FDLI FOOD & DRUG LAW INSTITUTE

Safeguarding Data and Privacy in Digital Health

January 31, 2024

Overview

- Data Protection Framework for Digital Health
- Enforcement Actions; Risk Parameters
- Data Privacy and Protection Best Practices

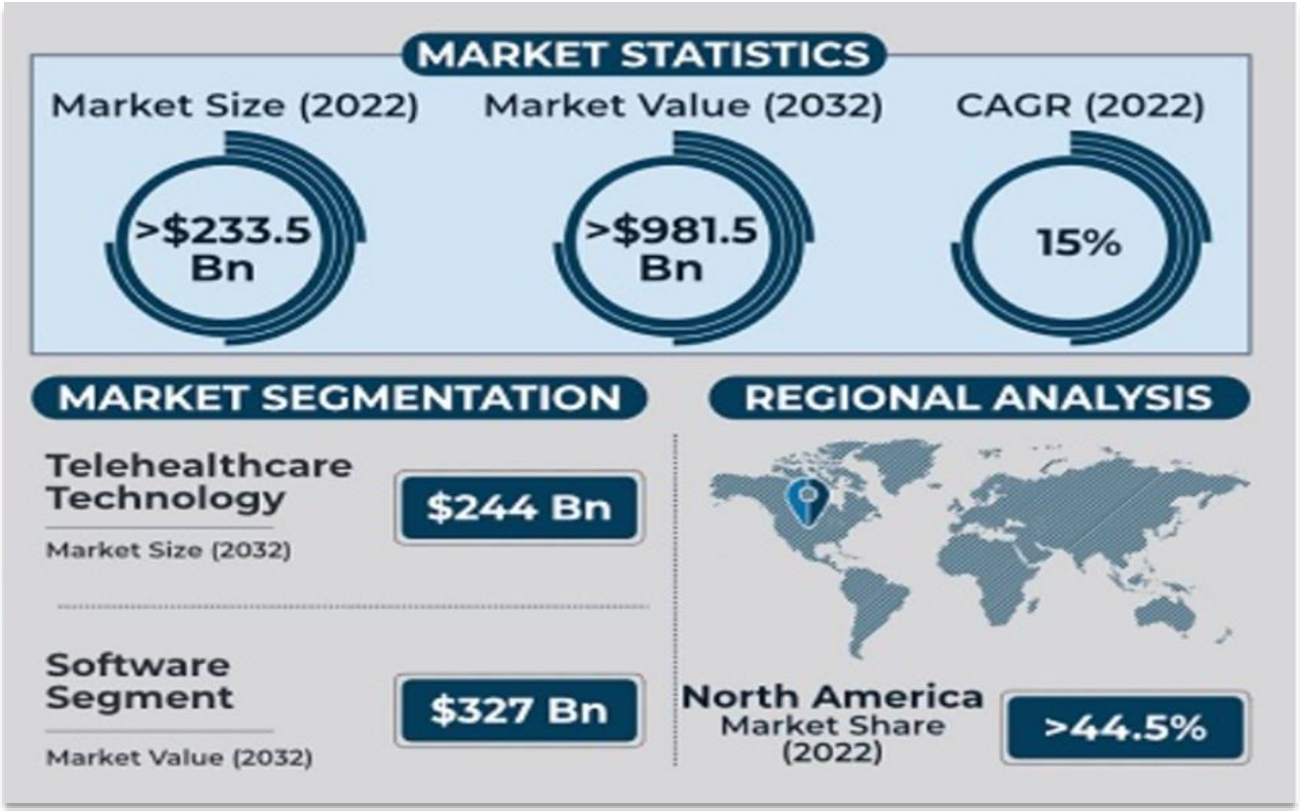
FDLI
FOOD & DRUG LAW INSTITUTE

Scope of Digital Health Technologies

- Digital Health encompasses broad categories of technologies, with an incredible trajectory, and evolving risks and solutions
- These digital tools are intended to give the industry more access and wider views and patients more control and resources
- The increased use of digital tools has led to heighted scrutiny and litigation and new cyber attacks

