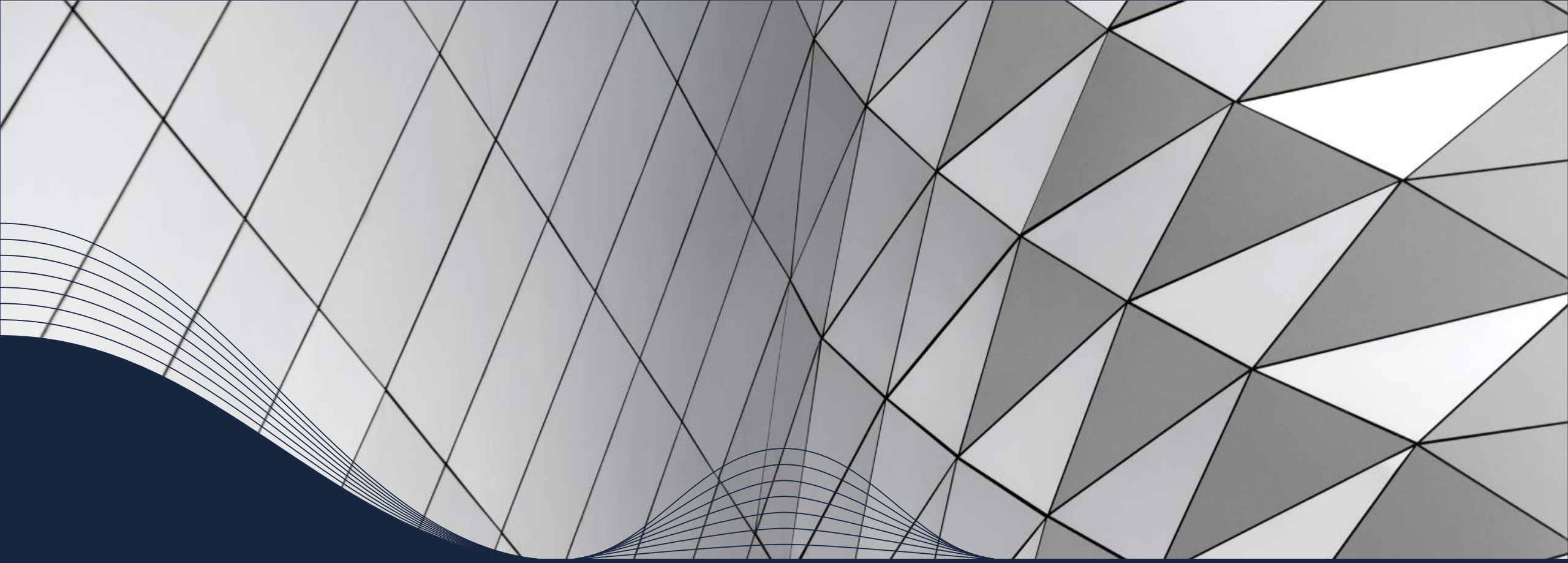


Digital Health:
How the Healthcare Industry and Related Technologies Are Making Use of Patient Data, and the Resulting Benefits and Risks

DLA PIPER

Presenters

Kristi V. Kung
Kristi.Kung@us.dlapiper.com
(703) 773-4290

Tracy Shapiro
Tracy.Shapiro@us.dlapiper.com
(415) 836-2545

Rebecca Jones McKnight
Rebecca.McKnight@us.dlapiper.com
(512) 457-7225

Nicole Greene
Nicole.Greene@dexcom.com
(858) 203-6445

What Is Digital Health?

- **Digital Health**: the convergence of digital and genomic technologies with health, healthcare, living, and society to enhance the efficiency of healthcare delivery and make devices/medicines more personalized and precise. Includes:
  - Hardware (computers, A/V equipment, sensors, wearables)
  - Software (algorithms, web-based analysis)
  - Services (telemedicine, store and forward, remote patient monitoring, digital therapeutics, augmented reality, virtual reality, etc.)

- "The broad scope of digital health includes categories such as mobile health (mHealth), health information technology (IT), wearable devices, telehealth and telemedicine, and personalized medicine." - FDA

2018-2019

HHS Secretary: Value-Based Care

- "Giving consumers greater control over health information through interoperable and accessible HIT."
- Price transparency

CMS

- MyHealthEData Initiative
- Medicare's new Blue Button 2.0
- Meaningful Use is Promoting Interoperability
- New Remote Patient Monitoring Codes

FDA

- Digital Health Innovation Action Plan
- Medical software pre-certification program
- Establishing a new incubator focused on health technology
- Encourage the use of AI in medicine and drug development

