ARNOLD & PORTER KAYE SCHOLER

Medical Devices: Innovation and Regulation of Emerging Technologies

Mahnu V. Davar
Nancy L. Perkins
ARNOLD & PORTER KAYE SCHOLER LLP

New York State Bar Association
2018 Annual Meeting

apks.com

Topics We Will Cover Today

- Updates in FDA device and software regulation following the 21st Century Cures Act
- Practical guidance on when my software is regulated by FDA
- Data transfers as a treatment tool
- Privacy and security risks and regulation

Basic Principles of FDA Regulation

- The "objective intent" of the manufacturer or distributor of the product determines the regulatory status of the product
- Regulated products cannot be marketed without appropriate premarket approval or clearance unless they are exempt from such requirements
- Regulated products must be designed and manufactured to ensure safety and quality
- Manufacturers, importers, distributors, and certain product users ("user facilities") must comply with good manufacturing practices and quality system requirements
- Every entity and individual in the product marketing or supply chain has potential liability for statutory violations if they distribute or further the distribution of non-compliant products

What is a Medical Device?

- A medical device is an "instrument, apparatus, implement, machine, contrivance . . . or other similar or related article, including **any *component, part, or accessory***"
  - **intended for** use in the *diagnosis, treatment, cure*, or *prevention* of a *disease or condition*, or
  - **intended to** affect the *structure or function* of the body
  - which does not achieve its primary intended purposes through chemical action within or on the body of man or other animals and which is *not dependent upon being metabolized* for the achievement of its primary intended purposes
    - *See* 21 U.S.C. § 321(h)

21st Century Cures Act Sec. 3060 (Dec. 2016)

- Clarifies that the term "device" does not include a software function that is intended:

  (1) For administrative support of a healthcare facility (e.g., billing)

  (2) For general health maintenance

  (3) To serve as an electronic patient record system (e.g., EHRs)

  (4) For transferring, storing, converting clinical laboratory or other device data results (already subject to FDA enforcement discretion); or

  (5) To display medical information or to support healthcare providers in diagnosis/treatment decision-making (e.g., CDS), unless analyzes data on its own

What is a Product's Intended Use?

- Intended use refers to the "objective intent" of the persons legally responsible for marketing the product, and is shown by:
  - ***Labeling*** (*e.g.*, packaging, user manuals, medication guides, other information that is integral to a transaction or necessary to ensure safe use of the product)
  - ***Promotional Statements*** (*e.g.*, advertising, sponsorships, or other activities intended to raise awareness of a business or product, or surrounding content/graphics are important factors)
  - ***Other Statements Made By or On Behalf of the Marketer*** (*e.g.*, securities registration, patent filings, testimonials, oral statements by sales reps, depictions of conduct or use)
  - ***Actual Knowledge*** of the marketer as to end user intent; circumstances of marketing
    - *See* 21 C.F.R. § 801.4
- Preamble to Final Rule on Intended Uses, 82 Fed. Reg. 2193 (Jan. 9, 2017)
  - "FDA may take into account *any* claim or statement made by or behalf of a manufacturer that explicitly or implicitly promotes a product for a particular use."
  - Note: Implementation Final Rule is delayed and under review and likely revision.

Key Regulatory Controls for Medical Devices

- Based on risk classification I, II, or III
- Adulteration/misbranding prohibitions
- Labeling requirements
- Establishment registration and listing
- Premarket notification ("510(k)")
- Notifications/remedies (repair, recall, etc.)
- Records and reports (adverse events, tracking, removals/correction reports)
- Good Manufacturing Practices/Quality Systems
- Investigational Device Exemptions

Quality System Regulation (QSR)

- Companies that make and market medical devices must have a comprehensive system to ensure product safety and quality
  - *See* 21 C.F.R. Part 820 (medical device good manufacturing practices / quality system requirements)

- Key features of a QSR System:
  - ***Management Oversight and Review***
    - Employee Qualifications and Training
    - Audit Processes
    - Process Documentation
    - Communication Policies (*e.g.*, with FDA, customers, and management)
  - ***Standard Operating Procedures (SOPs)***
    - Design Controls
    - Purchasing Controls (*e.g.*, Supplier Qualifications, tracking and tracing)
    - Production and Process Controls
    - Nonconforming Products/"Corrections and Removals" and other Recalls
    - Corrective and Preventive Actions (CAPA)
    - Complaint Handling/MDRs
    - Labeling and Packaging Controls