FDLI
FOOD & DRUG LAW INSTITUTE

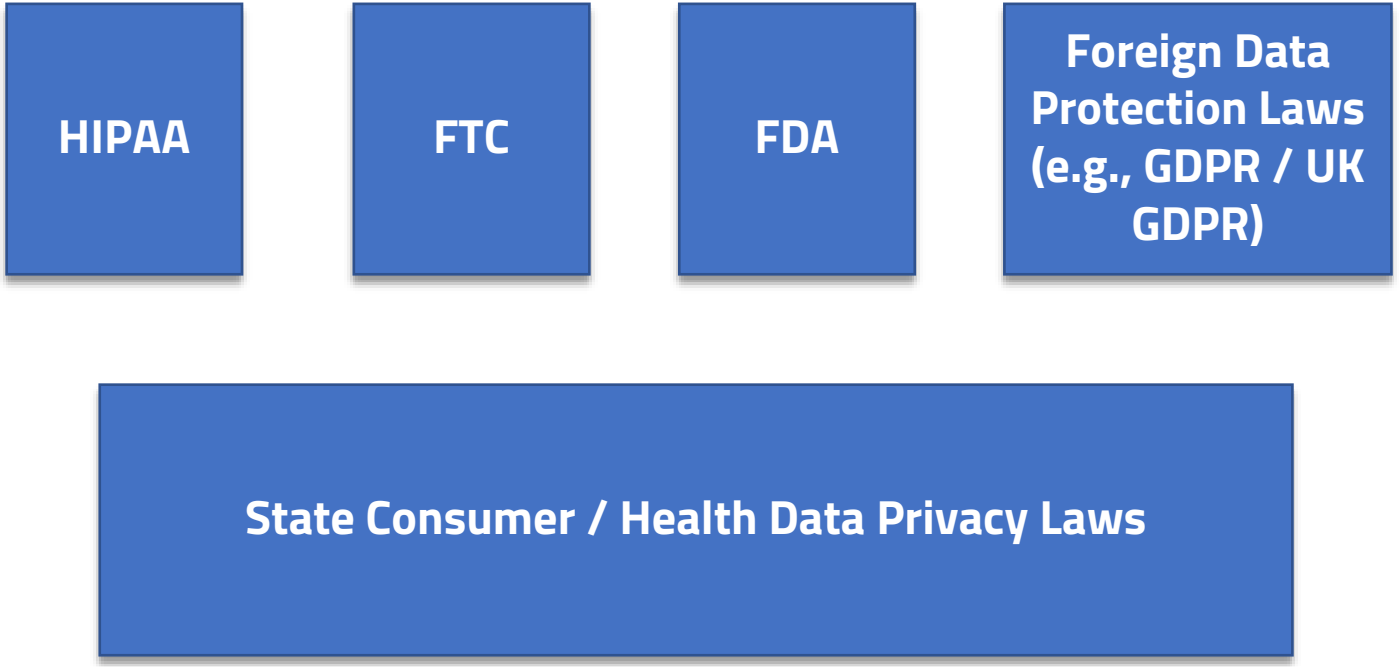
Market Growth of Digital Health Tech



FDLI
FOOD & DRUG LAW INSTITUTE

Data Protection Framework for Digital Health

Data Protection Framework for Digital Health



FDLI
FOOD & DRUG LAW INSTITUTE

Which Data Protection Frameworks Apply?

Initial Questions to Ask:

- What **type of data** are you collecting?
  - Identifiable health information / key-coded clinical trial data / de-identified data
- What **jurisdictions** are you operating in? Where are your **data subjects located**?
- Are you acting as a **covered entity / business associate** for HIPAA purposes?
- Is your technology a "**medical device**" for FDA purposes? Does it constitute "**Software as a Medical Device**"?

FDLI
FOOD & DRUG LAW INSTITUTE

When does HIPAA apply?

- HIPAA governs "**covered entities**" and "**business associates**"
- **Clinical trial sponsors** not typically governed by HIPAA

Covered Entities

- Health plans
- Health care clearinghouses
- Health care providers that *engage in standard electronic transactions*

Business Associates

- *Person or entity, other than a member of a covered entity's workforce, that creates, receives, maintains or transmits PHI on behalf of a covered entity for a function or activity regulated by HIPAA*

FDLI
FOOD & DRUG LAW INSTITUTE

Overview of HIPAA Rules

- **HIPAA Privacy Rule**: restrictions on *who* may use, disclose or access PHI; provides for individual rights to such PHI
- **HIPAA Security Rule**: administrative, technical and physical safeguards for electronic PHI
- **Breach Notification Rule**: reporting obligations in the event of a "breach" of unsecured PHI (*i.e.*, unauthorized acquisition, access, use or disclosure of PHI which compromises the security or privacy of such information)

FDLI
FOOD & DRUG LAW INSTITUTE

HIPAA Compliance

- ❑ HIPAA Security Officer / Privacy Officer
- ❑ HIPAA Policies & Procedures
- ❑ HIPAA Security Risk Analysis / Security Risk Management Plan
- ❑ HIPAA Training
- ❑ Business Associate Agreements

FDLI
FOOD & DRUG LAW INSTITUTE

FDA + Cybersecurity – *Is your technology regulated by FDA?*

Is your technology a "Medical Device" or "Software as a Medical Device"?