Digital Health is a Key Component to Value Based Care Success

Patient Engagement

Data Analytics

Population Health / Personalized Medicine

Overview of Regulatory Environment

Various government agencies have asserted jurisdiction over digital health

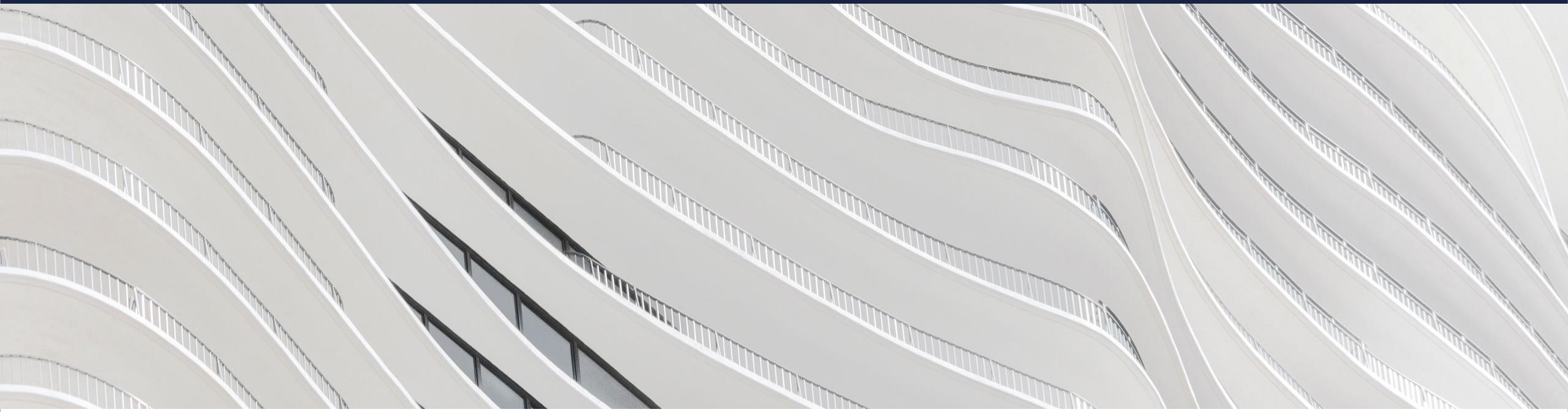
- Food and Drug Administration (“FDA”)
- U.S. Department of Health and Human Services (“HHS”)
- Federal Trade Commission (“FTC”)
- Federal Communications Commission (“FCC”)
- Office of the National Coordinator for Health Information Technology (“ONC”)
- State laws (e.g., California Consumer Protection Act)
- International Laws (e.g., General Data Protection Regulation)

Agenda

Key Takeaways

- When HIPAA Applies in Digital Health
- How CCPA and IOT Security Law Impacts Connected Health Devices
- Considering FDA Compliance During Digital Health Patient Engagements
- How FDA Views Real-World Data to Create Real-World Evidence in Decision-Making
- Applying State Laws When Using Patient Data During Remote Assessment and Treatment

When HIPAA Applies in Digital Health



HIPAA Overview

U.S. Department of Health and Human Services ("HHS")

- **Who is a <u>Covered Entity</u>?**
  - Health care providers (e.g., physicians, nurses, hospitals, laboratories, etc.) who engage in electronic standard transactions
  - Health plans (e.g., health insurance companies)
  - Healthcare clearinghouses (e.g., processors of non-standard health care data into standard format)
- **Who is a <u>Business Associate</u>?**
  - An entity that creates or receives "protected health information" on a covered entity's behalf
- **What is <u>Protected Health Information</u> ("PHI")?**
  - PHI is any information created or received by a health care provider, health plan, employer or health care clearinghouse relating to an individual's past, present or future health care or payment for health care and that *identifies the individual or could be used to identify the individual.*

HIPAA and Mobile Applications

- HIPAA may or may not apply to mobile health apps.
- In order to determine whether HIPAA is applicable:
  - Which entity created the app?
    - Is it a Covered Entity?
    - Is it a Business Associate?
  - What information will the application collect about its users?

HIPAA Privacy Rule

- Standard: **Minimum Necessary** (45 C.F.R. 164.502(b), 164.514(d))
  - Must make reasonable efforts to limit PHI to minimum necessary to accomplish the intended purpose of the use/disclosure.
- The Minimum Necessary Standard **does not apply** to:
  - Disclosures to or requests by a health care provider for treatment purposes.
  - Disclosures to the individual who is the subject of the information.
  - Uses or disclosures made pursuant to an individual's authorization.
  - Uses or disclosures required for compliance with HIPAA Administrative Simplification Rules.
  - Disclosures to HHS when disclosure of information is required under the Privacy Rule for enforcement purposes.
  - Uses or disclosures that are otherwise required by law.

Sale of PHI

- Prohibition on selling PHI, unless you have ***authorization***

- ***Sale*** means: Covered Entity or Business Associate directly or indirectly receives remuneration from or on behalf of the recipient of the protected health information in exchange for the protected health information
  - Sale of PHI includes a transfer of ownership of the PHI, as well as disclosures of PHI based on an access, license, or lease agreement

- Any authorization for a sale of PHI must state that the sale will result in ***remuneration***
  - If the third party is subject to HIPAA as a covered entity or business associate, then there must be an authorization or an exception to the sale of PHI.

Authorization (45 CFR 164.508)

- **What do you need in an Authorization?**
  - Make clear individual has right to revoke
  - To what extent treatment, payment, enrollment or eligibility for benefits is conditioned on the authorization
  - Potential for re-disclosure
  - If the authorization is for the sale of PHI, must disclose that the entity will be receiving remuneration

- Must be in plain language

- If the Covered Entity seeks the authorization, then must provide a copy of the signed authorization

De-Identification of PHI

- A covered entity can use a Business Associate to de-identify PHI on its behalf only to the extent such activity is authorized by their BAA.
- De-identification Methods:
  - **Expert Determinations**
    - Apply statistical or scientific principles
    - Very small risk that the recipient could identify individual
  - **Safe Harbor**
    - Removal of 18 types of identifiers
    - No actual knowledge residual information can identify individual
- ***Note:*** *Disclosure of a code (or other means) that enables de-identified information to be re-identified is considered a disclosure of PHI.*

What Types of Information Constitute PHI?