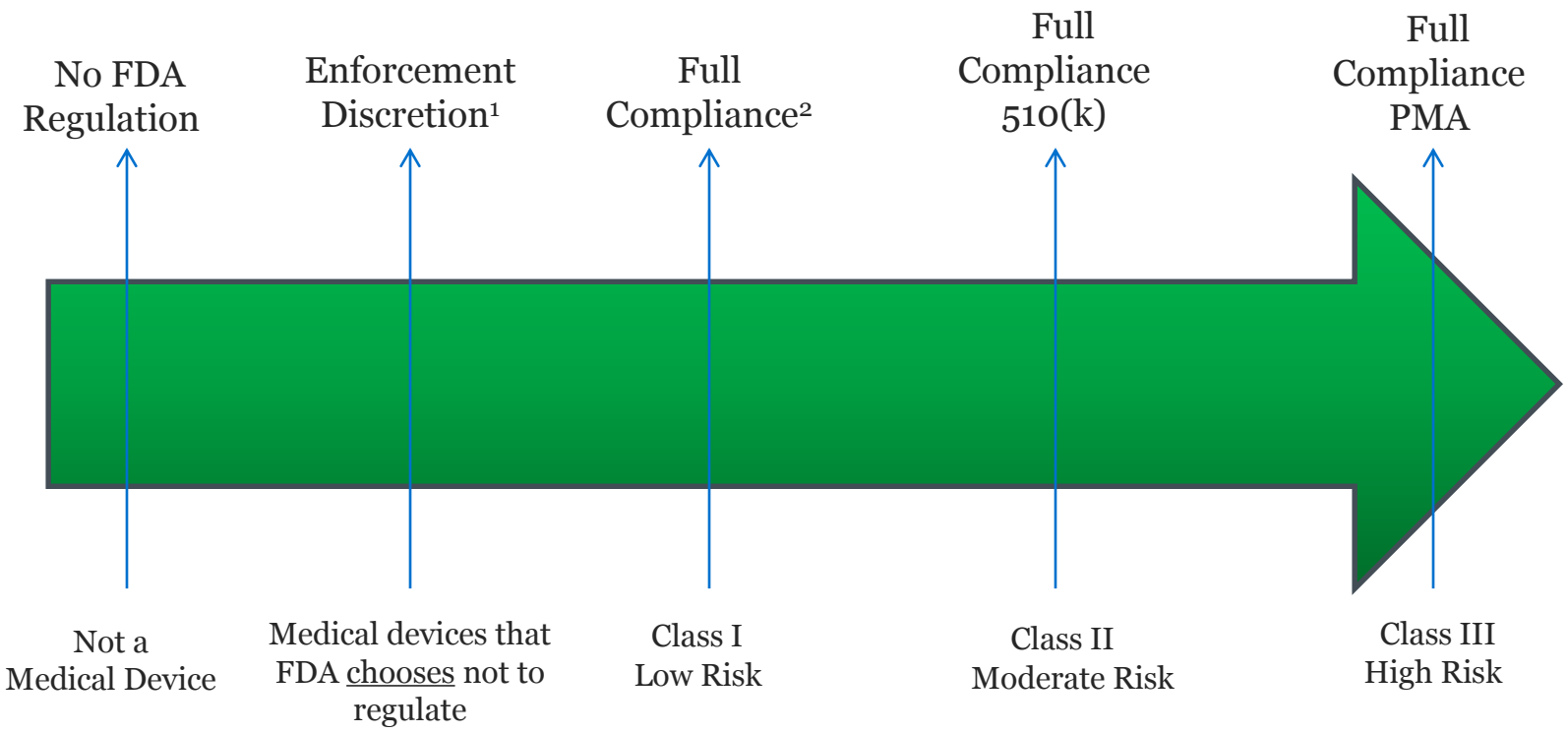
Important QSR Concepts

- Manufacturer (21 CFR 820.3(o))
  - "designs, manufactures, fabricates, assembles, or processes a finished device; includes but is not limited to those who perform the functions of contract sterilization, installation, relabeling, remanufacturing, repacking, or specification development, and initial distributors of foreign entities performing these functions"
- Design controls concepts (21 CFR 820.30)
  - Input, output, review, verification, validation, transfer
  - Specification design and development
  - Design changes and design history file (820.180 – 820.198)
- Production, process, acceptance, and release (21 CFR 820.70 & 820.80)
- Purchasing/supplier controls (21 CFR 820.50)

QSRs and Software

- Medical device software products are subject to **design control** provisions – *See* 21 C.F.R. 820.30
  - Validation is the most critical part of the QSR for software
  - Tasks supporting software validation:
    - Quality Planning
    - System Requirements Definition
    - Detailed Software Requirements Specification
    - Software Design Specification
    - Construction or Coding
    - Testing
    - Installation
    - Operation and Support
    - Maintenance
    - Retirement
- Software used to automate any part of the device production process or any part of the quality system must be **validated** for its intended use – *See* 21 C.F.R. 820.70(i)
  - In addition to software validation requirements above, software used as part of quality system is subject to additional security, data integrity, and validation requirements

FDA Regulatory Continuum



1. Enforcement discretion means that FDA has the discretion to decide not to enforce certain requirements for certain products. FDA may withdraw its "discretion" based on new information, safety issues, or other factors.

2. Unless otherwise exempt from certain requirements

Recent FDA Guidance

- December 7, 2017, FDA announced several digital health policy documents designed to "encourage innovation" and "bring efficiency and modernization" to the agency's regulation of digital health products
- Two draft and one final guidance which address, in part, the important changes made by Section 3060 of the Cures Act to the medical device provisions of the FDCA
- Dr. Gottlieb emphasized that these documents collectively "offer additional clarity about where the FDA sees its role in digital health, and importantly, where we don't see a need for FDA involvement "
- Comments on the drafts are due by Feb. 6, 2018

Draft CDS Guidance (Dec. 2017)

- Outlines FDA's approach to clinical decision support software (CDS)
- Intended to "make clear what types of CDS would no longer be defined as a medical device, and thus would not be regulated by" FDA
- FDA will "continue to enforce oversight of software programs that are intended to process or analyze medical images, signals from in vitro diagnostic devices or patterns acquired from a processor like an electrocardiogram that use analytical functionalities to make treatment recommendations, as these remain medical devices under the Cures Act."