- **Medical Device** is intended for **use in the diagnosis of disease** or **other conditions**, or in the **cure, mitigation, treatment, or prevention of disease, in man or animals**
- Intended to **affect the structure** or **any function of the body of man or other animals**, and 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** (Food, Drug & Cosmetic (FD&C) Act, Section 201(h))
- **Software as a Medical Device (SaMD)**: "software intended to be used for **one or more medical purposes** that perform these purposes **without being part of a hardware medical device**"

FDLI
FOOD & DRUG LAW INSTITUTE

FDA - *Ensuring Cybersecurity of Medical Devices*

A "**cyber device**" is defined as follows:

(1) includes **software** *validated, installed, or authorized* by the sponsor as a device or in a device,

(2) has the **ability to connect to the internet**, and

(3) contains any **such technological characteristics validated, installed, or authorized by the sponsor that could be vulnerable to the cybersecurity threats**

Cybersecurity requirements do not apply to an application or submission submitted to the FDA before March 29, 2023. However, if cyber device was previously authorized and manufacturer is making changes that require premarket review by the agency, law would apply for new premarket submission

Requirements for manufacturers of cyber devices:

Plan to monitor, identify, and address **postmarket cybersecurity vulnerabilities** and exploits, including coordinated vulnerability disclosure and related procedures;

- Design, develop, and maintain **processes and procedures** to provide reasonable assurance that **device + related systems are cybersecure**, and make available **postmarket updates** and **patches to the device + related systems**; and
- Provide **software bill of materials** (incl. commercial, open-source, and off-the-shelf software components)

2023 guidance (*Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions*)

- FDA recognizes that med device cybersecurity is **shared responsibility** for healthcare facilities, patients, healthcare providers and manufacturers of medical devices

FDLI
FOOD & DRUG LAW INSTITUTE

HHS Cybersecurity Strategy

OCR reported **93% increase** in large breaches reported from 2018 – 2022, with **278% increase** in large breaches reported to OCR involving **ransomware**

Overview of HHS Strategy

HHS will:

- Establish **voluntary cybersecurity performance goals for healthcare sector**
- **Provide resources to incentivize and implement these cybersecurity practices**
- Implement HHS-wide strategy to **support greater enforcement and accountability**
- Mature one-stop shop within **HHS for healthcare sector cybersecurity**

FDLI
FOOD & DRUG LAW INSTITUTE

Patchwork of State Consumer Privacy Laws

California

California Consumer Privacy Act / California Privacy Rights Act (CCPA)

Colorado

Colorado Privacy Act (CPA)

Connecticut

Personal Data Privacy & Online Monitoring Act (CPDPA)

Delaware

Delaware Personal Data Privacy Act (January 2025)

Indiana

Indiana Consumer Data Protection Act (January 2026)

Iowa

Act relating to consumer data protection (January 2025)

New Jersey

New Jersey Data Privacy Act (January 2025)

Montana

Montana Consumer Data Privacy Act (October 2024)

Oregon

Oregon Consumer Privacy Act (July 2024)

Tennessee

Tennessee Information Protection Act (July 2025)

Texas

Texas Data Privacy and Security Act (July 2024)

Utah

Utah Consumer Privacy Act (UCPA) (December 2023)

Virginia

Virginia Consumer Data Protection Act (VCDPA)

FDLI
FOOD & DRUG LAW INSTITUTE

Washington State & Nevada Health Data Privacy Laws

Exempts HIPAA and clinical trial research data.

Cannot collect or share consumer health data unless consent obtained, or collection/sharing is necessary to provide a product or service.

Cannot sell consumer health data absent signed authorization from consumer.

Must post a separate consumer health data privacy policy online.

Washington only: **Private right of action**

Most provisions of each law come into effect on March 31, 2024.