Removal of all 18 identifiers is required to satisfy the HIPAA De-Identification Safe Harbor

1. Name
2. Address
3. All elements of dates except year (and all ages over 89)
4. Phone number
5. Fax number
6. Email address
7. URL address
8. IP address
9. Social Security number
10. Account numbers
11. License numbers
12. Medical record number
13. Health plan member
14. Device identifiers/serial numbers
15. Vehicle identifiers/serial numbers
16. Biometric identifiers (finger and voice prints)
17. Full face photos and other comparable images
18. Any other unique identifying number, code or characteristic

“Any other Unique Identifying number, characteristic, or code”

- Identifying Number
  - E.g., clinical trial record numbers
- Identifying Code
  - Corresponds to a value that is derived from a non-secure encoding mechanism
  - E.g., code derived from a secure hash function without a secret key
    - Resulting value would be susceptible to compromise by the recipient of such data
  - E.g., embedded barcodes into patient records and medications
    - Unique for each patient or event in a patient’s record; can be easily applied for tracking purposes
- Identifying Characteristic:
  - Anything that distinguishes an individual and allows for identification
  - E.g., occupation of a patient (current President of State University)
- ***Note****: A data set that lists parts or derivatives of listed identifiers (e.g., contains patient initials, or last 4 digits of a social security number), would not meet the requirements of the Safe Harbor Method.*

2012 HHS De-identification Guidance

- In order to meet the Safe Harbor Method, all 18 identifiers of PHI must be removed, including:
  - All elements of dates (except year) for dates directly related to an individual, including but not limited to:
    - birth date,
    - admission date,
    - discharge date,
    - date of death; and
  - All ages over 89 and all elements of years (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of “age 90 or older”

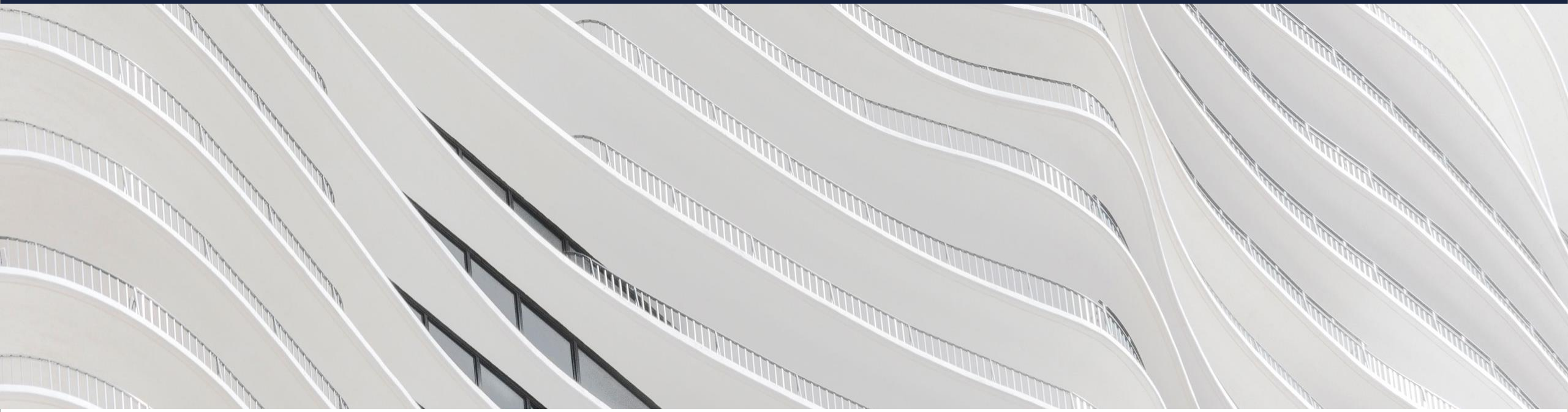
De-Identification Do's and Don'ts

- DO:
  - Remove all 18 identifiers of the individual or of relatives, employers, or household members of the individual
  - Ensure that there is no actual knowledge that the information could be used alone or in combination with other information to identify an individual
  - Obtain appropriate internal reviews and approvals prior to disclosing de-identified data
  - Document the values in health data that correspond to PHI, as well as the systems that manage PHI
- DO NOT:
  - Include ages over the age of 89, except if recorded as "90 or above"
  - Include dates more specific than the year of the event
  - Include parts or derivatives of any identifiers under safe harbor method (e.g., initials, last four digits of SSN)
  - Include identifiers that are in "free text fields"
  - Include information on rare clinical events that could lead to identification
  - Include unique identifying numbers, characteristics, or codes (e.g., barcode, clinical trial number)

De-Identification Moving Forward

- No additional de-identification guidance since 2012. In 2017, the National Committee on Vital and Health Statistics has provided HHS Secretary recommendations and asked for additional clarifications, including:
  - define the minimal skills and competencies to be considered an “expert” capable of de-identifying data under the Expert Determination Method, and
  - provide more sub-regulatory guidance on the Privacy Rule.
- Recognizes drive to create longitudinal databases
  - Database that tracks patients’ PHI over time, linking their clinical paths and treatments to socioeconomic, lifestyle, and employment data.
  - Does the merging of de-identified data sets to create longitudinal databases change the re-identification risk assessment of disclosing PHI?

