noise?
- Interoperability
- Privacy
- Security
- Patient Safety
- Intellectual Property
- Maintaining appropriate competition
- Cost
- Billing/payment integrity

Who Does What: Food and Drug Administration

- An agency of U. S. Dept of Health and Human Services
- Authority to review the safety and effectiveness of medical products
  - New definition of medical device in 21st Century Cures
- CDRH, the Center for Devices and Radiological Health, reviews medical devices, including in vitro diagnostics and software as a medical device
- Creating an Office of Digital Health within the Office of the Center Director
  - Focus on “medical device IT”, including artificial intelligence, wireless medical devices, telemedicine
- Cybersecurity related to how security impacts the safety or effectiveness of how a device functions
- Mobile medical apps are medical devices within FDA jurisdiction, but agency has taken a risk based approach and exercised enforcement discretion with respect to certain mobile medical apps
  - Mobile platform manufacturers not medical device manufacturers

Who Does What: Centers for Medicare and Medicaid Services

- An operating division of HHS, and the largest division within the largest civilian federal agency
- Runs Medicare
- Develops baseline rules for Medicaid and for disbursement of Medicaid funds
- Implements the ACA
- CMS developed the rules and administered the programs that financially rewarded hospitals and providers for using certified EHRs in specified ways, aka the “meaningful use” program.
- Tests innovations that use digital tools through programs funded by the Center for Medicare and Medicaid Innovation, or CMMI.

Who Does What: Federal Trade Commission

- Independent law enforcement agency
- Section 5 of the Federal Trade Commission Act broadly prohibits “unfair or deceptive acts or practices in or affecting commerce.”
  - Deception: a material representation or omission that is likely to mislead consumers acting reasonably under the circumstances
  - Unfairness: a practice that causes or is likely to cause substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers

  Note: Section 5 authority extends to both HIPAA and non-HIPAA covered entities
- FTC’s Health Breach Notification Rule requires certain businesses to notify consumers when the security of their electronic health information is breached.

  Note: Rule does NOT apply to entities covered by HIPAA

Who Does What: Federal Communications Commission

- Another independent commission
- Has authority over use of broadband and transmission wavelengths
- Includes behavior of the companies who provide broadband services on which mobile health platforms run
  - And their servers, where health information may pass or be stored.
- Includes oversight of rural broadband infrastructure.

Who Does What: Dept. of Health and Human Services, Office for Civil Rights

- A Staff Division within HHS, OCR
- Enforces the HIPAA Privacy, Security and Breach Notification Rules
- Enforces other federal civil rights rules as they apply to HHS programs.
- Collaborates with FDA, ONC and FTC on areas of common interest and expertise.

Who Does What: HHS, Office of the Inspector General

- An independent office within HHS, the Office of the Inspector General enforces laws against fraud, abuse, and kickbacks.
- OIG has new responsibilities under 21st Century Cures to enforce rules against "information blocking" in health information technology, once such rules are final.

Who Does What: Office of the National Coordinator for Health IT

- A Staff Division within HHS, the Office of the National Coordinator for Health IT
- Specifies by regulation minimum functionality for "certified electronic health records" and oversees certification and withdrawal of certification.
- New authorities in 21st Century Cures to define and help OIG enforce rules against "information blocking"
- Develops policy recommendations on privacy, security and interoperability of health IT writ large—not limited to EHRs.

Case Study Review

The Case Study: Issues to Look For

- Certified Electronic Health Record or other Health IT?
- Covered Entity or Non-covered Entity?
- Does the FTC have jurisdiction?
- International vs domestic?
- How will the wearable be regulated? What kind of wearable is it? Who supplied it to the individual?

Appendix

FDA Resources

FDA and 21st Century Cures

- Specific impact of law yet to determined, depends on implementation by FDA
- Revision to definition of medical device
  - Exempts medical device data systems (MDDS), wellness devices, devices for admin support and EHRs
  - Some clinical decision support NOT medical devices
- Consider whether software is an accessory or component of medical device
- FDA available software-related guidances and regulations
  - Content of premarket submissions for software contained in med devices (May 2005)
  - General principles of software validation (Jan. 2002)
  - Off-the-shelf software use in med devices (Sept. 1999)

FDA and Software

- Consider whether software is an accessory or component of medical device
- FDA available software-related guidances and regulations
  - Draft Guidance on Software as a Medical Device (SaMD): Clinical Evaluation (Aug. 2016)
  - Content of premarket submissions for software contained in med devices (May 2005)
  - General principles of software validation (Jan. 2002)
  - Off-the-shelf software use in med devices (Sept. 1999)
- Still awaiting clinical decision support guidance

FDA and Health IT

- Draft FDASIA Report on Health IT and FDA Oversight (issued 4/3/14)
  - Risk based regulatory strategy
  - Participating Agencies: FDA, FCC, ONC FDA focus on "medical device IT"
    - E.g., computer diagnostic software
  - Other rules apply to "health management IT"
    - E.g., electronic medication administration system, clinical software
  - Software
    - FDA CDRH in May announced a Digit Health Unit in the Office of the Center Director under direction of Bakul Patel, Associate Center Director for Digital Health

