Mobile Health (mHealth) Applications in a Health Care Environment

Brandon Goulter, Facility Compliance Professional
Steven Baruch, Senior Compliance Director

Dignity Health.

Agenda

- Overview of Mobile Health Applications & The State of Mobile Health
- Mobile Health Applications Related to Patient-Centric Care
- Legal and Privacy Implications
  - Health Insurance Portability and Accountability Act (HIPAA)
  - Federal Food, Drug, and Cosmetic Act (FD&C)
  - Federal Trade Commission Act (FTC)
  - FTC's Health Breach Notification Rule.
- HIPAA and the Liability for Clinical Providers

Reflection

"The internet of things connects our devices to help us improve our healthy lifestyles; and big data may help researchers improve health outcomes for our nation. At the same time, these important tools also create risks to the privacy and security of our health information"

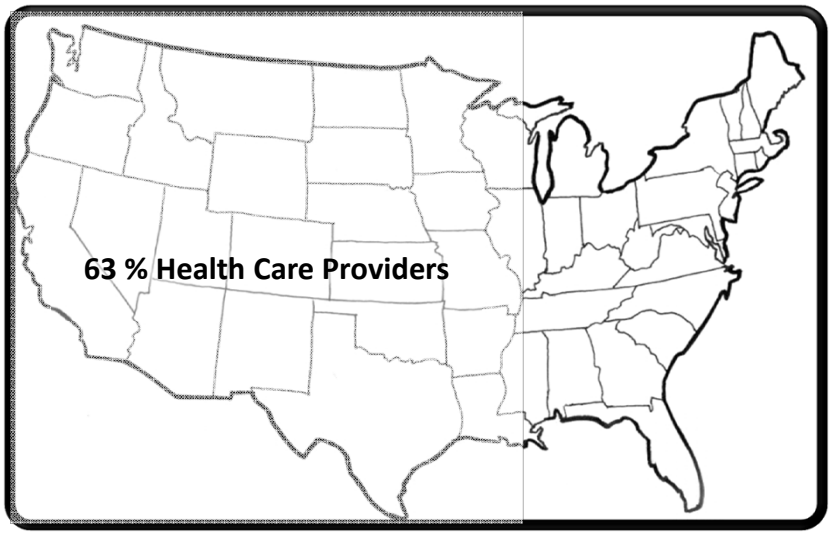
- Jocelyn Samuels, Director of the HHS Office for Civil Rights

(October 13, 2016)

Dignity Health.

3

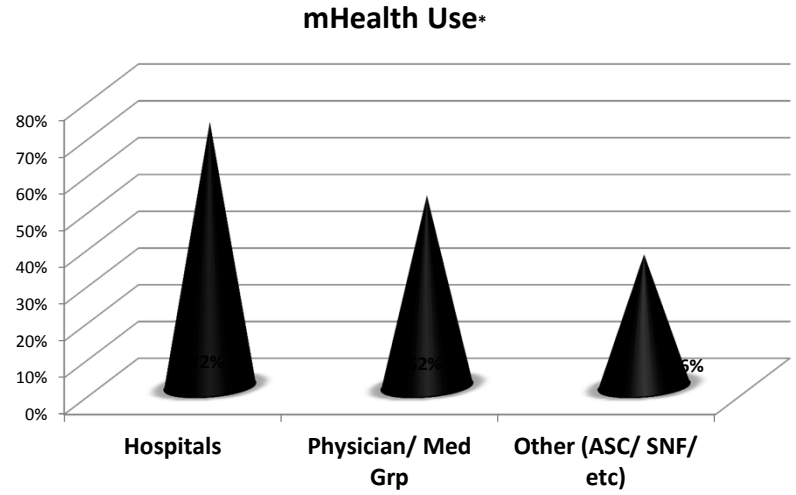
mHealth Applications



Dignity Health.

4

mHealth Applications

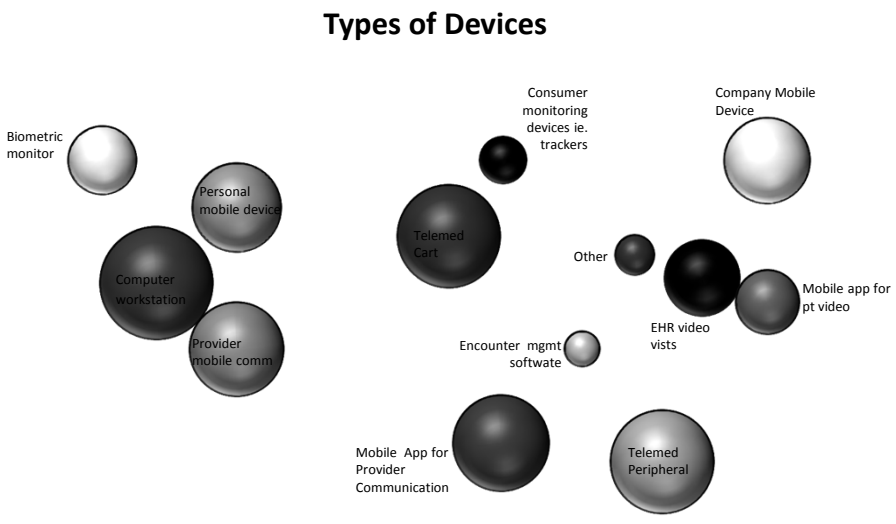


Dignity Health.