How CCPA and IOT Security Law Impacts Connected Health Devices



What is the CCPA and why is it a big deal?

California Consumer Privacy Act

- **Game-changing new privacy law** broadly applicable to **businesses** (regardless of location) that collect **personal information** about California residents
- **Substantial new rights** for CA residents
- **Significant operational impacts** for covered business, likely require significant time and effort to prepare
- **High potential fines** for privacy violations
- Potentially **massive class action liability** for data breaches
- **Broad definitions and scope**
- **Effective January 1, 2020** (further amendments expected and the CA Attorney General is to issue implementing regulations)
  - Privacy provisions enforceable by CA AG **sometime between January 1, 2020 and July 1, 2020**
  - Data breach private right of action available from **January 1, 2020**

CCPA Scope – covered businesses and exemptions

- "**Business**" is any entity that **collects personal information** about California residents and **makes decisions** (alone or jointly with others) about how and why the personal information is processed, **if the business either** –

  (a) has ***annual gross revenues over $25 million*** **OR**

  (b) annually buys, sells, shares, or ***receives personal information of 50,000+ consumers*****, OR**

  (c) derives 50% or more of annual revenue from selling personal information

- Also includes parents or subsidiaries (with common branding) of businesses that meet the above
- **Non-profit entities** are not covered
- **Limited exemptions for certain regulated entities**
  - Partial exemption for entities and information covered by certain sector-specific laws - CCPA does not apply to certain information regulated under HIPAA/HITECH or California Medical Information Act

Sweeping Definitions

- **Personal information**: **“Any information that directly or indirectly identifies, relates to, describes or can be associated with or reasonably linked to a California resident or household” —** explicitly includes, to the extent they meet the above definition:
  - Name, contact info, government IDs, account numbers
  - Biometrics, location data, audio data
  - Employment and education history
  - Purchase history, behavior, and tendencies
  - Online and device IDs
  - Search and browsing history and other activities online or from connected devices
  - Inferences drawn from any personal info to create a consumer profile
- Applies to **consumer, employee, and B2B data** currently
- Includes **household level** data and **device** data
- **Narrow exclusion for publicly available data *from government records***

Key Components – New Consumer Rights

Individuals have rights to —

- **Access and obtain copy** of personal info collected in past 12 months
- **Learn how a business has handled the individual's personal information in the preceding 12 months:**
  - Categories of personal info collected
  - Sources of personal information (by category)
  - Purposes of collection, use, disclosure and sale
  - Categories of personal information sold and disclosed
  - Categories of third parties to whom personal info has been sold/disclosed
- **Requests may be made up to 2xs/year, free of charge**

Key Components – New Consumer Rights (cont.)

Individuals have rights to —

- **Request deletion** of all personal information
- Business must direct service providers to delete
- Numerous exceptions:
  - Certain internal uses e.g., complete a transaction requested or reasonably expected by consumer, perform a contract with consumer, use compatible with context in which consumer provided personal information
  - Detect and prevent security incidents and fraud
  - Newspapers (free speech)
  - Compliance with law
  - Using the consumer's information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information

Key Components – New Consumer Rights (cont.)

Individuals have rights to —

- **Opt out of sale** of personal info
  - Broadly includes selling, providing, or disclosing personal information in exchange for **monetary** or other **valuable consideration**
  - Home page link to a "**Do Not Sell My Personal Information**" page
  - Resellers of data must confirm compliant notice and opt-out provided
- **Consent (opt in) to sale of minor's** personal info (age 16)

Complying with requests

- **May not charge** for exercising rights
- Must offer **equal service and price**, unless the difference is "reasonably related to the value" of the consumer's data
- Must provide, at a minimum, **toll-free number and a website address** (if business maintains a website) so individuals can exercise their rights

Key Components – Enhanced Disclosures

Disclosure at or before collection: must disclose personal info collected and its use

New privacy policy requirements:

- Describe rights and how to exercise
- List categories of personal info collected, sold, and disclosed in prior 12 months
- Describe purposes for collection of personal info
- Link to “Do Not Sell” page (home page and data collection page that allows consumer to submit request not to sell his or her data (or household or device data))

Key Components – Service Providers

- Mandatory contract terms for service providers
  - Prohibit recipient from selling the personal information
  - Restrict use of personal information to performing services under contract
  - Prohibit use of personal information outside the direct relationship between person and the (disclosing) business
  - Include a certification regarding above
- Absent terms, vendor will be treated as a “third party” for purposes of disclosures and other obligations
- Notify service providers of deletion requests

Heightened Enforcement Risks

Private right of action and statutory damages of USD $100-$750 per consumer per violation in the event of data breach of unencrypted or "un-redacted" personal information, *if company did not have "reasonable" security*; **significant class action risk!**

Enforcement of privacy and security provisions by California Attorney General with penalties of up to $2,500 ($7,500 if intentional) per violation