Draft CDS Guidance (cont'd)

- To meet the exemption under the Cures Act, CDS software must meet all of the following criteria:

  (1) Not intended to acquire, process, or analyze a medical image or a signal from an in vitro diagnostic device or a pattern or signal from a signal acquisition system;

  (2) Intended for the purpose of displaying, analyzing, or printing medical information about a patient or other medical information (such as peer-reviewed clinical studies and clinical practice guidelines);

  (3) Intended for the purpose of supporting or providing recommendations to a health care professional about prevention, diagnosis, or treatment of a disease or condition; and

  (4) Intended for the purpose of enabling such health care professional to independently review the basis for such recommendations that such software presents so that it is not the intent that such health care professional rely primarily on any of such recommendations to make a clinical diagnosis or treatment decision regarding an individual patient.

Draft CDS Guidance (cont'd)

Examples of CDS software that meets the exemption:

- Software that uses rule-based tools that compare patient-specific signs, symptoms, or results with available practice guidelines (institutions-based or academic/clinical society-based) to recommend condition specific diagnostic tests, investigations or therapy, and provide options to users to obtain up-to-date information.
- Software intended for use by HCPs to aid in diagnosing patients suspected to have diabetes mellitus. The HCP enters patient parameters and laboratory test results (i.e., fasting plasma glucose, oral glucose tolerance test results, and/or hemoglobin A1c test results), and the device suggests whether the patient's condition meets the definition of diabetes based on established guidelines.

Examples of CDS software still subject to device regulation:

- Software that analyzes CT images to compute and/or approximate fractional flow reserve. In this case the software performs and provides the user an image analysis that the user could not independently derive.
- Software that analyzes a patient's laboratory results using a proprietary algorithm to recommend a specific radiation treatment, for which the basis of the recommendation is unavailable for the HCP to review.

Draft Guidance on Sec. 3060 of the Cures Act (Dec. 2017)

- In Dec. 2017, FDA also issued draft guidance entitled, "Changes to Existing Medical Software Policies Resulting from Section 3060 of the 21st Century Cures Act"
- Outlines FDA's interpretation of the types of software that are no longer considered medical devices (*e.g.*, lifestyle or wellness apps)
- Proposes changes to FDA's previously published guidance documents on General Wellness products and Mobile Medical Applications (MMA), among others, to "be consistent with the Cures Act and reflective of the agency's new, more modern approach to digital health products"
- Updates the categories of products for which FDA had already intended to exercise enforcement discretion due to their low risk and makes "an even clearer distinction, consistent with the Cures Act," that "many of these products no longer qualify as medical devices that would be subject to" FDA oversight"

Draft Cures Act Guidance (cont'd)

- In the Draft Guidance, FDA confirms its definition of general wellness products from prior guidance as those:
  - Intended for uses that relate to maintaining or encouraging a general state of heath or healthy activity, or
  - Intended for a use that relates the role of healthy lifestyle with helping to reduce the risk or impact of certain chronic diseases or conditions and where it is well understood and accepted that healthy lifestyle choices may play an important role in health outcomes for the disease or condition
- Such products are exempt from the definition of "device" if they
  - (1) are intended for only general wellness use; and
  - (2) present a low risk to the safety of users and other persons

  (*e.g.*, weight management, physical fitness software not related to diagnosis, cure, mitigation, or prevention of a disease or condition)

Draft Cures Act Guidance (cont'd)

- As noted, under the Cures Act, products "solely intended to transfer, store, convert formats, and display medical device data and results, including medical images, waveforms, signals, or other clinical information are not devices and thus are not subject to FDA regulatory requirements"
  - However, "software functions that analyze or interpret medical device data in addition to transferring, storing, converting formats, or displaying clinical laboratory test or other device data and results remain subject to FDA's regulatory oversight"
- The Draft Cures Act Guidance clarifies that this exclusion "does not capture software functions intended to generate alarms or alerts or prioritize multi-patient displays, because these functions involve analysis or interpretation of laboratory test or other device data and results"
  - For example, if a "software function is intended to prioritize patients in an Intensive Care Unit based on their clinical status, then this function is intended to interpret or analyze device data, results, and findings and is, therefore, not excluded from the definition of device"

Draft Cures Act Guidance (cont'd)

- The Draft Guidance notes that software functions that analyzes medical device data in order to "provide a notification or flag (*e.g.*, that a parameter is out of range)" are still subject to regulation
  - FDA will prioritize regulatory oversight on software functions "intended to generate alarms or alerts or prioritize multi-patient displays if they are intended to alert a caregiver to take an immediate clinical action"
  - Existing FDA guidance on MMAs and MDDS will be modified accordingly

Final Guidance on Software as Medical Device (Dec. 2017)

