PRIVACY LAW

CALIFORNIA LAWYERS ASSOCIATION

presents

Inaugural Annual Privacy Summit

Session 5, Track 1

Health Privacy: Pixels, Apps and Emerging Issues

MCLE: 1.0 Hours

Friday, February 10, 2023
10:15 a.m. – 11:15 a.m.

Speakers:

Harry Nelson, Founder and Managing Partner, Nelson Hardiman LLP
Dona Fraser, Senior Vice President, Privacy Initiatives, BBB National Programs Robert J. Quigley, Attorney, Federal Trade Commission, Western Region, Los Angeles

Conference Reference Materials

PRIVACY LAW

CALIFORNIA LAWYERS ASSOCIATION

Health Privacy: Pixels, Apps + Emerging Issues

Harry Nelson/February 9, 2023

PRIVACY LAW
CALIFORNIA LAWYERS ASSOCIATION

Where to Look for Health Privacy Laws

1. **Federal:**
   -Health Information Portability and Accountability Act (HIPAA)
   -Title 42 CFR Part 2 (Substance Use Disorder-focused)
   -Family Educational Rights and Privacy Act (FERPA)
   -Genetic Information Nondiscrimination Act (GINA)
   -Americans with Disabilities Act / DOL / EEOC regulations (employees)

2. **State Health Privacy Laws (*e.g.* California's Confidentiality of Medical Information Act (CMIA, Civil Code §§ 56 *et seq.*)**

3. **Subject-Specific Related Laws (*e.g.* Psychiatric records (Welfare & Institutions Code § 5328); HIV Blood Tests (Health & Safety Code § 120975); Genetic Information Privacy Act (GIPA) (not exhaustive)**

4. **Common Law, Evidence Code §§ 990 *et seq.* (Provider-Patient Privilege)**

5. **Consumer Privacy Laws (CCPA, CPRA, etc.)**

PRIVACY LAW
CALIFORNIA LAWYERS ASSOCIATION

Recent Developments in Health Privacy

- **Title 42 CFR Part 2:** November 2022 Proposed Rule to bring Substance Use Disorder Record Management into alignment with HIPAA (Still pending; expected 2023)

- **HIPAA:** January 2021 proposed revisions to strengthen individual right to access own health information; facilitate information sharing for care coordination, case management, family and caregiver involvement (emergencies/health crises); reduce administrative burdens on HIPAA covered health care providers and health plans (Still pending; expected 2023)

- **Confidentiality of Medical Information Act** (CMIA)
  - AB 1184 prohibits disclosure of medical information related to sensitive services (mental or behavioral health, sexual and reproductive health, sexually transmitted infections, substance use disorder, gender-affirming care, and intimate partner violence)
  - AB 2089 CMIA revision to include “mental health application information” in its new expanded definition of “medical information,” and imposing additional obligations for businesses offering a mobile-based application or online “mental health digital service” to a consumer for the purpose of allowing the consumer to manage their own information, or for the diagnosis, treatment or management of a medical condition.

PRIVACY LAW

CALIFORNIA LAWYERS ASSOCIATION

Drivers of questions and evolving attitudes to health privacy

- *Dobbs v. Jackson Women's Health Organization* (2022): Ramifications of state government (and private attorney general action) **threats to pursue providers, patients, and third parties** for their activities related to seeking/offering/enabling/providing/obtaining prohibited procedures

- Growing attention of the capacity of technology to compromise health privacy via **tracking of activity** across sites, apps, platforms harnessed in the interest of selling

- Growing awareness of the **limits of HIPAA** in addressing problems of the moment

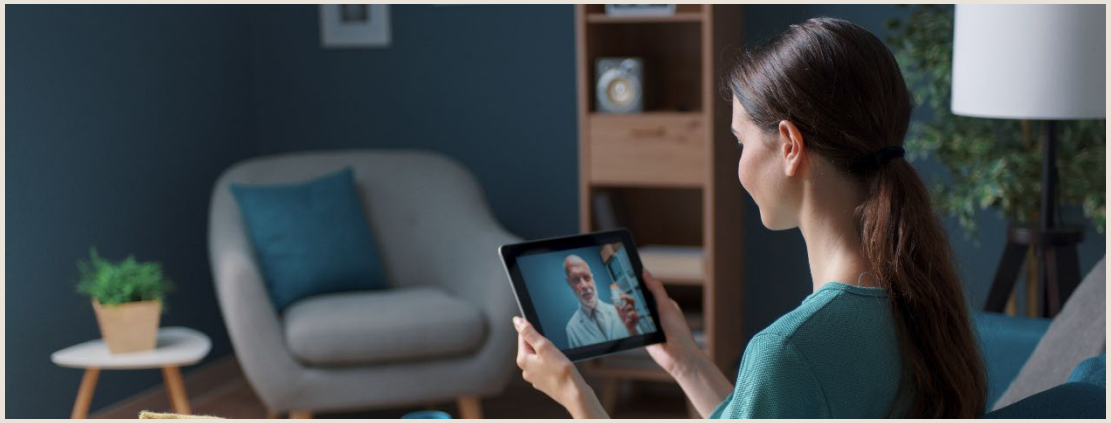
- On the horizon: next generation ability of personalized health information to deliver a new generation of customized healthcare recommendations and revealing a **new level of insight into future health risks**

PRIVACY LAW

CALIFORNIA LAWYERS ASSOCIATION

Did *Dobbs v. Jackson Women's Health* expose the inadequacy of our current health privacy laws?