FDA and Mobile Apps

- Only subset of apps are the focus of FDA regulatory oversight
  - Guidance available
- Enforcement discretion
  - Still a medical device, FDA just not enforcing applicable regulations
  - E.g., simple tools to organize and track health information; self manage conditions without providing specific Tx or Tx suggestions
- FDA jurisdiction depends on what you say
  - Fitness, health, wellness likely okay
  - See FDA General Wellness Guidance
- Guidance does not address software that performs patient-specific analysis to aid or support clinical decision-making

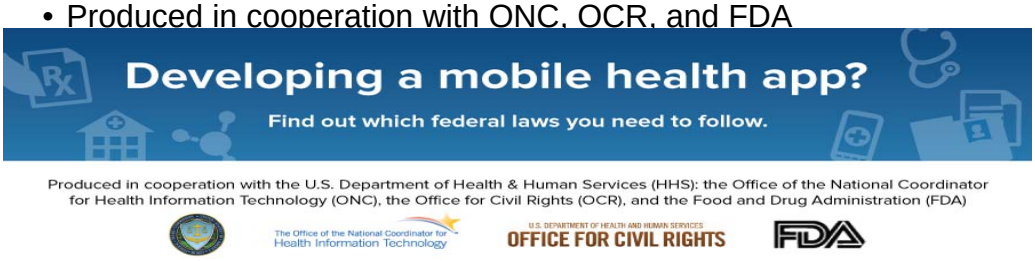
FDA and Cybersecurity Concerns

- Med devices are vulnerable to security breaches, potentially affecting safety and effectiveness of device
  - Risk increases as devices are connected to Internet, hospital networks, other med devices
- Manufacturers are responsible for identifying risks and hazards to devices, including risks related to cybersecurity
- FDA Guidance
  - Guidance for Industry – Postmarket Management of Cybersecurity in Medical Devices (Dec. 2016)
  - Guidance for Industry - Content of Premarket Submissions for Management of Cybersecurity in Medical Devices (Oct. 2014)
  - Guidance for Industry - Cybersecurity for Networked Medical Devices Containing Off-the-Shelf Software (Jan. 2005)
  - FDA-CMS Parallel Review Program (Oct. 2016)

FTC Resources

FTC Resources

- Mobile Health Apps Interactive Tool – to help health app developers figure out which federal laws might apply to their app
  - Produced in cooperation with ONC, OCR, and FDA



FTC Resources

Mobile Health Apps Developers: FTC Best Practices

- Minimize data
- Limit access and permissions
- Keep authentication in mind
- Consider the mobile ecosystem
- Implement security by design
- Don’t reinvent the wheel
- Innovate how you communicate with users
- Don’t forget about other applicable laws

FTC Resources (www.ftc.gov)

- Complying with the FTC’s Health Breach Notification Rule
- Mobile Health Apps Interactive Tool
- Mobile Health Apps Developers: FTC Best Practices
- Start with Security: A Guide for Business
- Ransomware – A closer look
- Big Data: A Tool for Inclusion or Exclusion?

HHS Resources

OCR HIPAA Resources

- HIPAA (in the US)
  - HHS HIPAA guidance for health app developers
    - Includes interactive Q/A tool
  - ONC/OCR Model Privacy Notice and related challenge
  - HIPAA Privacy, Security and Breach Notification Rule (2013—unofficial)

- Data sharing Permitted by HIPAA
  - Health care treatment
  - Health care operations
  - Public health
  - Health care [regulatory] oversight
- Data aggregation
- Individuals' Rights to Get (or Transmit from an EHR) their own data

ONC Resources

ONC Resources on Health IT, Privacy & Security

- Mobile Device Roundtable and Mobile Health Security for Providers
- Medication List Project—a test case using apps, the FHIR based API, and the rights under 45 CFR 164.524
- Security Risk Assessment Tool
- API Privacy & Security Task Force
- Report to Congress on Non-Covered Entities
- Privacy & Security Guide

When Healthcare Meets Technology:
What Lawyers Need to Know
in the Era of Health IT and Digital Health

A CASE STUDY

Two academic medical centers (Red and Blue) and TechCo, a well-known tech company, partner to study a particular devastating and deadly disease. They propose to combine EHR data from Red's HIPAA covered EHR and from Blue's digital health record system which is not covered by HIPAA s to solicit research participants. Red and Blue will also collect and store in their respective data systems health information from research volunteers. Red is a HIPAA Covered Entity, but Blue's research institution is not a Covered Entity. Participants who volunteer will be supplied with wearable sensors and other electronic data collection equipment supplied by TechCo. TechCo will collect this data in a business unit that is not a HIPAA Covered Entity or Business Associate. The data from the wearable sensors will be collected by TechCo 24/7 for a year.

Once all the data is collected, Red, Blue and TechCo will, through a third-party data company, combine data from Red's and Blue's data systems and the information TechCo has collected via the wearable sensors. Red, Blue and TechCo will then use statistical methods and algorithms to find particular patterns that might provide insights into treatments for the devastating disease. The combined data will be housed in a large secure server farm in the Philippines to reduce the costs of storage and administration.

The project will yield data outputs that are statistical, but physicians at Red and Blue will also get back identifiable data on particular individuals for whom medical issues have been identified.

On Month 14, after the wearable data collection ends, a group of activated, organized participants write to the research project and ask to have copies of their data combined from all three sources (Red, Blue and TechCo.) provided back to them via an app one of the participants wrote for this sub-group. The App, if allowed to work, delivers the health information to each user's smartphone.