- Lastly, FDA finalized its October 2016 draft guidance entitled, "Software as Medical Device: Clinical Evaluation," which establishes common principles for regulators to use in evaluating the safety, effectiveness, and performance of Software as a Medical Device (SaMD)
- Specifically, the guidance sets forth a three-step clinical evaluation process for ongoing activities conducted in the assessment and analysis of SaMD's clinical safety, effectiveness, and performance as intended by manufacturers in the SaMD's definition statement
- The guidance emphasizes that the level of evaluation and independent review should be commensurate with the risk posed, and encourages manufacturers to use continuous monitoring to understand and modify software based on real-world performance

Final SaMD Guidance (cont'd)

- FDA has adopted the International Medical Device Regulators Forum (IMDRF) definition of SaMD: "software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device"
- SaMD ranges from software that allows a smartphone to view images obtained from MRI medical device for diagnostic purposes to software that is intended for diagnosis of a condition using the tri-axial accelerometer that operates on the embedded processor on a consumer digital camera.
- However, software that merely relies on data from a medical device, but does not have a medical purpose, or software that monitors performance or proper functioning of a device for the purpose of servicing the device, for example, do not meet the definition of SaMD

Is it a Medical Device?

- Does the product affect the structure or function of the body?
- Is it intended for use in the diagnosis, treatment, cure, or prevention of a disease or condition?
- Will the device perform an essential clinical function or require/prompt an immediate clinical action?
- Or does it meet the carve-outs for general wellness products, electronic health records, or clinical decision support?
- Will the product be marketed towards patients directly, or will it be marketed and used by licensed healthcare providers?
- Is the product in a category of products that FDA currently or historically has regulated as medical devices?

Is It a Medical Device? (cont'd)

IBM's Watson - Not a medical device

- For oncology, "Watson provides clinicians with evidence-based treatment options based on expert training by MSK physicians." Source: http://www.ibm.com/watson/health/oncology/
- Analyzes patient's medical record, identifies potential evidence-based treatment options, finds and provides supporting evidence from medical journals, textbooks, and other research

Biogaming's YuGo - 510(k) cleared device (unclassified)

- Indications for use: "A software system used with the Microsoft Kinect intended to be used to support the physical rehabilitation of adults in the clinic/at home. The system includes rehabilitation exercises for the lower and upper extremities with audio-visual feedback & graphic movement representations for patients as well as remotely accessible patient performance metrics for the medical professional." Source: K151955 Summary, http://www.accessdata.fda.gov/cdrh_docs/pdf15/K151955.pdf

Is It a Medical Device? (cont'd)

LifeWatch's ECG Mini System Continuous ECG Monitor **- 510(k) cleared device (Class II)**

- Continuously monitors patient ECG, automatically generates an alarm triggered by an arrhythmia detection algorithm, and transmits the recorded data transtelephonically to a monitoring center. Source: K151269 Summary, http://www.accessdata.fda.gov/cdrh_docs/pdf15/K151269.pdf

Biotricity's Bioflux Software **- 510(k) cleared device (Class II)**

- Indications for use: "Bioflux software is intended to be used to analyze, view, and report ECG data acquired from a variety of ECG sources including single and 3-lead ECG devices. Bioflux software is operated locally in a browser and data is accessed via the users' credentials on the hardware platform running the browser." Source: K162571 Summary, http://www.accessdata.fda.gov/cdrh_docs/pdf16/k162571.pdf

Related Legal Considerations

- Promotion/marketing claims
- Product liability
- Fraud and abuse compliance
- Reimbursement
- Privacy and data security…

Privacy and Security Risks and Regulations

- HIPAA Regulations: Scope and Content
- FTC Guidance and Enforcement
- FDA Jurisdiction and Security Guidance

Key Regulators

- Department of Health and Human Services (HHS)
  - Data privacy and security regulations under Health Insurance Portability and Accountability Act (HIPAA)
  - Data breach notification requirements under Health Information Technology for Economic and Clinical Health (HITECH) Act
- 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