*2016 Avizia Healthcare Executive Survey

5

mHealth Applications



Dignity Health.

6

mHealth Applications

The largest anticipated future growth of mHealth…

Patient video visits, including mobile apps

Dignity Health.

7

Mobile Health Applications

- Affordable Care Act
  - Made access to health Information more impo
  - Value over Volume
- Meaningfully Using Data to treat
  - Chronic Diseases (e.g. Diabetes)
  - Remote monitoring of data (e.g. electrocardiogram or fetal monitoring)
- Enables the physician to work with the patient to make better and more informed decisions

Dignity Health.

8

Examples

- Telehealth & Communication:
  - Encrypted Messaging (OnePass/Consult Accelerator, Signal, WhatsApp)
  - Video Conferencing/Consulting
- Medical Device:
  - Concussion Monitoring (BrainCheck),
  - Patient Fetal/EKG Monitoring (Airstrip).
  - Glucose Monitoring
- Patient Management
  - Electronic Preventive Services Selector (AHRQ)
- Personal Health
  - Fitbit
  - Microsoft HealthVault (PHR)

Dignity Health.

9

Pro's and Con's of mHealth Technology

- Patients & Providers Have access to data they wouldn't ordinarily have
- Patients have access to specialists they wouldn't ordinarily have
- Timely access to emergency care
- Physicians are able to diagnosis, provide guidance, assist with preparing a patient for transfer, and assist in lowering the rates of unnecessary care.
- Encourage healthy behavior
- Lack of ability to bill for "virtual visits"
- Data Security / Data Privacy
- Complicated regulations
- Lack of Regulation (e.g. Apps that should be regulated, aren't)
- Long and complicated privacy policies or terms and conditions.

Dignity Health.

10

Regulatory Environment

- Office for Civil Rights (OCR):
  - Health Insurance Portability and Accountability Act (HIPAA)
- Food and Drug Administration (FDA)
  - Federal Food, Drug, and Cosmetic Act (FD&C)
- Federal Trade Commission (FTC)
  - Federal Trade Commission Act
  - FTC's Health Breach Notification Rule
- State Specific Laws
  - E.g. California includes the Confidentiality of Medical Information Act (CMIA)

Dignity Health.

11

mHealth Device / mHealth App (Application)

A mHealth App is any application that can be run on a mobile platform with or without wireless (internet) connectivity. This includes any application that is running as a software as a service (e.g. hosted on a server and is customized to run on a portable or mobile device).

The intended use of the device, <u>not the hardware</u>, is what will inevitably define which regulation will be used when assessing compliance or liability.

Dignity Health.

12

Where does your mHealth device fall?

- Determine which laws apply. Multiple Laws?
  - Health Information Present? FTC / HIPAA
  - Prescription Needed? FTC/ HIPAA / FD&C (FDA)
  - Medical Device? HIPAA / FDA
    - Minimal Risk? FTC / FDA (Not enforced)
  - Mobile Medical App? FTC / FDA / HIPAA
- Are you seeing a trend? Lets dive into each law.

Dignity Health.

13

Health Insurance Portability & Accountability Act (HIPAA)

- HIPAA's focus is on provider data; when HIPAA does not apply:
  - Patients can collect data on themselves for their own purposes
  - Patients may voluntarily collect data and give to covered entity.
  - Healthcare providers may receive data in any fashion the patient chooses
- Any solution deployed by a covered entity requires a HIPAA risk assessment be performed
- Litmus Test: App Developer must be creating, receiving, maintaining or transmitting protected health information (PHI) on behalf of a covered entity or business associate.

Dignity Health.

14

Health Insurance Portability & Accountability Act (HIPAA)

- Health information is protected by the HIPAA rules when it is individually identifiable and created, received, maintained, or transmitted by a covered entity (or a business associate on the covered entity's behalf) in its role as a covered entity.
  - mHealth application developers are business associates if:
    - They are directly contracting with the healthcare organization;
    - The device or software allows a patient to enter PHI;
    - The information transfers directly into the patient's EHR for the purposes of medical decision making and planning.

Dignity Health.