California IoT Security Law

SB 327

- Requires manufacturers of connected devices (devices that are capable of connecting to the Internet and are assigned an IP or Bluetooth address) to implement reasonable security features that are:
  - Appropriate to the nature/function of the device
  - Appropriate to the information the device may collect, contain, or transmit
  - Designed to protect the device and any information contained in the device from unauthorized access, destruction, use, modification, or disclosure
- If the device includes a means of authentication outside a local area network (LAN), the following would be considered reasonable security features:
  - A preprogrammed password that is unique to each device manufactured; or
  - The device contains a security feature that requires a user to generate a new means of authentication before access is granted to the device for the first time

Federal Trade Commission

Jurisdiction over Digital Health Services

- Concurrent jurisdiction with HHS over HIPAA-covered digital health services
- Jurisdiction over digital health services not covered by HIPAA
- Section 5 of the FTC Act
  - Prohibits "*unfair or deceptive acts or practices in or affecting commerce*"
  - An act or practice is **deceptive** if:
    - There is a representation, omission, or practice that is likely to mislead
    - A consumer acting reasonably in the circumstances, and
    - The representation, omission, or practice is material
  - An act or practice is **unfair** if it:
    - Causes or is likely to cause substantial consumer injury that
    - Cannot be reasonable avoided by consumers, and
    - Is "not outweighed by countervailing benefits to consumers or to competition"

Federal Trade Commission

Enforcement

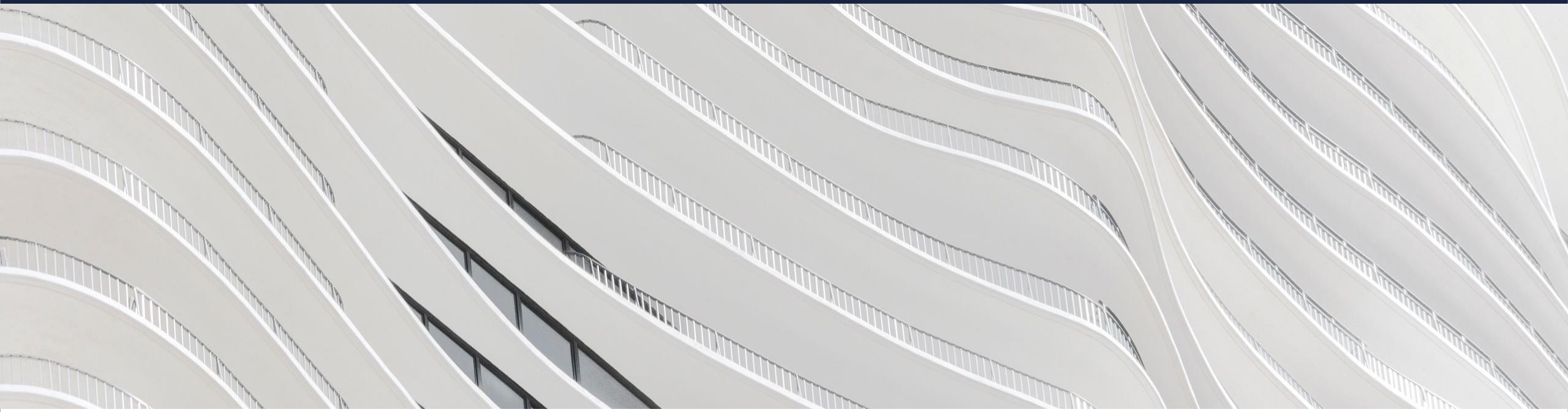
- FTC/OCR coordination in security investigations
  - Investigations into health information disposal practices of CVS Caremark and Rite Aid (consent decrees with FTC and resolutions agreements with HHS)
- FTC security enforcement against business associates
- LabMD – Commission rules that HIPAA/HITECH does not restrict the Commission's authority over unfair or deceptive practices
- Practice Fusion - a cloud-based electronic health record company allegedly misled consumers by soliciting reviews for their doctors, without adequately disclosing that these reviews would be publicly posted in an online healthcare provider directory. Resulted in patient's sensitive personal and medical information being posted.

Federal Trade Commission

Reports & Guidance

- FTC Privacy Report: *Protecting Consumer Privacy in an Era of Rapid Change* (2012)
- *Mobile Health App Developers: FTC Best Practices* (2016)
- Mobile Health Apps Interactive Tool (2016) (in coordination with HHS / OCR / FDA / ONC)
- *Sharing Consumer Health Information? Look to HIPAA and the FTC Act* (2016)
- *Internet of Things: Privacy & Security in a Connected World* (2015). FTC raised concerns about risks posed by connected health devices (especially consumer safety risks).