Interagency Mobile Health Apps Compliance Tool

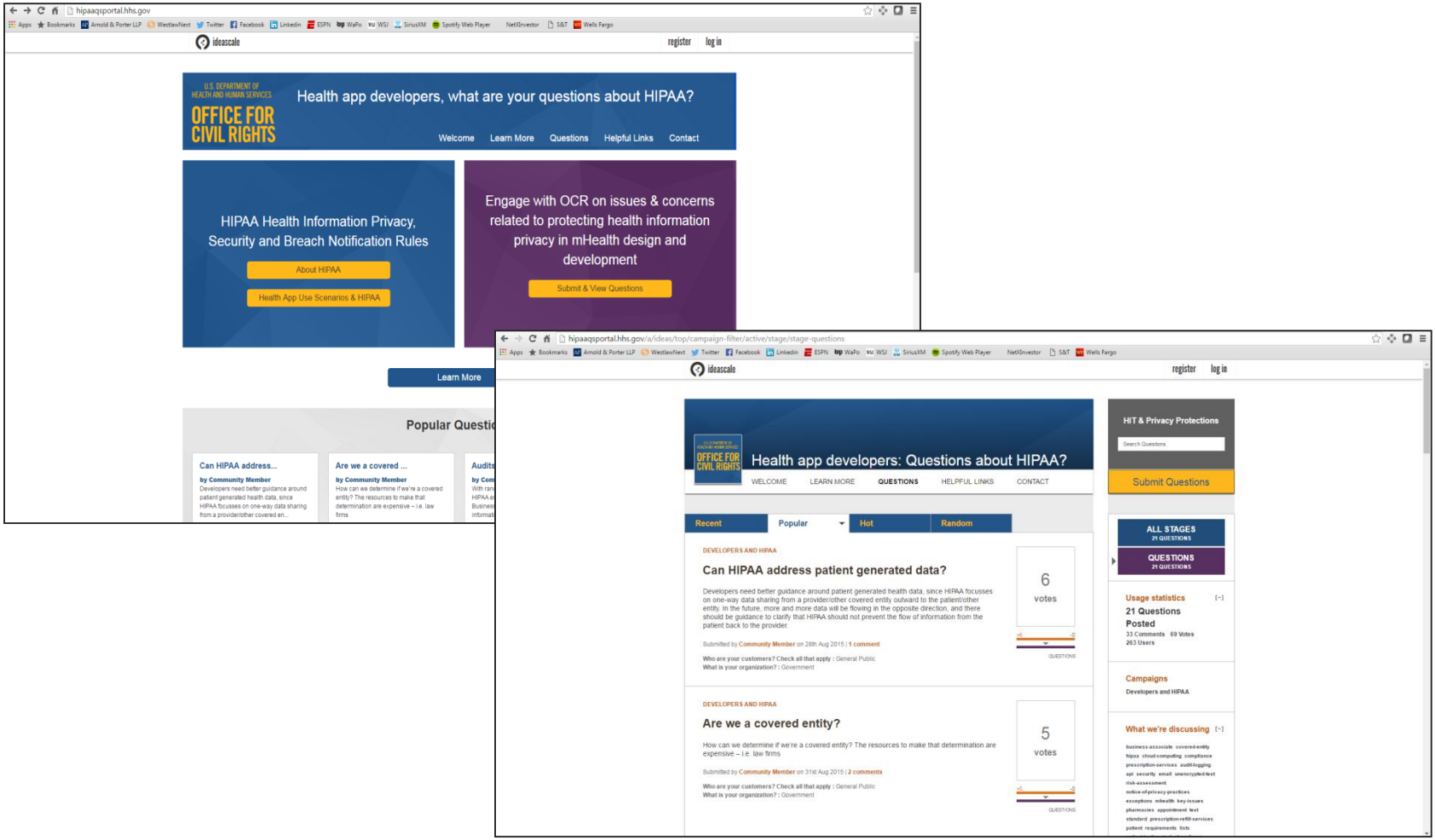
HHS Jurisdiction

- Regulated entities:
  - health care providers and health plans ("covered entities")
  - "business associates" of covered entities
- Regulated information: "protected health information" (PHI), *i.e.*, information in any form that:
  - Is created, received, or maintained by a covered entity,
  - Identifies or reasonably could be used to identify an individual, and
  - Relates to a past, present, or future health condition or the provision of, or payment for, health care.

HHS and Mobile Health Technologies

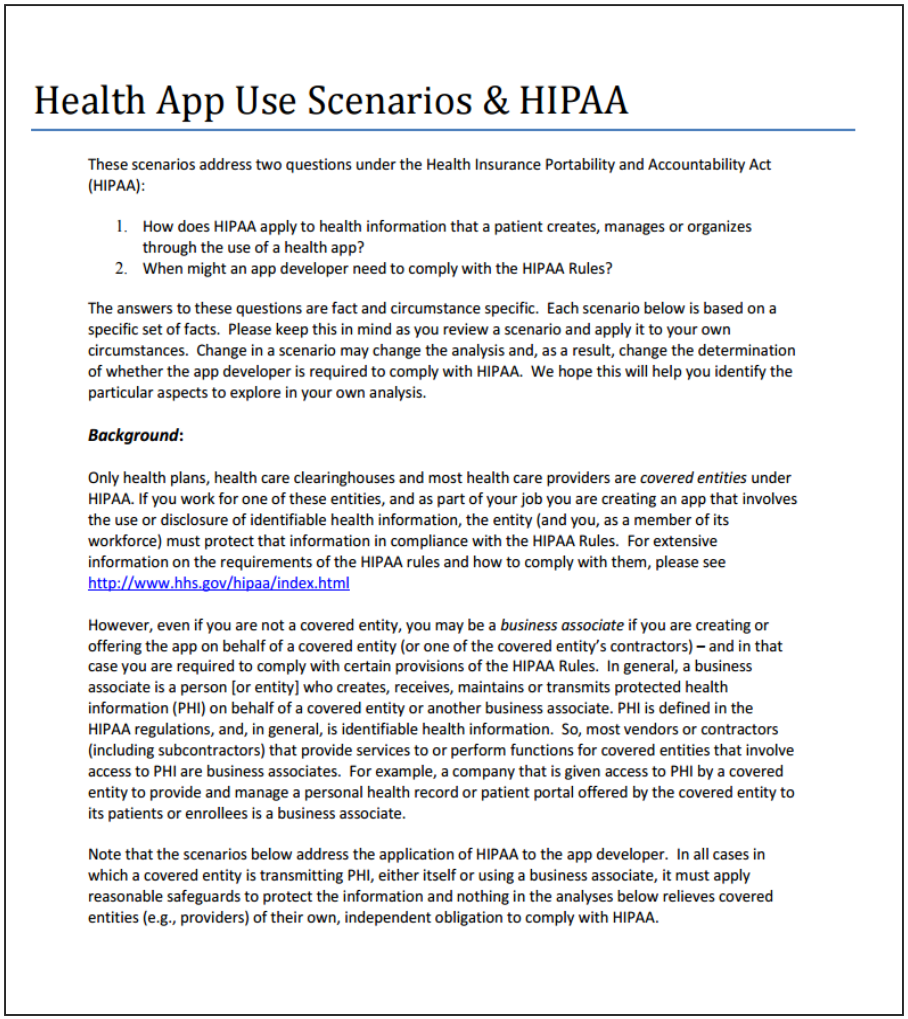
- Use and disclosure of PHI via mobile health ("mHealth") technologies offered by covered entities or business associates must comply with the HIPAA and HITECH Act rules
- In 2015, HHS Office of Civil Rights (OCR) created a developer portal to provide guidance on the application of the HIPAA rules to new health technologies