15

Federal Food, Drug, and Cosmetic Act (FD&C Act)

- The Food and Drug Administration (FDA) enforces the FD&C Act
- The FD&C Act regulates the safety and effectiveness of medical devices, including certain mobile medical apps.
- Scope is limited to those devices that pose a greater risk.
  - Class I, II, III – Lowest to highest in terms of regulatory controls
  - Current Regulations indicate that most mobile devices fall into Class I or II
  - Premarket notifications are often required on Class II under the submission type of 510k.

Dignity Health.

16

Medical Device Companies

- Subject to the jurisdiction of the FDA
- May be a health care provider if it furnishes, bills, or is paid for "health care" in the normal course of business.
- Business Associate agreements are **not** required for treatment related disclosures.
- When is a Business Associate Agreement Needed?

Navigating regulations regarding medical devices can be complicated, consider guidance from counsel

Dignity Health.

17

Trust Gained / Trust Lost?

- Internet Connected Children's Toys: Privacy Concern?
  - FTC complaint filed Dec. 6
  - Did not obtain consent to disclose children's recordings to Nuance Communications, Inc. who is using the data for voice recognition products.
- Pokémon Go!
  - Full control over your Google Account and no notice to consumers.

Dignity Health.

18

Federal Trade Commission (FTC) Act

- Companies must not mislead consumers!
  - Consider all statements to consumers that when taken together don't create deceptive or misleading impressions.
  - Don't promise to keep information confidential when, in fact, you will ask customers later to authorize the disclosure of the same information.
  - Eliminate contradictions from Privacy Statements, Terms and Conditions, or Terms of Use.
- Bottom Line: If you say you will or will not do something, make sure that what is written is happening.

Dignity Health.

19

FTC's Health Breach Notification Rule

- Apply only when you've experienced a breach of PHR-identifiable health information.
  - Personal Health Records (Mobile & Non-Mobile)
  - Businesses that deal in Medical Information but are not covered by HIPAA.
- Triggers for Notification
  - Unsecured/Unauthorized acquisition
- Notification to:
  - Each affected person who is a citizen or resident of the United States; the Federal Trade Commission; and in some cases, the media.

Dignity Health.

20

Enforcement & Liability

- Catholic Health Care Services ($650,000)
  - Failure of a Business Associate to secure PHI stored on a mobile device (Unencrypted iPhone without password protection)
  - Individuals impacted: 412
  - Lack of Enterprise-Wide Risk Assessment
- Feinstein Institute for Medical Research ($3.9 Million)
  - Unencrypted Laptop stolen from an employee's vehicle
  - Contained 13,000 patients' and research participants ePHI
  - OCR investigation found other deficiencies, which underscores the need to encrypt portable devices and other necessary safeguards

Enforcement & Liability

- Biosense Technologies (2013) – uCheck (Urinalysis)
  - FDA Required Biosense to seek 510(k) clearance of its mobile medical app or convince the FDA that such clearance is not needed.
  - Smartphone App: Not Cleared, Strips: Cleared
  - Currently no longer available in the United States – India Only.
- Carrot Neurotechnology (2015) – Ultimeyes (Improve Vision)
  - "Scientifically shown to improve vision" through the use of a mobile interactive game.
  - $150,000 settlement with the FTC and an agreement to stop making deceptive claims related to improving patient vision using an App.
  - Any future advertising would require verbose and competent scientific evidence.

Legal and Privacy Implications: Takeaways

Ensure you are doing what you state you are doing with the data.

Ensure you have a Business Associate Agreement for provider sponsored devices.

If the Mobile Application is a Medical Device, ensure it is FDA cleared or approved.

If the Mobile Application is a Medical Device, ensure you know whether the representative from the company is acting as a Covered Entity or a Business Associate.

Dignity Health.

23

Legal and Privacy Implications: Takeaways

Perform risk assessments on all devices that store PHI that are being used to store or transmit data on behalf of your organization.

Ensure your leadership teams and employees are aware that device manufacturers should be cleared by Compliance, Privacy and Security prior to their use (and who to call!)

Lack of follow-through may cost the organization time, money, and a corrective action plan!

Dignity Health.

24

Tools & Resources

- Federal Trade Commission: Mobile Health Apps Interactive Tool (https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool)
- FDA Cleared Mobile Apps (http://www.fda.gov/MedicalDevices/DigitalHealth/MobileMedicalApplications/ucm368784.htm)
- FDA Guidance Document on Mobile Medical Apps (http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf)
- DHHS / OCR Website for App developers (http://hipaaqsportal.hhs.gov/)
- DHHS / OCR Website: Health Information Privacy (http://www.hhs.gov/hipaa/for-professionals/faq)
- Podcasts (iTunes, etc.): Help Me With HIPAA, Security Now, This Week in Law, Unfair & Unbalanced (SCCE).

Dignity Health.

25

Questions?

Dignity Health.

26