- "***Consumer health data***": personal information that is linked or reasonably linkable to a consumer and that identifies a consumer's past, present, or future physical or mental health.
- "***Consumer***": an individual resident of the state or a person whose consumer health data is collected in the state, excluding individuals acting in an employment context.

FDLI
FOOD & DRUG LAW INSTITUTE

Enforcement Actions; Risk Parameters

California AG Enforcement: Glow Case

- **Glow, Inc. offered a fertility-tracker app**
  - Tracked periods, ovulation
  - Other data related to sexual and reproductive health
- **Stored Information on app users':**
  - Medications
  - Fertility test results
  - Medical appointments
  - Medical records
- **CA AG alleged Glow unlawfully:**
  - Allowed disclosure of app users' sensitive health information to supposed partners without authorization
  - Failed to provide password protection and thereby made user health information accessible to unauthorized users
- **Claimed violations of**, *inter alia*, the California Confidentiality of Medical Information Act (CMIA)

FDLI
FOOD & DRUG LAW INSTITUTE

California Confidentiality of Medical Information Act (CMIA)

- CMIA is much like HIPAA privacy and security rules
- Prohibits use/disclosure of personal health information without individual authorizations, with limited exceptions
- Applies to health care providers and health plans, but ALSO applies to:
  - *Pharmaceutical companies*
  - *Mobile applications and technologies that collect personal health information*
- Enforceable by the CA Attorney General
- Private Right of Action

FDLI
FOOD & DRUG LAW INSTITUTE

CA AG Settlement With Glow (2020)

- $250,000 civil penalty
- Injunctive requirements for Glow to, among other things:
  - Implement and comply with detailed information security program
    - Prevent partner access to user information without affirmative authorization
    - Prevent password changes without identity verification
  - Obtain individuals' affirmative authorization to share personal health information with *any third parties other than service providers*, except as required by law
  - Restrict access to personal health information within Glow based on necessity and job function

FDLI
FOOD & DRUG LAW INSTITUTE

FTC Action Against Flo Health

- FTC Alleged Flo Health app, which tracked women's ovulation cycles through inputs from users, engaged in unfair and deceptive practices.
- Example of Alleged Practices:
  - Flo App privacy policy said Flo would only share personal information for purposes of operating and servicing the app.
  - But Flo "entered into agreements with third parties . . . That permitted them to use Flo App users' personal information for the third parties' own purposes, including for advertising and product improvement."

FDLI
FOOD & DRUG LAW INSTITUTE

FTC Authority

- Section 5 of the FTC Act prohibits unfair or deceptive conduct that harms consumers
- Section 5 applies broadly across industries, including entities regulated by HIPAA and those that are not
- FTC Health Breach Notification Rule requires notification of security breaches involving personal health information stored in personal health records
- FTC actions can result in substantial penalties, including fines and injunctive relief

FDLI
FOOD & DRUG LAW INSTITUTE

FTC on Data Privacy and Security

- The FTC considers misleading statements or omissions in a privacy policy, user interface, or privacy setting, to constitute a *deceptive trade practice* under FTC Act Section 5
- Failure to provide reasonable security for personal information may constitute an *unfair trade practice* under FTC Act § 5
- Unauthorized *sharing* of personal health information by a vendor of personal health records constitutes a "breach" of security

FDLI
FOOD & DRUG LAW INSTITUTE

FTC Settlement With Flo Health

- Flo settlement agreement (2021) requires that Flo:
  - notify affected users about the disclosure of their health information
  - instruct any third party that received users' health information to destroy that data
- Agreement prohibits Flo from misrepresenting:
  - how and for what purposes it collects, maintains, uses, discloses, deletes, or protects users' personal information
  - how much consumers can control these data uses; its compliance with any privacy, security, or compliance program

FDLI
FOOD & DRUG LAW INSTITUTE

FTC Action Against Premom

- Premom app, offered by Easy Healthcare Corp, is a fertility app that allows users to upload information about periods, ovulation tests, temperature, weight, and other health information
- FTC alleged the app shared users' personal information with third parties, including two China-based firms, without notice to consumers
- Complaint alleges:
  - Failure to disclose + privacy misrepresentations
  - Collection of location data without notice
  - Unfair sharing of health information for advertising without affirmative express consent
  - Failure to notify consumers about unauthorized disclosure, as required by Health Breach Notification Rule