HHS Web Portal for Mobile App Developers



HHS Guidance

- In February 2016, HHS-OCR published additional guidance with 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?

Liability Risks: HHS Penalties

Extent of Intent	Minimum	Maximum
Person did not know (and by exercising reasonable diligence would not have known) that conduct violated HIPAA	$100 per violation, with an annual maximum of $25,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
Violation due to reasonable cause – not to willful neglect	$1,000 per violation, with an annual maximum of $100,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
Violation due to willful neglect, but is corrected within 30 days	$10,000 per violation, with an annual maximum of $250,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
Violation is due to willful neglect and is not timely corrected	$50,000 per violation, with an annual maximum of $1.5 million	$50,000 per violation, with an annual maximum of $1.5 million

Non-HIPAA-Regulated Entities

- HHS-ONC conducted a study 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

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

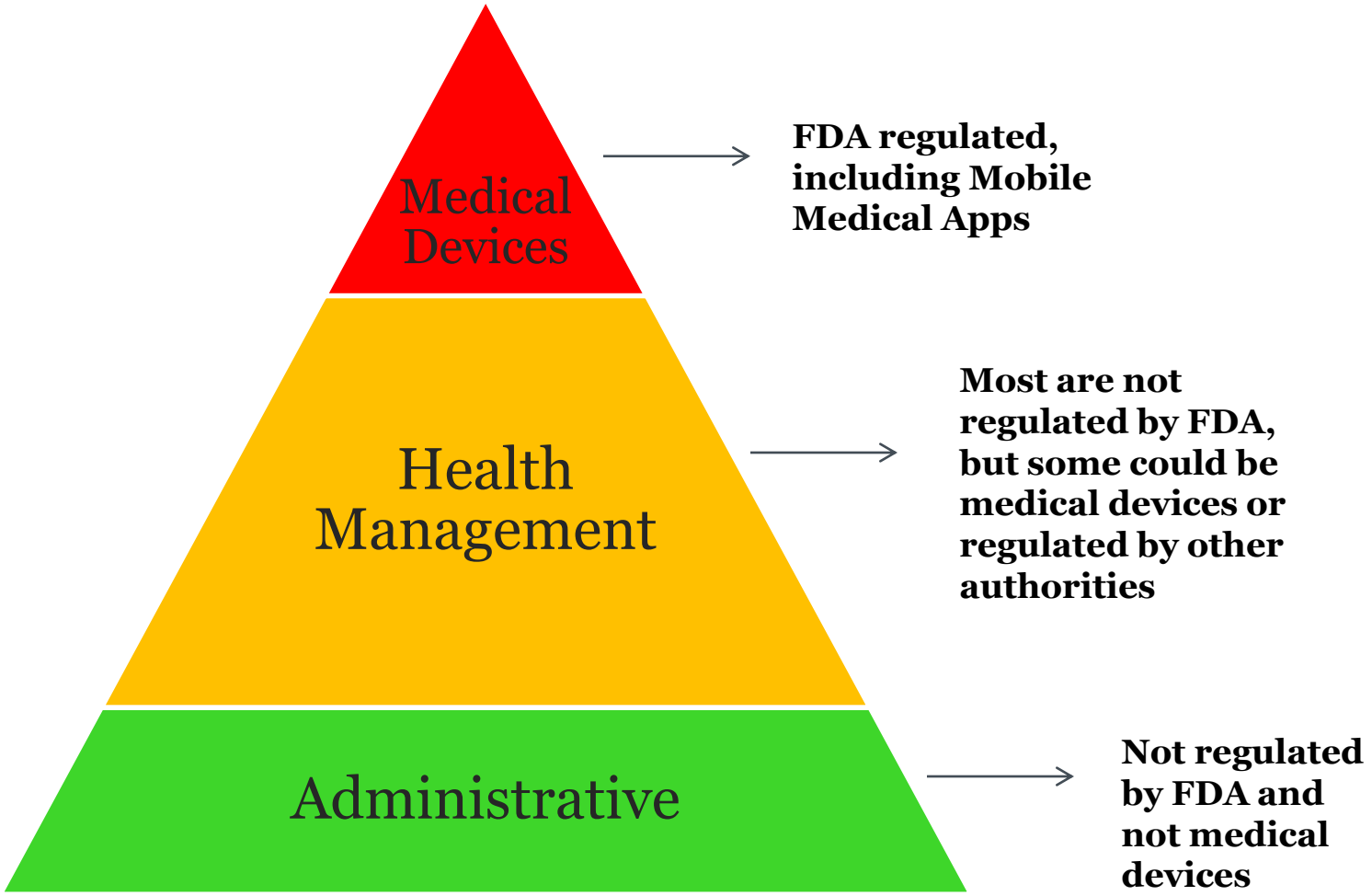
- **Henry Schein Practice Solutions, Inc.**
  - FTC alleged that provider of office management software for dental practices misrepresented that its software provided industry-standard encryption of sensitive patient information.

