Arnold & Porter

CONFIDENTIALITY COALITION

Personal Health Information Beyond HIPAA Protection

Who is Regulating its Privacy? Who Should, and How?

Tina Olson Grande, MHS
Chair, Confidentiality Coalition
SVP, Healthcare Leadership Council

March 5, 2019

Nancy L. Perkins, MPP, JD
Counsel, Arnold & Porter
Washington, DC

Confidentiality Coalition

A broad group of organizations working to ensure that we as a nation find the right balance between the protection of confidential health information and the efficient and interoperable systems needed to provide the very best quality of care.

Members

AdventHealth
Aetna, a CVS Health business
America's Health Insurance Plans
American Hospital Association
American Society for Radiation Oncology
AmerisourceBergen
Amgen
AMN Healthcare
Anthem
Ascension
Association of American Medical Colleges
Association of Clinical Research Organizations
athenahealth
Augmedix
Bio-Reference Laboratories
Blue Cross Blue Shield Association
BlueCross BlueShield of Tennessee
Cardinal Health
Cerner
Change Healthcare
Children's Hospital of Philadelphia (CHOP)
CHIME
Cigna
Ciox Health
City of Hope
Cleveland Clinic
College of American Pathologists
Comfort Keepers
ConnectiveRx
Cotiviti
CVS Health
Datavant
dEpid/dt Consulting Inc.
Electronic Healthcare Network Accreditation Commission
EMD Serono
Express Scripts
Fairview Health Services
Federation of American Hospitals
Genetic Alliance
Genosity
Healthcare Leadership Council
Hearst Health
HITRUST
Intermountain Healthcare
IQVIA
Johnson & Johnson
Kaiser Permanente
Leidos
LEO Pharma
Mallinckrodt Pharmaceuticals
Marshfield Clinic Health System
Maxim Healthcare Services
Mayo Clinic
McKesson Corporation
Medical Group Management Association
Medidata Solutions
Medtronic
MemorialCare Health System
Merck
MetLife
National Association for Behavioral Healthcare
National Association of Chain Drug Stores
National Community Pharmacists Association
NewYork-Presbyterian Hospital
NorthShore University Health System
Pfizer
Pharmaceutical Care Management Association
Premier healthcare alliance
SCAN Health Plan
Senior Helpers
State Farm
Stryker
Surescripts
Teladoc
Texas Health Resources
UCB
UnitedHealth Group
Vizient
Workgroup for Electronic Data Interchange
ZS Associates

Why is Congress interested in privacy?

Facebook charged with misleading users on health data visibility

A report says the social network's handling of personal health information put its users' health at risk.

2019 Data Breach Barometer Report Shows Massive Increase in Exposed Healthcare Records

HEALTH • GLAXOSMITHKLINE

GlaxoSmithKline Is Acquiring a $300 Million Stake in Genetic-Testing Company 23andMe

TECH

Google Exposed User Data, Feared Repercussions of Disclosing to Public

Google opted not to disclose to users its discovery of a bug that gave outside developers access to private data. It found no evidence of misuse.

Popular apps caught secretly sending health data and more to Facebook, should Apple intervene?

Michael Potuck - Feb. 22nd 2019 9:11 am PT @michaelpotuck

You Give Apps Sensitive Personal Information. Then They Tell Facebook.

Under Armour is urging 150 million customers to take action after its wildly popular fitness app was hacked

Genealogy site MyHeritage discovered passwords of 92 million accounts on a private server, but says the data was encrypted

How Does HIPAA Apply to Wearable Health Technology?

The use of wearable health technology is expected to expand substantially within the next few years. How do HIPAA security and privacy protections apply to wearables and the health data they collect and store?

Facebook Accused of Privacy Violations and Exposure of Sensitive Health Information Disclosed in Private Groups

Who is in charge?– Key Committees

- **Senate Committees**
  - Commerce, Science & Transportation
    - Hearing on “Policy Principles for a Federal Data Privacy Framework in the United States” (February 27, 2019)
  - Judiciary
  - Banking
  - Finance
- **House Committees**
  - Energy & Commerce
    - Consumer Protection & Commerce Subcommittee
      - Hearing on “Protecting Consumer Privacy in the Era of Big Data” (February 26, 2019)

Who is in charge?– Key Members of Congress

- **Senate**
  - Richard Blumenthal (D/CT)
  - Maria Cantwell (D/WA)
  - Ed Markey (D/MA)
  - Jerry Moran (R/KS)
  - Brian Schatz (D/HI)
  - John Thune (R/SD)
  - Roger Wicker (R/MS)
- **House**
  - Frank Pallone (D/NJ-6)
  - Jan Schakowsky (D/IL-9)
  - Tony Cárdenas (D/CA-29)
  - Peter Welch (D/VT-At large)
  - Cathy McMorris Rodgers(R/WA-5)
  - Greg Walden (R/OR-2)

What is Congress seeking to achieve?