Considering FDA Compliance During Digital Health Patient Engagements



FDA Digital Health Innovation Action Plan

- **Key Goals**
  - Increasing the number and expertise of digital health staff at FDA
  - Launching the Digital Health Software Precertification Pilot Program
  - Issuing guidance to modernize FDA policies
- **FDA is working to provide clarity on the following topics:**
  - Wireless Medical Devices
  - Mobile medical apps
  - Health IT
  - Medical Device Data Systems
  - Medical device Interoperability
  - Software as a Medical Device (SaMD)
  - General Wellness
  - Cybersecurity

Mobile Apps and Other Software

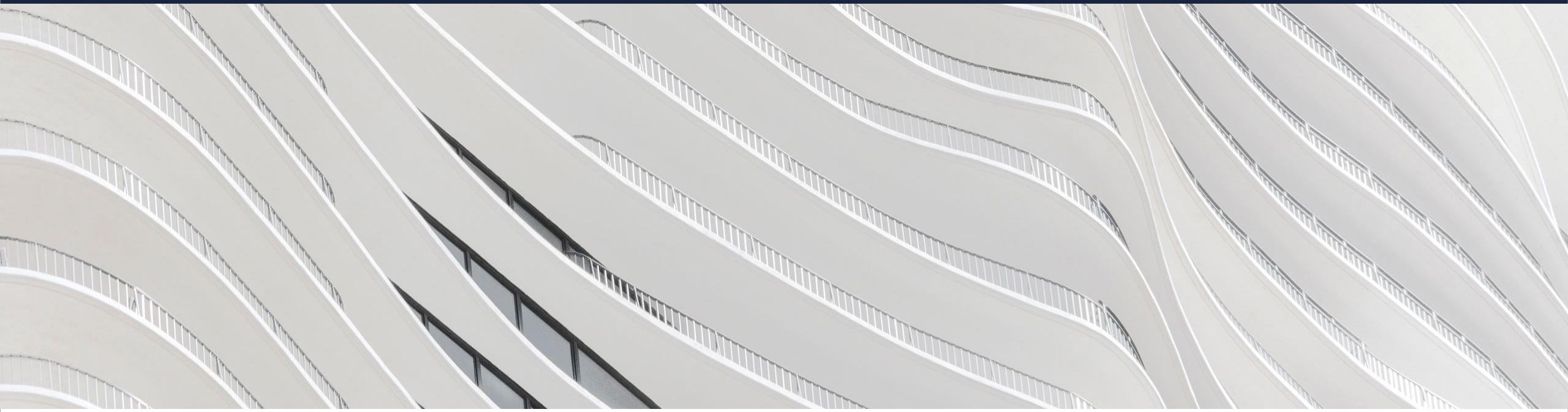
- Are they regulated devices, not a device, or maybe a device but subject to enforcement discretion?
- Analysis of functionality and claims/intended use.
- Consider medical device definition as impacted by 21st Century Cures Act software carve-out.
- 21st Century Cures Act is still new and being interpreted.
- Historical guidance impacted by new law; draft guidance updated but not finalized.
- Some clear areas but many remaining gray areas.

Other FDA Compliance Considerations

Other Issues Which May be Implicated When Interacting with Patients and HCPs

- Even if a technology or platform you are considering utilizing is not a device, if the program *relates to* one of your devices, consider:
  - Advertising and Promotion
  - Potential for Changes to Cleared/Approved Devices
  - Complaint / Adverse Event Capture, Escalation, and Reporting
  - Cybersecurity

How FDA Views Real-World Data to Create Real-World Evidence in Decision-Making



FDA Views on Data from Nontraditional Sources

Overview of Recently Enacted Authorities and Recently Adopted Guidance

- 21st Century Cures Act (2016)
  - Real World Evidence (Applies to drugs.)
  - Patient Experience Data (Applies to drugs.)
- FDA, Draft Guidance, *Submitting Documents Utilizing Real-World Data and Real-World Evidence to FDA for Drugs and Biologics* (May 2019)
- FDA, Draft Guidance, *Patient-Focused Drug Development: Collecting Comprehensive and Representative Input* (June 2018)
- FDA, Guidance, *Use of Real-World Evidence to Support Regulatory Decision-Making for Medical Devices* (August 2017)
- FDA, Guidance, *Use of Electronic Health Record Data in Clinical Investigations* (July 2018)
- FDA, Guidance, *The Least Burdensome Provisions: Concept and Principles* (February 2019)

Recognition of the Opportunity

What has FDA said about Real World Evidence?

- “The use of computers, mobile devices, wearables and other biosensors to gather and store huge amounts of health-related data has been rapidly accelerating. This data holds potential to allow us to better design and conduct clinical trials and studies in the health care setting to answer questions previously though[t] infeasible. In addition, with the development of sophisticated, new analytical capabilities, we are better able to analyze these data and apply the results of our analyses to medical product development and approval.”

21st Century Cures Act

Real World Evidence

- Section 3022 of the Cures Act defines "**real word evidence**" to mean "data regarding the usage, or the potential benefits or risks, of a drug derived from sources other than randomized clinical trials."
- Under the Cures Act, FDA is required to establish a program that evaluates the potential use of real world evidence in relation to drug development to: (1) help support the approval of new indications for a drug that FDA approved via the NDA process (i.e., a 505(b)(1) or 505(b)(2) application); and (2) help support or satisfy postapproval study requirements.
  - FDCA § 505F(a); 21 U.S.C. §§ 355g(a).

21st Century Cures Act

Patient Experience Data

- Section 3001 of the Cures Act defines “patient experience data” to include data collected by any person, including patients, caregivers, patient advocacy groups and drug manufacturers that are intended to provide information regarding a patients’ experiences with a disease.
  - FDCA § 561A; 21 U.S.C. § 360bbb-8c(c).
- Section 3002 of the Cures Act called for FDA to develop a plan to issue one or more draft and final guidance documents “regarding the collection of patient experience data, and the use of such data and related information in drug development.”