- **Practice Fusion**
  - FTC alleged that electronic health records provider misled consumers by failing to disclose adequately that physician reviews would be publicly posted.

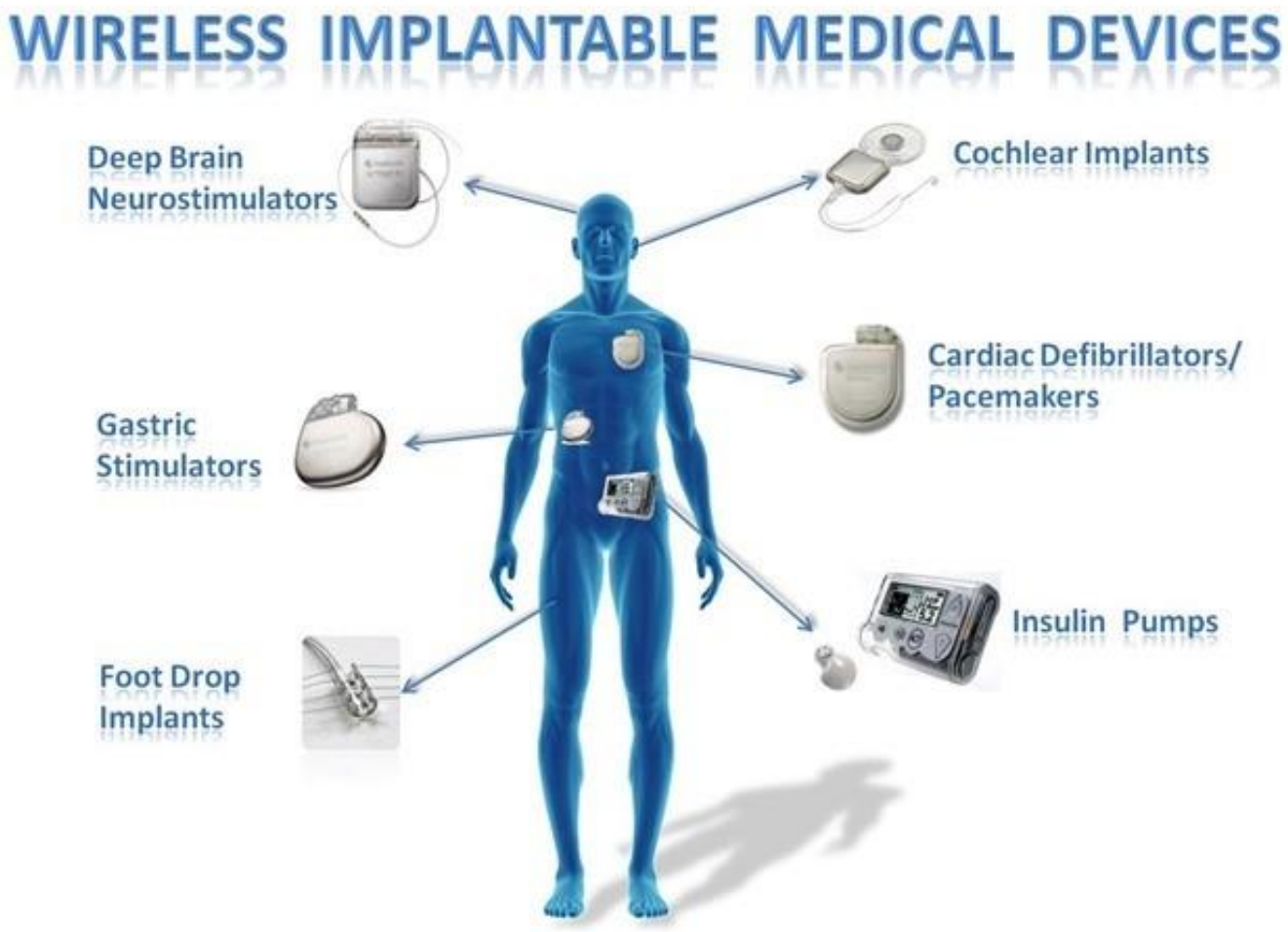
FTC Guidance: *Mobile Health App Developers: FTC Best Practices* (2016)

- 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?