116th Congress

- S.142 – American Data Dissemination Act
- S. 189 – Social Media Privacy Protection and Consumer Rights Act of 2019

115th Congress

- Consumer Data Protection Act
- S. 3744 – Data Care Act of 2018
- S.2639 – CONSENT Act
- H.R.2520 – BROWSER Act of 2017
- H.R.6864 – Information Transparency & Personal Data Control Act

Proposed Privacy Frameworks/Model Legislation

U.S. Chamber of Commerce

NIST National Institute of Standards and Technology
U.S. Department of Commerce

intel

Information Technology Industry Council

National Telecommunications and Information Administration
United States Department of Commerce

HIPAA Implications

- How would a new national privacy approach affect covered entities and business associates under HIPAA?
- Issues to consider
  - Federal pre-emption
  - Fines and penalties
  - Consent
  - Definition of personal data/sensitive information
  - Individual rights
  - Regulatory oversight

Reaction of Industry

- “HIPAA for all”
- HIPAA carve out
- Details matter
- New privacy paradigm for health information

Scope of HIPAA Privacy and Security Rules

- The HIPAA Privacy and Security Rules are applicable only to:
  - protected health information ("PHI")
    - as used and/or disclosed by
  - covered entities and their business associates
- "covered entities" are only:
  - **Health plans** (HMOs, PPOs, health insurers);
  - **Health care clearinghouses** (companies that convert health data into standard formats); and
  - **Health care providers** *IF* they conduct "standard" reimbursement-related transactions electronically.
- PHI is individually identifiable health information in any form, but only:
  - if it is created, received or maintained by a HIPAA covered entity or an employer.

Who Has Health Data Outside of HIPAA's Regulatory Scope?

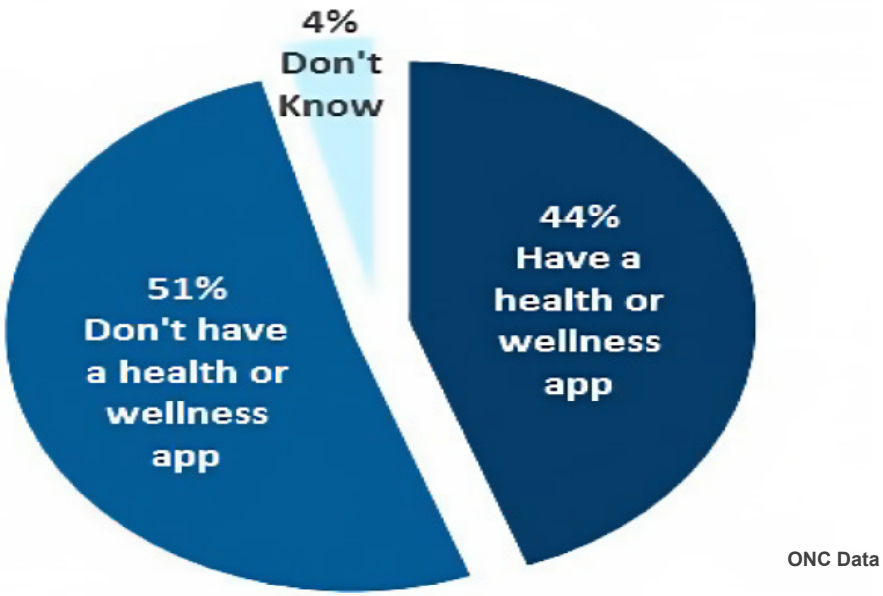
These are just some examples:

- Health care providers who do not bill patients' insurers electronically
- Pharmaceutical companies
- Researchers who are not clinicians who bill patients' insurers
- Medical device manufacturers (with some exceptions)
- Vendors of Personal Health Records for individuals
- Life insurers
- Ancestry.com and 23andMe
- Mobile health apps such as FitBit and Google Fit

Who is Using a Mobile Health App?

More than four in ten smartphone or tablet owners possessed a health or wellness app.

Figure 10: Percent of individuals who have a health & wellness app on their smartphone or tablet, 2017.