FDLI
FOOD & DRUG LAW INSTITUTE

FTC Settlement with Easy Healthcare

- To settle the FTC's complaint, Easy Healthcare had to pay a $100,000 civil penalty for violating the Health Breach Notification Rule
- Also, Easy Healthcare is:
  - Permanently prohibited from sharing user personal health data with third parties for advertising;
  - Required to obtain user consent before sharing personal health data with third parties for other purposes;
  - Required to retain users' personal information for only as long as necessary to fulfill the purpose for which it was collected;
  - Prohibited from making future misrepresentations about Easy Healthcare's privacy practices and required to comply with the HBNR notification requirements for any future breach of security;
  - Required to seek deletion of data it shared with third parties;
  - Required to send and post a consumer notice explaining the FTC's allegations and the settlement; and
  - Required to implement comprehensive security and privacy programs that include strong safeguards to protect consumer data.
- As part of a related action, Easy Healthcare also has agreed to pay a total of $100,000 to Connecticut, the District of Columbia, and Oregon, which worked with the FTC on the case, for violating their respective laws

FDLI
FOOD & DRUG LAW INSTITUTE

FTC Action Against BetterHelp

- BetterHelp, an online mental health provider, allegedly shared customers' identifiable health data with social media companies for advertising purposes, contrary to online representations the company made to customers
- The allegedly identifiable health data consisted of customer email addresses, which had been hashed to protect customer identities
- The FTC claimed BetterHelp knew the recipient social media companies could undo the hashing, and, by not informing consumers of the sharing, BetterHelp deceived them

FDLI
FOOD & DRUG LAW INSTITUTE

BetterHelp Consent Order (2023)

- Monetary penalty: $7.8 Million
- Injunctive relief -- BetterHelp must:
  - cease sharing any identifiable mental health information for advertising purposes
  - obtain affirmative, express consent before sharing consumers' personal information third parties
  - direct third parties to whom disclosed consumer health information to delete it
  - limit the period of its retention of personal health information
  - put in place a comprehensive privacy program to protect consumer data

FDLI
FOOD & DRUG LAW INSTITUTE

FTC Action Against GoodRx

- GoodRx, which offers prescription drug discounts and telehealth visits, allegedly promised its users that it would:
  - Only share their personal information with certain third parties for limited purposes;
  - Never share PHI with advertisers or other third parties.
- GoodRx allegedly breached these promises by:
  - Sharing sensitive user information with third-party advertising companies and platforms (Facebook, Google, Criteo, Branch, Twilio) without providing **notice** to its users or seeking their **consent**
  - Exploiting the info shared with Facebook to target GoodRx users with **ads**
- FTC Settlement (2023):
  - $1.5 million civil penalty
  - Prohibition on sharing users' identifiable health information with third parties for most advertising purposes

FDLI
FOOD & DRUG LAW INSTITUTE

Online Tracking Technologies

Cookies and Pixels

- Track visitor activity on a website
  - At least a third of the largest health systems are using pixels
  - E.g., the Meta Pixel – used by more than 6.7 million websites to analyze consumers site usage

Video, Session Replays, and Chatbots

- Videos posted on a website, including videos incidental to a product offering
- Chatbots streamline inquiries by using AI to answer customer questions or to connect them
- Session replay tools collect information about a user's interactions with a webpage (cursor movements, clicks, pageviews)

FDLI
FOOD & DRUG LAW INSTITUTE

Claims Concerning Pixels Collecting Health Information

Unauthorized disclosure; improper safeguards

- Information from MyChart patient portal and appointment scheduling disclosed to Meta
- Negligence for failing to implement reasonable safeguards to prevent disclosure and failing to train
- E.g., *In re Advocate Aurora Health Pixel Litigation* (W.D. Wis.) and *Weddle v. WakeMed Health and Hospitals d/b/a WakeMed* (N.C.)

Violation of privacy (no prior consent)

- Websites containing third party analytics tools that divulged information without their consent
- E.g., *Doe v. Partners Healthcare System, Inc.* $18.4 million settlement

Class Actions Challenging Insurers' Use of AI

- Health insurers (Cigna, United Healthcare, Humana) are being targeted by class action lawsuits alleging breach of contract, bad faith, and insurance law violations
- Complaints allege:
  - Use of AI models resulted in denial of claims that, if reviewed by humans, would have been covered.
  - "Defendants have deliberately failed to fulfill their statutory, common law, and contractual obligations to have a doctor determine individual coverage for post-acute care in a thorough, fair, and objective manner, instead using the nH Predict AI Model to supplant real doctors' recommendations and patients' medical needs."
  - AI was used "to automatically deny payments in batches of hundreds or thousands at a time for treatments that do not match certain present criteria, thereby evading the legally-required individual physician review process."