Guidance for Device Companies

Use of Real-World Evidence to Support Regulatory Decision-Making for Medical Devices

- "Under the right conditions, data derived from real world sources can be used to support regulatory decisions. RWD and associated RWE **may constitute valid scientific evidence depending on the characteristics of the data**. This guidance…describes the circumstances under which RWD may be used to support a variety of FDA decisions based on the existing evidentiary standards."

Underlying Standards for Product Marketing Authorization

Focus on Devices

- 510(k) Clearance: The device is demonstrated to be at least as safe and effective, that is, “substantially equivalent” to a legally marketed device that is not subject to a PMA.
- De Novo: General controls alone, or general and special controls, provide reasonable assurance of safety and effectiveness for the intended use, but there is no legally marketed predicate device.
- PMA: The PMA contains sufficient valid scientific evidence to provide reasonable assurance that the device is safe and effective for its intended use.

Key Concepts

Real World *Data*

- Real-world ***data*** are data relevant to patient health status and/or health care delivery collected from various sources. RWD can come from a number of sources including, for example:
  - Electronic health records (EHRs)
  - Claims and billing activities
  - Product and disease registries
  - Patient-generated data including in home-use settings
  - Data gathered from other sources that can inform on health status, such as mobile devices

Key Concepts

Real World *Evidence*

- Clinical evidence regarding the usage and potential benefits or risks of a medical product derived from analysis of RWD.

Device Guidance on RWE

Quality Matters

- FDA will maintain its evidentiary standards through the process of regulatory decision-making, by evaluating "whether the available RWE is of **sufficient quality to address the specific regulatory decision being considered**. FDA believes that the increased use of electronic data systems in the healthcare setting has the potential to generate substantial amounts of RWD. Because these systems can vary greatly in terms of quality, not all RWD can by itself generate sufficient evidence to support an FDA regulatory decision. Nevertheless, these RWD may still provide a valuable contribution to the totality of evidence considered for the decision."
  - FDA, Guidance, *Use of Real-World Evidence to Support Regulatory Decision-Making for Medical Devices*, at 9 (August 31, 2017)

Device Guidance on RWE

- Characteristics for Real World Data to Generate Real World Evidence
  - Accuracy in Comparison to Verifiable Source Documentation
  - Relevance
    - Is the source adequate for evaluating the performance of a device in the identified regulatory context (as a sole source or partial source of evidence)?
  - Reliability
    - How were the data collected (data accrual), and do the people and processes in place during data collection and analysis provide adequate assurance of error minimization, and sufficient data quality and integrity (data assurance)?

Device Guidance on RWE

Data Quality

- Certain sources of RWD, such as some administrative and healthcare claims databases or EHRs, may not have established data quality control processes.
- Consider any methods and systems used to help ensure sufficient data quality.
- Regardless of the original purpose for collecting the RWD, procedures for data collection and quality assurance should be put into place during the data source design and development stages (when applicable) to optimize the reliability, quality and usefulness of the data.
- Data collection procedures used for data platforms such as registries should be clearly defined and described in a detailed data management standard operating procedures (SOP) manual.
- Standardizing procedures to ensure the use of uniform and systematic methods for collecting and cleaning data are vital to ensuring data quality.
- **Document your approach.**

Device Guidance on RWE

Data Quality Assessment

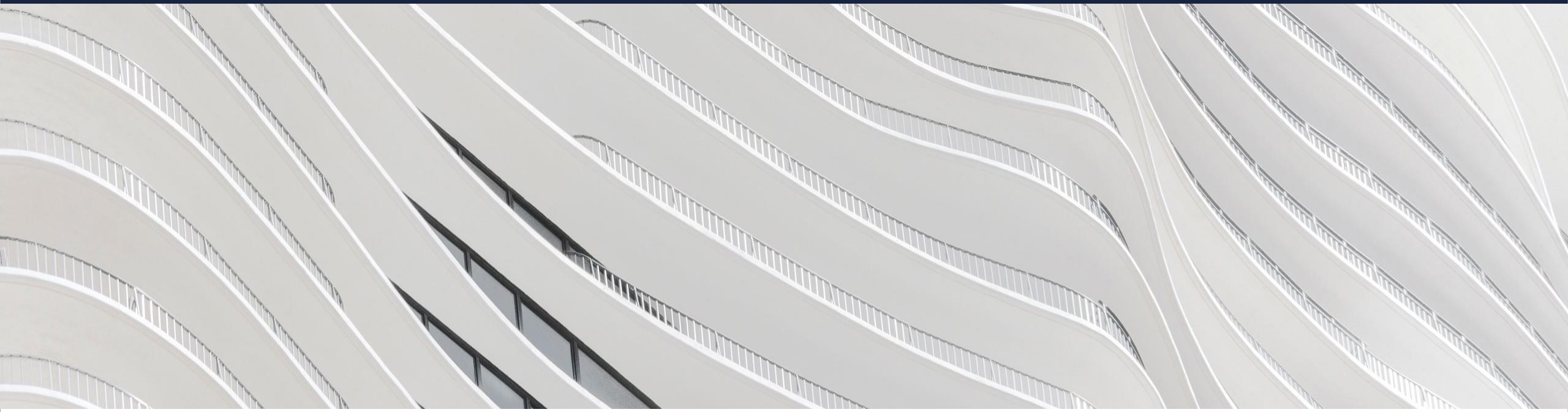
- Factors for consideration:
  - the quality of data element population (e.g., whether abstracted from a verifiable source to assess transcription errors or automatically populated through a data extraction algorithm);
  - adherence to source verification procedures and data collection and recording procedures for completeness and consistency;
  - completeness (i.e., minimized missing or out of range values) of data necessary for specified analyses, including adjustment for confounding factors;
  - data consistency across sites and over time;
  - evaluation of on-going training programs for data collection and use of data dictionaries at participating sites;
  - evaluation of site and data monitoring practices; and
  - the use of data quality audit programs.