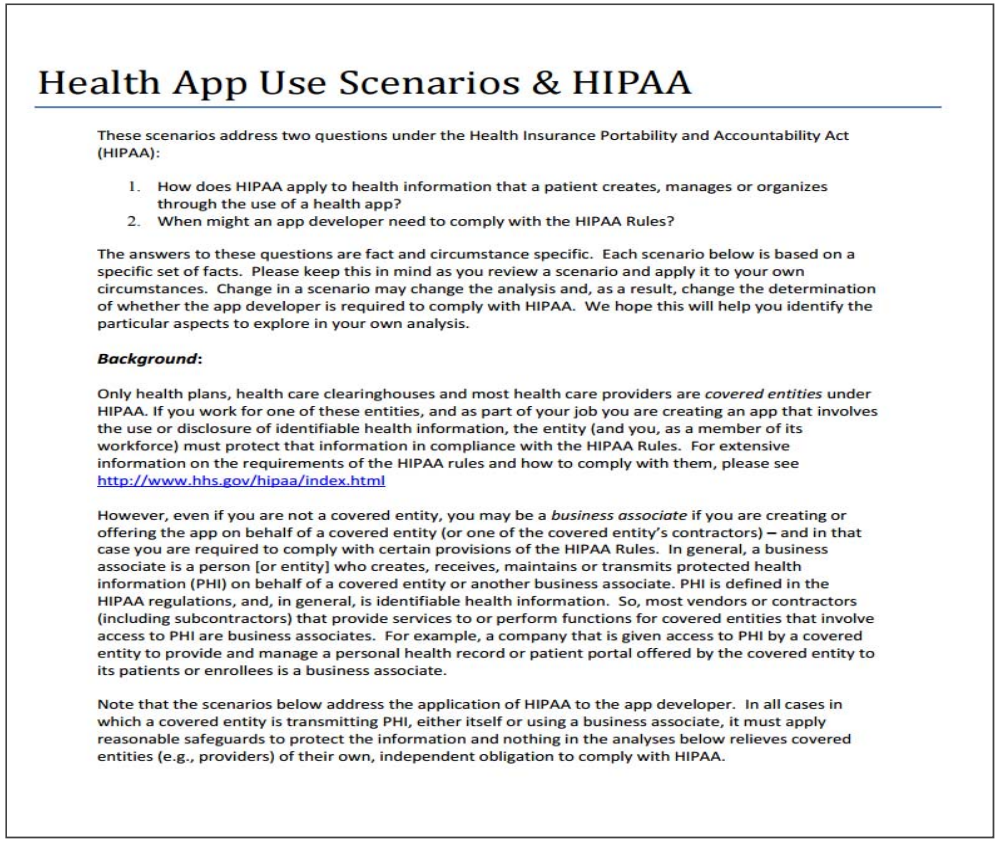
ONC Data Brief, No. 40, April 2018

HIPAA and Mobile Health Technologies

- Mobile health ("mHealth") technologies are subject to the HIPAA privacy and security rules only if a HIPAA covered entity or business associate:
  - Uses the technology;
  - Offers the technology for use by an individual for purposes of the covered entity/business associate's relationship with the individual.
- Other mobile health apps are not HIPAA-regulated.

HHS Guidance

- The HHS Office of Civil Rights (OCR) created a developer portal to provide guidance on the application of the HIPAA rules to mobile apps and other mHealth technologies.
- HHS-OCR guidance includes specific examples of when a health app is or is not subject to the HIPAA rules.



Health App Use Scenarios & HIPAA

These scenarios address two questions under the Health Insurance Portability and Accountability Act (HIPAA):

1. How does HIPAA apply to health information that a patient creates, manages or organizes through the use of a health app?
2. When might an app developer need to comply with the HIPAA Rules?

The answers to these questions are fact and circumstance specific. Each scenario below is based on a specific set of facts. Please keep this in mind as you review a scenario and apply it to your own circumstances. Change in a scenario may change the analysis and, as a result, change the determination of whether the app developer is required to comply with HIPAA. We hope this will help you identify the particular aspects to explore in your own analysis.

***Background*:**

Only health plans, health care clearinghouses and most health care providers are *covered entities* under HIPAA. If you work for one of these entities, and as part of your job you are creating an app that involves the use or disclosure of identifiable health information, the entity (and you, as a member of its workforce) must protect that information in compliance with the HIPAA Rules. For extensive information on the requirements of the HIPAA rules and how to comply with them, please see http://www.hhs.gov/hipaa/index.html

However, even if you are not a covered entity, you may be a *business associate* if you are creating or offering the app on behalf of a covered entity (or one of the covered entity's contractors) – and in that case you are required to comply with certain provisions of the HIPAA Rules. In general, a business associate is a person [or entity] who creates, receives, maintains or transmits protected health information (PHI) on behalf of a covered entity or another business associate. PHI is defined in the HIPAA regulations, and, in general, is identifiable health information. So, most vendors or contractors (including subcontractors) that provide services to or perform functions for covered entities that involve access to PHI are business associates. For example, a company that is given access to PHI by a covered entity to provide and manage a personal health record or patient portal offered by the covered entity to its patients or enrollees is a business associate.

Note that the scenarios below address the application of HIPAA to the app developer. In all cases in which a covered entity is transmitting PHI, either itself or using a business associate, it must apply reasonable safeguards to protect the information and nothing in the analyses below relieves covered entities (e.g., providers) of their own, independent obligation to comply with HIPAA.

Health App Scenario 1

- Consumer downloads a diabetes health app to her smartphone and inputs blood glucose levels and blood pressure readings she obtained herself using home health equipment.

Is the app developer subject to HIPAA?

Health App Scenario 2

- As directed by her provider, patient downloads a health app to her smart phone. Provider has contracted with app developer for patient management services, including electronic health record (EHR) integration and application interfaces, and the information the patient inputs is automatically incorporated into the provider's EHR.

Is the app developer subject to HIPAA?

Health App Scenario 3

- Consumer downloads a health app to her smartphone that is designed to help her manage a chronic condition. She downloads data from her doctor's EHR through a patient portal onto her computer and then uploads it into the app. She also adds her own information to the app.

Is the app developer subject to HIPAA?

HHS ONC Study of Non-HIPAA-Regulated Entities

- HHS-ONC conducted a study in 2016 of HIPAA non-covered entities' health data collection
- Focused on data collection through mHealth technologies (smartphones, software applications, wearable sensors, etc.) and social media websites
- Study revealed that vast amounts of electronic health data are being collected and shared in a largely unregulated environment

HHS-ONC Findings of Concern

- Lack of encryption
- Other security measures often inadequate
- Individuals lack understanding of risk
- Privacy policies and notices are unclear; hard to find and understand
- Privacy policies change without notice
- Data collection, use and sharing for marketing is not limited

Regulators Other Than HHS

- Federal Trade Commission (FTC)
  - Section 5 of the FTC Act
  - HITECH Act data security breach notification requirements for certain entities not regulated under HIPAA
- Food & Drug Administration (FDA)
  - Regulates mobile medical devices (MMDs), including mobile medical applications
  - Has enforcement jurisdiction over the safety of MMDs
- States
  - Medical provider and insurer privacy laws
  - Data security breach laws

FTC Act Fundamentals

- Section 5 of the FTC 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

Deception and Unfairness

- Misrepresentation or deceptive omission in a privacy policy, user interface, or privacy setting, may constitute a deceptive trade practice under FTC Act § 5.