FDLI
FOOD & DRUG LAW INSTITUTE

Department of Justice Investigation of AI Use in Healthcare

- Justice Department reportedly is investigating digital health companies' use of AI embedded in patient records for treatment recommendation purposes*
- Subpoenas to pharmaceutical and digital health companies reportedly seek information on:
  - Algorithms built into electronic medical records that may prompt recommendations for excessive screening or treatment
  - Algorithms identify conditions, trends, and treatment responses
  - Justice may be concerned about the anti-kickback implications
    - In 2020, Justice settled criminal charges against Practice Fusion and Perdue Pharma for allegedly colluding to prompt painkiller prescriptions through automated EMR alerts (https://www.justice.gov/opa/pr/electronic-health-records-vendor-pay-145-million-resolve-criminal-and-civil-investigations-0)

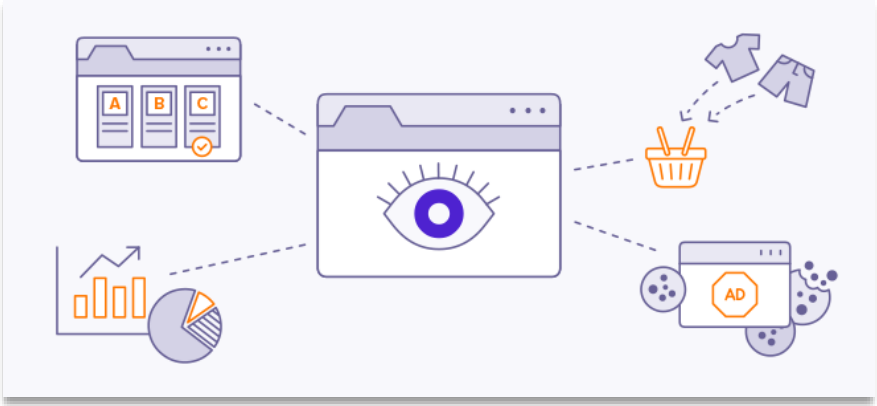
* Bloomberg Law, January 29, 2024

FDLI
FOOD & DRUG LAW INSTITUTE

Best Practices

Best Practices for Digital Health

- **Act, Plan, Review, Repeat**
  - Don't wait, Be Proactive
  - Know your Assets, Visit your App, Website
- **Teamwork** – C-Suite, Compliance, Facilities, IT, Legal, Workforce
- **Mission Possible**: Continue to find areas to improve
  - Breach Logs
    - In Diligence, "no breaches" can be a flag
  - Red Team Reviews
  - Risk Analysis/Risk Management Plans
  - Table Top Breaches

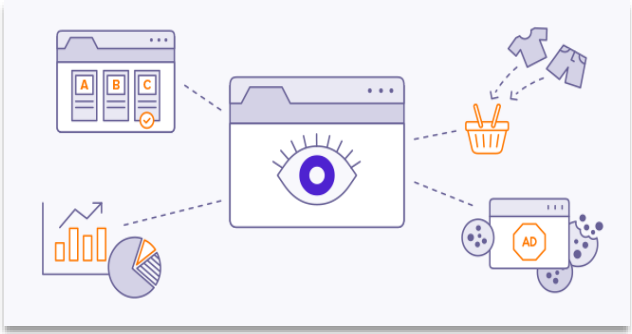


FDLI
FOOD & DRUG LAW INSTITUTE

Best Practices for Digital Health

Do

- Maintain an up-to-date data flow and governance
    - Consider silo-ing the most restricted/sensitive data from flows
    - Consider when less data means less exposure
- Carefully consider the use of chatboxes, scheduling and video interfaces
- Embrace secured communication channels (secure messaging platforms, VPNS);
- Enforce data and mobile device hygiene by workforce
- Conduct annual vendor assessments/attestations
    - Ensure internal audits/assessments are under legal privilege