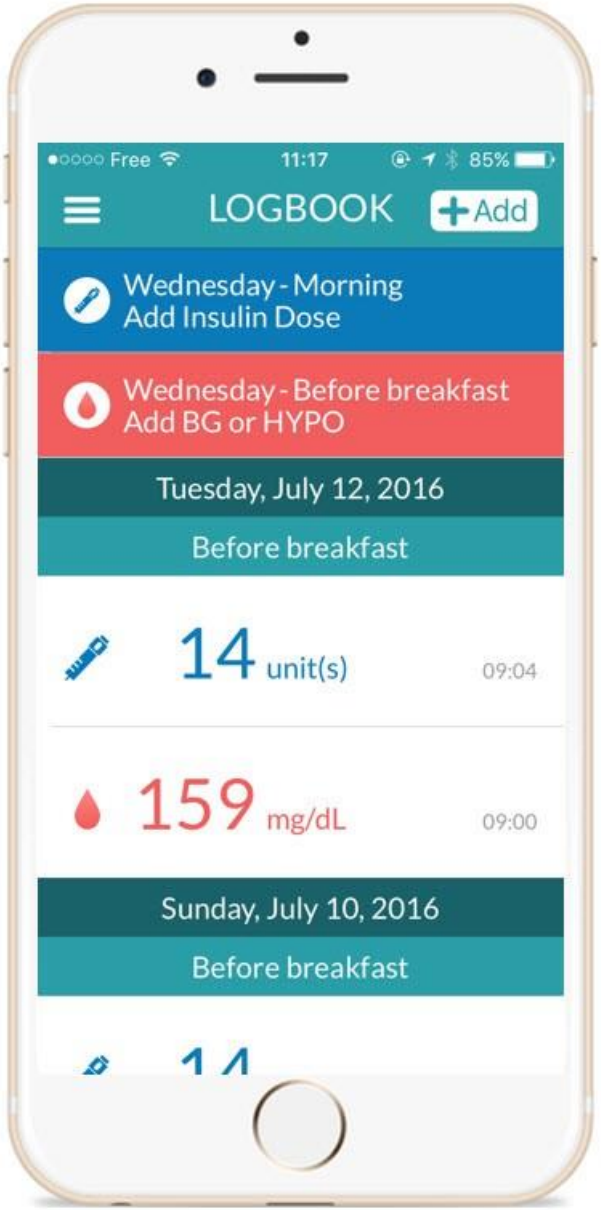


Cybersecurity



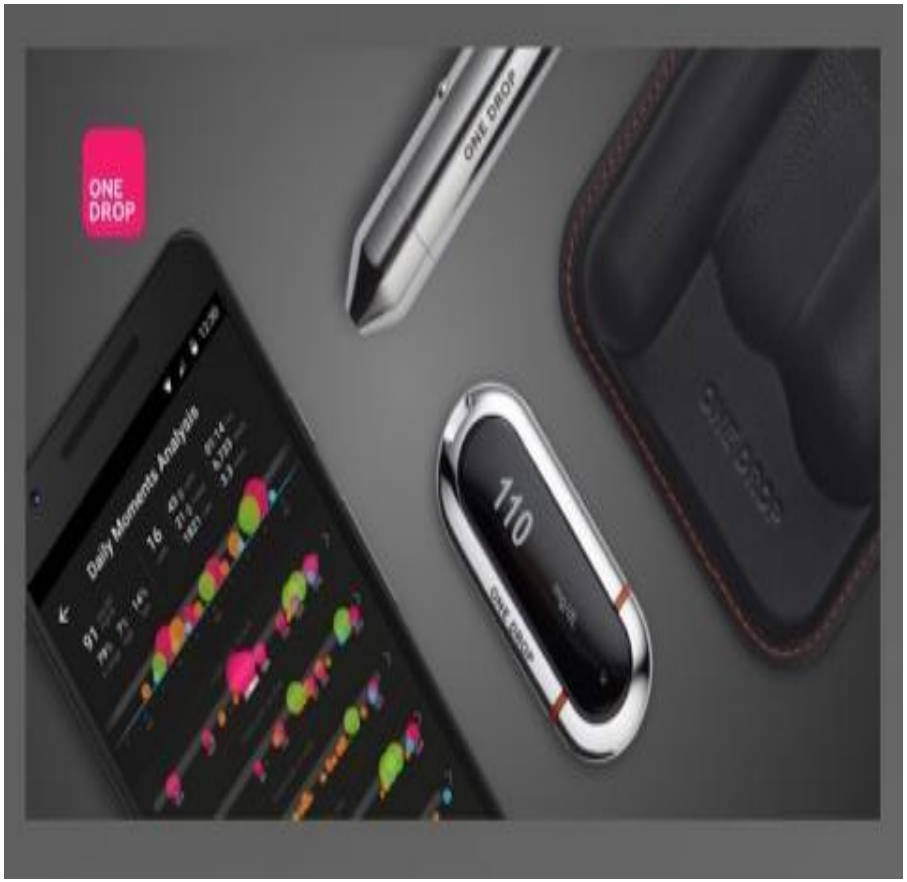
FDA-Approved MMA: Insulia

- 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



FDA-Approved MMA: 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 Guidance on Medical Device Interoperability

- Guidance released in September 2017 on electronic information interchange among interoperable medical devices
- Outlines design considerations, such as:
  - Anticipated users
  - Risk of others connecting to electronic interface
  - Labeling to ensure users connect for intended purposes
  - Verification and validation
- Provides recommendations for contents of pre-market submissions

FDA's Digital Health Innovation Action Plan

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

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

Questions?

Mahnu Davar
Mahnu.Davar@apks.com

Nancy Perkins
Nancy.Perkins@apks.com