- Failure to provide reasonable security for personal information may constitute an unfair trade practice under FTC Act § 5.

FTC Act Enforcement

- **Henry Schein Practice Solutions, Inc.**
  - FTC alleged that provider of office management software for dental practices misrepresented that its software provided industry-standard encryption of sensitive patient information.
- **Practice Fusion**
  - FTC alleged that electronic health records provider misled consumers by failing to disclose adequately that physician reviews would be publicly posted.

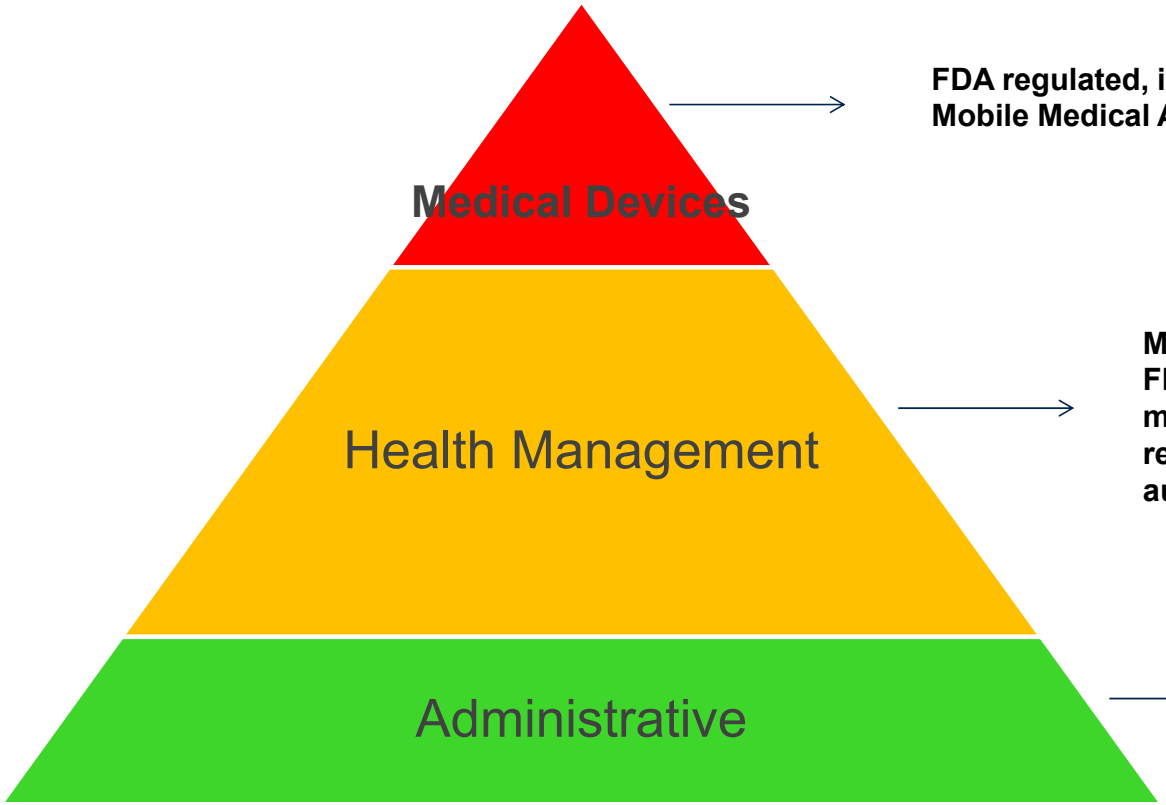
FTC Health Breach Notification Rule

- Vendors of personal health records (PHRs), PHR-related entities, and their service providers (if not HIPAA covered entities or business associates) must comply
- PHRs and PHR-related entities that suffer a breach must:
  - Notify everyone whose information was breached
  - In some cases, notify the media
  - Notify the FTC
- Service providers must notify their PHRs or PHR-related entities

FTC Guidance: *Mobile Health App Developers: FTC Best Practices* (2016)

- 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

How Does the FDA Regulate Health IT?