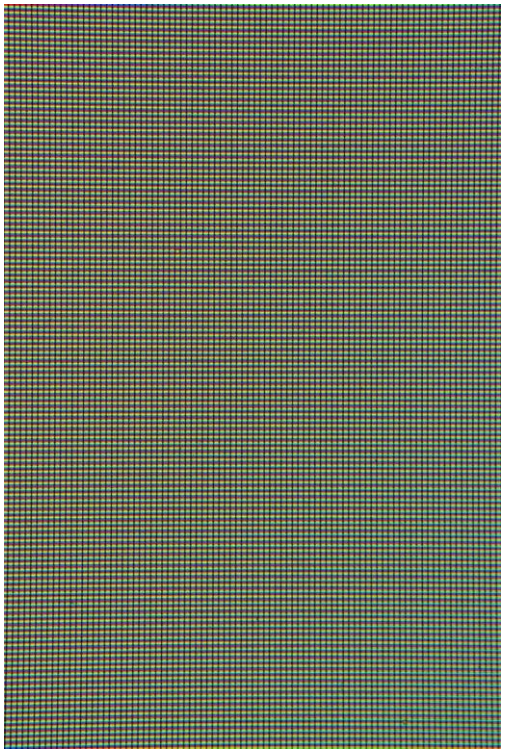


Don't

- Underestimate encryption and standards
- Get comfortable
- Treat all information as equal
- Be afraid of using different third-party experts
- Forget to read your cyber coverage exclusions

FDLI
FOOD & DRUG LAW INSTITUTE

Best Practices for Web-Tracking Compliance



- Comprehensive App and Website Review
  - Determine Consumer vs. PHI
  - Determine any PHI Tracking without BAAs
- Website Privacy Policy and Public-Facing Representations Review
- Vendor Attestation and Contractual Standards Review
- Customized Trainings, Including Reporting Mechanisms
- Internal Systems and Processes Review
- Privileged Forensic Assessment
- Corrective/Improvement Action Plan

FDLI
FOOD & DRUG LAW INSTITUTE

Best Practices for Digital Health

A.I. Calibrations and Data Asset Tracking

A.I. and ML in asset tracking systems allow healthcare entities to quickly identify and visualize historic patient data, creating simpler and more streamlined resolutions to patient care. Healthcare entities that use these tools should:

- Consider whether the state scope of practice, licensure, and marketing laws (e.g., the white coat rule) may restrict the use of AI/ML in healthcare;
- Assess whether appropriate restrictions or guardrails should be put in place to limit the extent of provider reliance on the AI's determinations;
- Evaluate whether the informed consent should include additional descriptions of AI interplay or other disclaimer language for services using AI and what guardrails should be implemented to enhance transparency and patient trust;
- Conduct auditing and testing through the implementation of oversight and safety mechanisms to mitigate and manage potential risks.

FDLI
FOOD & DRUG LAW INSTITUTE

A.I. Privacy Standards

Notable 2024 Developments

- As of Jan. 9th the ONC issued its Final Rule, aimed at "enhance[ing] the access, exchange, and use of electronic health information", by demystifying the complexities of certain A.I. tools in healthcare. The Final Rule aimed at increased transparency in the use AI/ML will require the following:
    - That developers of certified health IT conduct risk management for all predictive DSIs in their health IT modules;
    - That developers of certified health IT must submit summary information on their intervention risk management practices to a publicly accessible ONC site; and
    - That certified health IT modules with predictive DSIs disclose comprehensive performance information to end users.
- As of January 24th, the FDA's ISTAND Pilot Program accepted its first submission based on AI digital health technology. The submission, for an automated tool that assesses indicators of depression and anxiety, is also the first accepted into the program to be neuroscience-focused.

FDLI
FOOD & DRUG LAW INSTITUTE

Best Practices for Digital Health

Building Patient Trust

- Consider DUA Drops: As high as 90% after 30 days
- Building patient trust in digital health requires transparency, feedback and security
- Transparently communicating how health-tech platforms use data collected from patients (chatbots, questionnaires, or speaking to providers);
- Allowing patients to exercise some measure of control over when and how their data is being shared (UC Davis Study);
- Making data policies more transparent and understandable, avoiding burying patients in legalese.

Bottom line: Patients feel more comfortable sharing information when they understand and trust

FDLI
FOOD & DRUG LAW INSTITUTE

Heather Deixler, Partner, Latham & Watkins LLP
heather.deixler@lw.com

Nancy Perkins, Counsel, Arnold & Porter Kaye Scholer LLP
nancy.perkins@arnoldporter.com

Sara Shanti, Partner, Sheppard Mullin Richter & Hampton LLP
sshanti@sheppardmullin.com

FDLI
FOOD & DRUG LAW INSTITUTE