Guidance on Use of EHRs in Clinical Investigations

Take-Aways

- Guidance applies to *prospective* clinical trials, across product types
- Potential Advantages:
  - Improve data accuracy
  - Promote clinical trial efficiency
  - Increase access to a variety of data types (e.g., clinical notes, physician orders, radiology and laboratory results, and pharmacy records)
  - Access to real-time data and opportunities for long-term follow up
- Key Concerns:
  - Interoperability of EHR systems with ***electronic data capture (EDC) systems*** in clinical investigations
  - Ensuring the quality and integrity of EHR data collected and used as ***electronic source data*** in clinical investigations

Remote Assessment and Treatment: State Professional Law Considerations



Key Concepts

- Using patient data to teach patients to manage their own health can be beneficial
- Whether health coaching or other activities require a license depends on the state ***where the patient is located***
- States have different rules about how health professionals and corporations can interact

Examples of Remote Patient Engagement

- “Telehealth” or “telemedicine” models include:
  - asynchronous store-and-forward evaluation
  - patient-to-provider video assessment
  - provider-to-provider video consultation
  - provider-to-provider imaging analysis
- Government coverage varies—CMS is constrained to a narrow definition of “Medicare telemedicine services” by statute but has begun exploring other avenues of reimbursement
- There are also specialty devices that collect specific types of biometric data (e.g. cardiac implants) and may be configured to permit remote monitoring

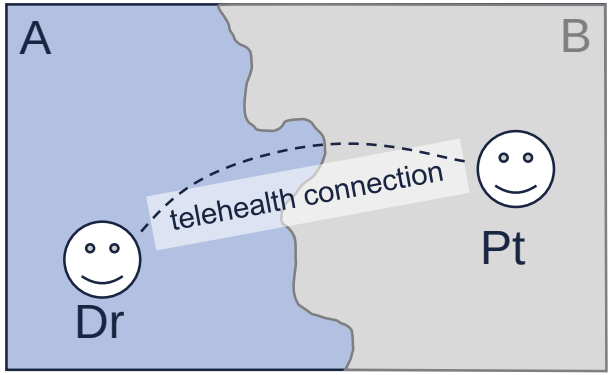
Health Professional Licensing

It's all about state law!

- The requirements that individuals need to meet before holding themselves out to the public as nurses, physicians, physical therapists, etc. ***vary from state to state***.
- For example, most state legislatures have passed laws with titles like "Nurse Practice Act" that generally prohibit anybody from performing certain acts of nursing unless they hold a current license from the state board of nursing.
- States then delegate development and enforcement of professional practice rules to regulatory boards, typically headed by committees of members of the regulated profession.
- These boards can enact binding rules and also conduct ***disciplinary hearings*** or even revoke licenses.
- The "scope of practice" for a profession is often a mix of clear rules from the legislature and board, and murkier local traditions expressed through disciplinary rulings.
- Even the list of licensure categories is not consistent from state to state.

Health Care Across State Borders

- The state-by-state professional licensing approach made the most sense when almost all health care was provided in person.
- ***The rise of reliable digital health allows easy inter-state health consultation, and not all states are keeping up***.
- The norm is that to treat anyone located in a given state, a professional license from that state is required (even if the health professional is outside the state at the time).
- Many states have made this restriction explicit through telehealth laws.
- States also have detailed, highly varied requirements for remote prescribing and other forms of telehealth interactions.
- Efforts like the Interstate Medical Licensure Compact aim to ease the burden of getting a new license for every state where a professional has a remote patient—but have not been widely adopted and still require a license in each state.



Dr needs a **State B** license

Corporate Practice

- Some states worry that if a company (with non-medical shareholders) employs health professionals, it will try to call the shots and interfere with the professionals' judgment of what is best for the patient. They have come up with more or less straightforward ways to stop this.
- For example: You need a state license to practice a health profession, and only natural persons or individuals can get licenses. Some states have long-standing interpretations saying that when a business hires a doctor to treat patients, the business is improperly "practicing medicine."
- Typically, even if a state forbids "corporate practice" of one or more health professions, it will provide exceptions for things like non-profit hospitals to employ professionals directly.
- Licensed professionals can also form their own partnerships. Corporations in the health care industry avoid practicing professions themselves by entering into management arrangements and other contracts with these independent professional groups.
- This is another area where state law varies widely, and another reason why it is very important to check with an attorney before attempting to arrange for any health care services provided on behalf of a business.

Thank you