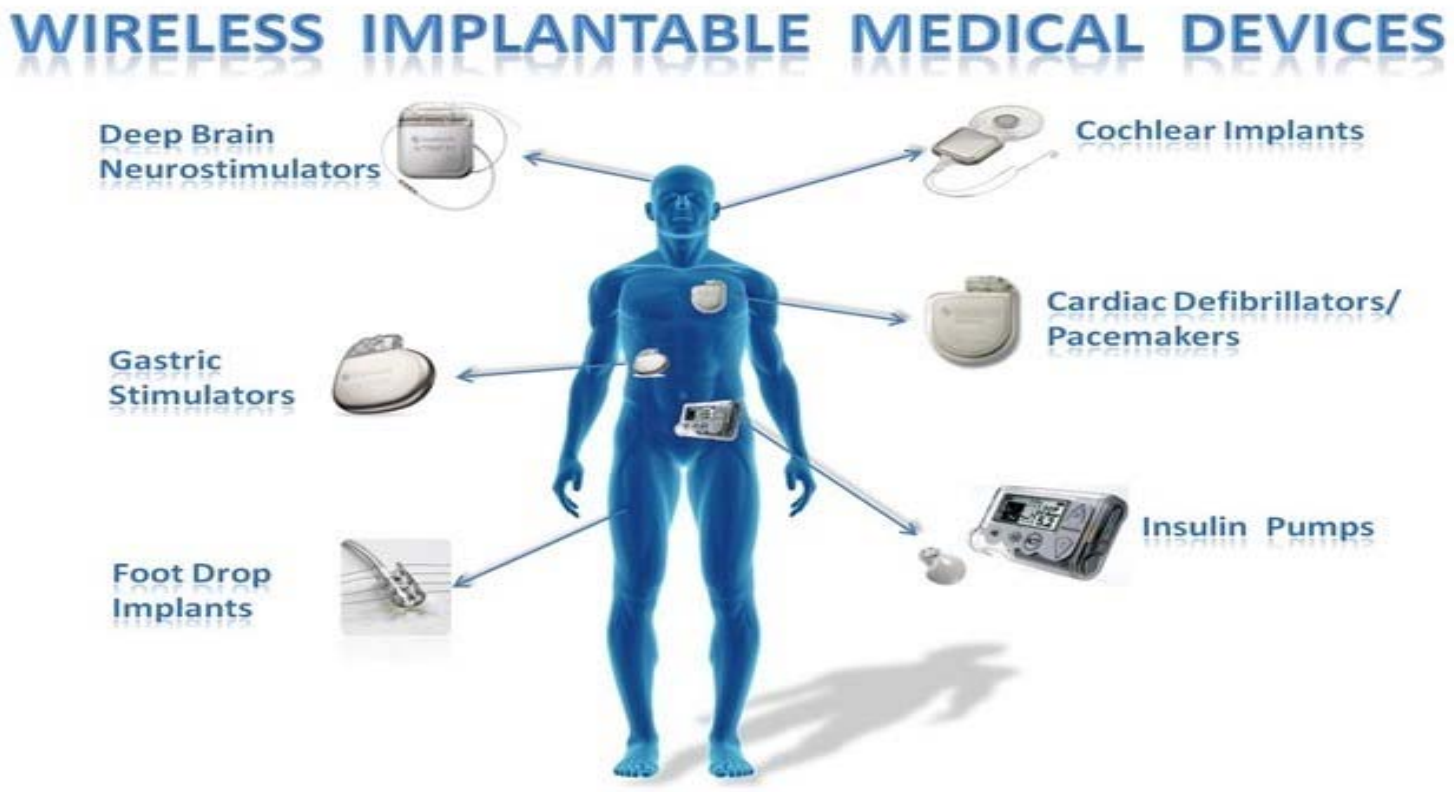


FDA regulated, including Mobile Medical Apps

Most are not regulated by FDA, but some could be medical devices or regulated by other authorities

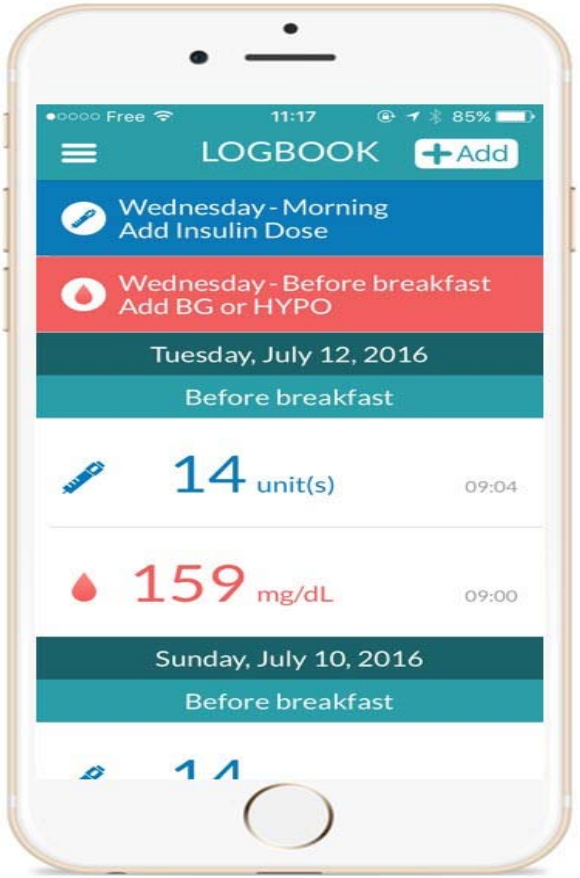
Not regulated by FDA and not medical devices

Cybersecurity



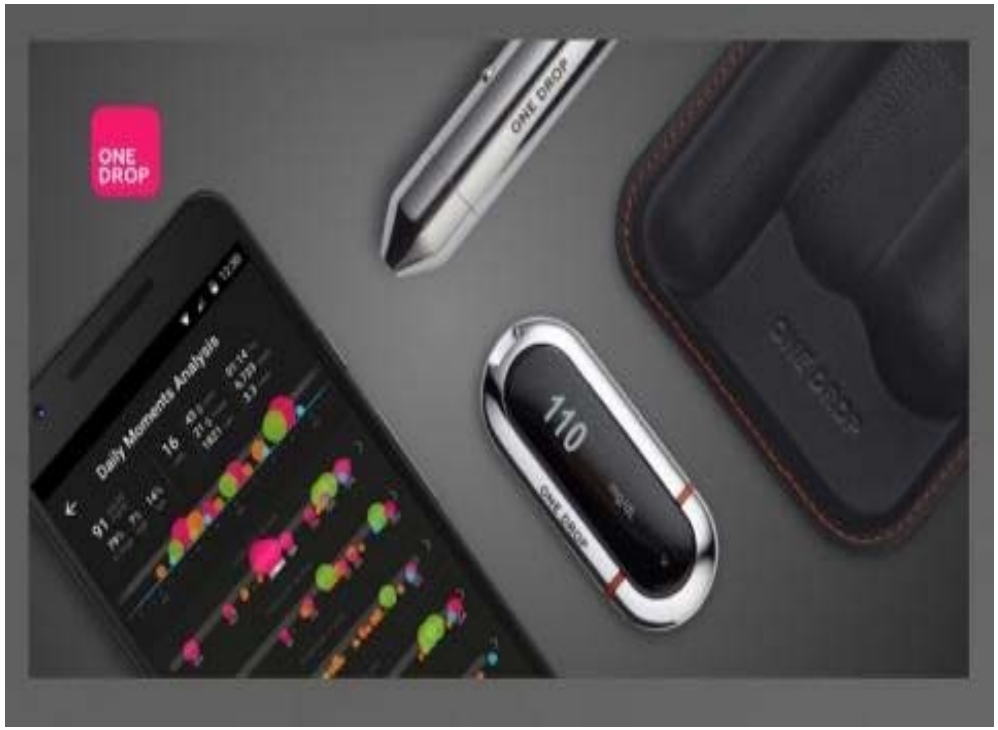
Medical Mobile App: Insulia

- Type 2 diabetes management app for people treated with basal insulin
- Classified as a prescription-only medical device
- Offers users dosage recommendations, educational coaching and diabetes-related data.
- Uses a dose-adjusting algorithm to help the user manage their diabetes
- Data is automatically shared with the patient's health care team



Medical Mobile App: One Drop

- Mobile blood glucose monitoring system
- Transmits blood glucose data directly to the cloud
- Offers a 24/7 certified diabetes educator coach for in-app chats
- Provides actionable insights to users based on their data



Example of MMA Security Vulnerability

- Vulnerabilities in certain Johnson & Johnson wireless insulin pumps put the devices at risk for hacking
- Exploitations could have caused delivery of an insulin overdose
- Wireless control unit enables patients to remotely command the dose of insulin, but the radio frequency communication path between wireless control unit and insulin pump was unencrypted
  - Johnson & Johnson sent notification letters to about 114,000 patients and physicians

Photo: Johnson & Johnson

FDA Guidance on Premarket Cybersecurity

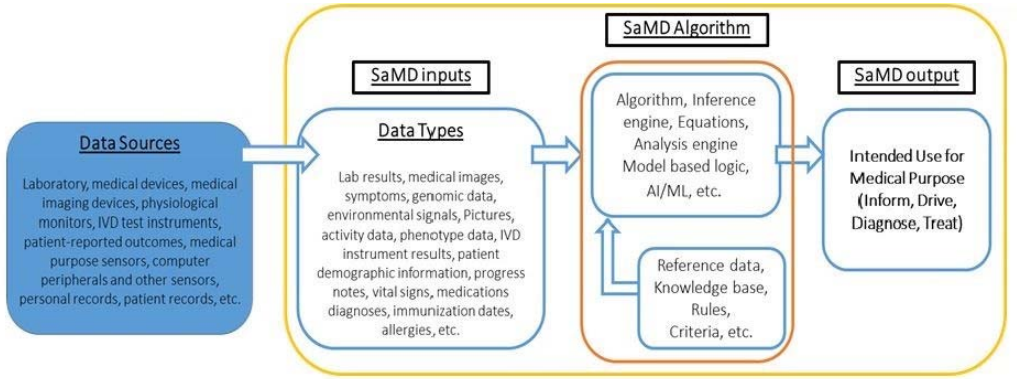
- Address cybersecurity at design/development stage:
  - Establish design inputs and cybersecurity vulnerability and management approach as part of software validation/risk analysis
  - Identify assets, threats, and vulnerabilities and their impact on device functionality and end users/patients
  - Assess likelihood of a threat and of a vulnerability being exploited
  - Determine risk levels and suitable mitigation strategies
- Extent of security controls may depend on:
  - Device's intended use
  - Presence and intent of electronic data interfaces
  - Intended environment of use (*e.g.*, patient, hospital, etc.)
  - Type of cybersecurity vulnerabilities present
  - Likelihood vulnerability will be exploited (intentionally/unintentionally)
  - Probable risk of patient harm due to cybersecurity breach

FDA Guidance on Postmarket Cybersecurity

- Outlines FDA's recommendations for monitoring, identifying, and addressing cybersecurity "vulnerabilities" and "exploits" in devices that have already entered the market
- Applicable to devices that contain software (including firmware) or programmable logic, as well as software that is a medical device
- For cybersecurity vulnerabilities and exploits that may compromise the "**essential clinical performance** of a device and present a reasonable probability of serious adverse health consequences of death," FDA requires notification to the agency under 21 CFR 806.10

FDA's Digital Health Innovation Action Plan

- Spearheaded by FDA's Center for Devices and Radiological Health
- Inaugurates new approach to approval of digital health products
- Provides for new guidance on:
  - medical software
  - clinical decision support software
  - multi-functionality
  - software modification approvals



Software Precertification Program: Working Model – Version 1.0 – January 2019

A New Approach to Regulation of Digital Health Software

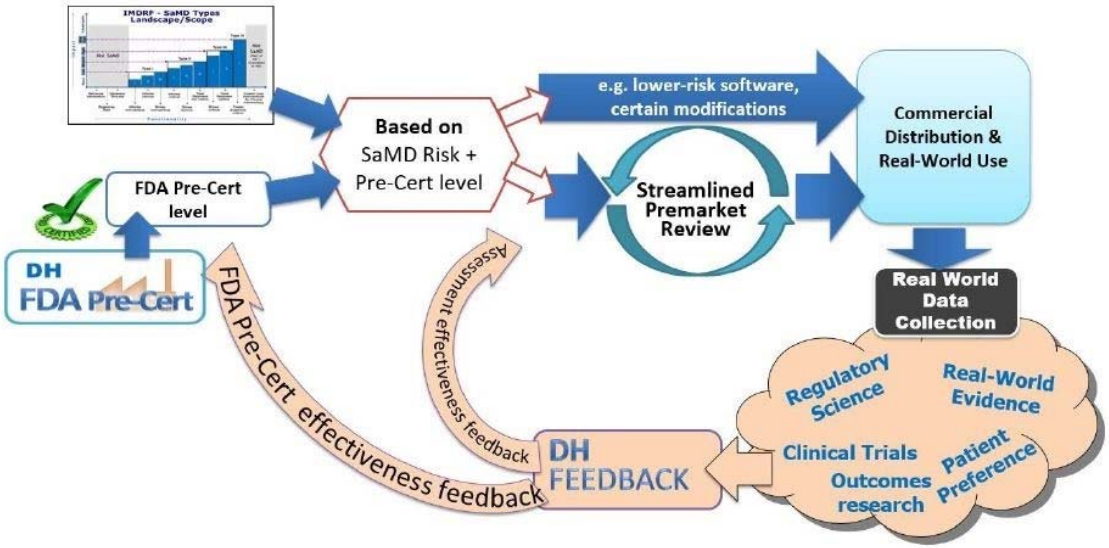


Figure 1. A reimagined approach for the regulation of software

Software Precertification Program: Working Model – Version 1.0 – January 2019

Digital Health Software Precertification Program

- Pilot program launched in July 2017 to test pre-certification of software for digital health products
- Focuses on developer quality and reliability rather than product capability
- Requires developers to demonstrate
  - Embedded culture of quality
  - Organizational excellence
- First pilot pre-certifications announced September 2017:
  - Apple, FitBit, Johnson & Johnson, Pear Therapeutics, Phosphorus, Roche, Samsung, Tidepool, Verily

HHS OCR Request for Information
December 2018

HIPAA Privacy Rule: Care Coordination Concerns

- OCR seeks information on whether the HIPAA Rules obstruct the ability of covered entities and business associates to conduct care coordination and/or case management.
- HIPAA covered health care providers may disclose PHI to a third party for the coordination or management of treatment, but some HIPAA covered entities are resistant to sharing this information for fear of violating HIPAA.
- Should OCR amend the Privacy Rule to encourage covered entities to share PHI with non-covered entities when needed to coordinate care and provide related health care services and support for individuals?

Would It Help to Require Certain PHI Disclosures to Non-HIPAA Covered Health Care Providers?

- Currently, HIPAA covered entities are permitted, but not required, to disclose PHI to a health care provider who is not covered by HIPAA (i.e., a health care provider that does not engage in electronic billing or other covered electronic transactions) for treatment and payment purposes of either the covered entity or the non-covered health care provider.
- Should a HIPAA covered entity be required to disclose PHI to a non-covered health care provider for these purposes?
- Would the benefits of such sharing outweigh the privacy risks?

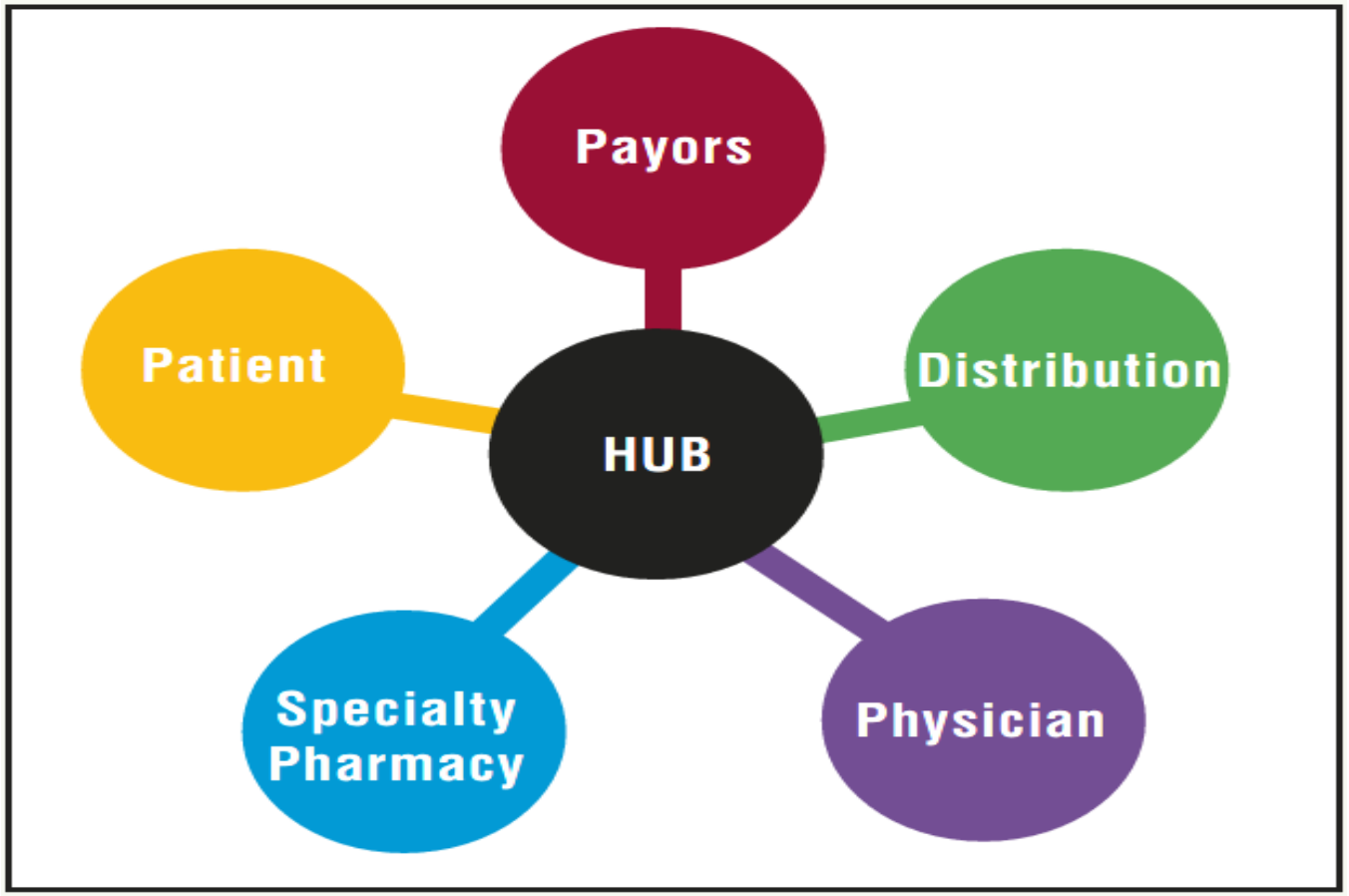
What Privacy Protections Should Apply to Disclosures to Non-HIPAA Covered Health Care Providers?

- Should a non-covered health care provider requesting PHI from a HIPAA covered entity provide a verbal or written assurance that the request is for an accepted purpose (e.g., TPO) before a potential disclosure requirement applies to the covered entity receiving the request?
- If so, what type of assurance would provide the most protection to individuals without imposing undue burdens on covered entities?
- Would a covered entity receiving the request want or need to set up a new administrative process to confirm the identity of the requester?
- How much would it cost covered entities to comply with this requirement?

What About Disclosures Beyond Health Care Providers?

- Should the Privacy Rule allow disclosures of PHI to non-covered entities who are not health care providers for care coordination purposes?
- What types of non-health care providers are key to care coordination and patient assistance?

Pharmaceutical HUB Services



Pharmacy *Today*, Jan. 2017, pg. 41

HUB Servicer Vendors (2017 data)

Hub service vendors (parent company)	
• Asembia	• OptumRx (United Health)
• AssistRx	• Opus Health (QuintilesIMS)
• CareMetx (Walgreens)	• P5 Connect
• CoPilot Provider Support Services (CareMed)	• Sonexus Health (Cardinal)
• Dohmen Life Science Services	• Therigy Specialty Therapy Management
• eMaxHealth	• TrialCard & TC Market Access
• EnvoyHealth (Diplomat)	• Triplefin (H. D. Smith)
• InVentiv Health (Xerox)	• UBC (Express Scripts)
• Lash Group (AmerisourceBergen)	• VirMedica
• Occam Health Services	• Vivaleas
• Omnicare Specialty Care Group (CVS)	• ZappRx

Pharmacy *Today*, Jan. 2017, pg. 41

What About Disclosures to Social Service and Community Support Organizations?

- Should OCR modify the Privacy Rule to encourage disclosures of PHI to social services agencies and community-based support programs to facilitate treatment and coordination of care?
- For example, if a disabled individual needs housing near a specific health care provider to facilitate their health care needs, to what extent should the Privacy Rule permit a covered entity to disclose PHI to an agency that arranges for such housing?
- Should this permission apply only where the social service agency itself provides health care products or services?
- In order to make such disclosures to social service agencies (or other organizations providing such social services), should covered entities be required to enter into agreements with such entities that contain provisions similar to the provisions in business associate agreements?

Questions?

Tina Olson Grande

Chair, Confidentiality Coalition
750 9th Street, NW, Suite 500
Washington, DC 20001

tgrande@hlc.org

www.confidentialitycoalition.org

Nancy L. Perkins

Arnold & Porter
601 Massachusetts Ave., NW
Washington, DC 20001

Nancy.Perkins@arnoldporter.com

www.arnoldporter.com