Post-Dobbs, the scope of privacy as a constitutionally protected right is substantially narrower *(i.e.* abortion is no longer a protected part of privacy), permitting states to restrict personal decisions/medical options related to terminating a pregnancy.



Op-Ed: Facebook helped police with an abortion investigation in Nebraska. That's troubling news everywhere

The "Pixel" and the Front Line of Health Privacy

PRIVACY LAW
CALIFORNIA LAWYERS ASSOCIATION


Pixel Hunt

"Out Of Control": Dozens of Telehealth Startups Sent Sensitive Health Information to Big Tech Companies

An investigation by The Markup and STAT found 49 out of 50 telehealth websites sharing health data via Big Tech's tracking tools

By Todd Feathers, Katie Palmer for STAT, and Simon Fondrie-Teitler

- The Pixel: Transmission of data to designated social media platforms embedded in websites/apps. A 2-sided use of consumer health (and other) data.
- Consumers unaware of use of third party identifiers, tracking technologies (location tracing), search engine usage being used to share health data
- Consumer voluntary inputting of health data in various platforms (GPSchat, Fitness Trackers, *etc.*)
- Consumer businesses unaware of their responsibilities with health data

HIPAA's Limits (protecting like it's 1996)

PRIVACY LAW
CALIFORNIA LAWYERS ASSOCIATION

- Limited focus on specifically defined "covered entities" (health plans, healthcare data clearinghouses, and healthcare providers who electronically transmit health information in transactions for which HHS has adopted standards) and their "business associates" –driven by concern with federal jurisdictional constraints.
- Not focused on risk of governmental overreach (replete with exceptions to protect authority of state public health and law enforcement investigation, including "reporting of disease or injury, child abuse, birth, or death, public health surveillance, or public health investigation or intervention.")
- HIPAA was groundbreaking in creating national standards to protect sensitive patient information but does not address key issues that have arisen recently, *e.g.*
- Privacy/security of patient health information accessed or stored on personal cellphones or tablets.
- Geo-location information, Internet search history, information voluntarily shared online or data entered into mobile apps (unless a covered entity provides the app).

Traditional definition of Health Privacy: Practices undertaken by providers to maintain the security and confidentiality of "individually identifiable health information" (HIPAA) in medical and patient records.

PRIVACY LAW
CALIFORNIA LAWYERS ASSOCIATION

Evoution of the definition of Health Privacy:

- Increasingly overlapping with **Health Data Security** (protecting electronic personal health information (ePHI) created, received, used, or maintained by a provider

- What about the privacy individually identifiable health information in **other settings** (outside of provider-patient relationships)? When voluntarily offered by consumers?
- What about the risk of "de-identified" health information being "re-identified"
- To what extent can patients and providers secure information and record it selectively? Decline to cooperate with inquiries?
- Where do we need new laws to protect social boundaries of what we don't want other people to know

PRIVACY LAW
CALIFORNIA LAWYERS ASSOCIATION

New Questions About Need for Greater Privacy Protection Even Within U.S. Healthcare

Epic

Hospitals that use Epic hold medical records of 78% of patients in the United States in a cloud-based platform. Providers using Epic share 100M records per month with each other and providers using other EHR systems.

surescripts

Apart from the large EHR vendors (who embed e-prescribing solutions), SureScripts is the leading e-prescribing platform embedded in many telehealth platforms.

dose spot

E-prescribing platform for accessing SureScripts, e.g. for telemedicine, may allow one clinician using the platform to see and reference another provider's prescribing history for a common patient

PRIVACY LAW
CALIFORNIA LAWYERS ASSOCIATION

Stakeholders with competing interests in the Health Privacy Conversation and Pressure for a new Ethic of Health Privacy

- Patients: Voluntary oversharing data. Emerging concerns with health data in the “wrong” hands
- Providers: Concerns over licensing risks from information “leakage”. Searching for ways to find “lookalike” patients/clients without violating legal obligation
- Social media/technology platforms: aggregating multiple sources of data to sell or show consumers more ads
- Consumer Services: interested in streamlined approaches to data and resistant to health data-specific limits
- State and federal regulators (protecting and, in some cases, pursuing data)
- Employers
- Payers
- Other Insurers (*e.g.* life/disability): interested in data to reduce underwriting risks
- Entities that store/transmit patient health data:

PRIVACY LAW
CALIFORNIA LAWYERS ASSOCIATION

Towards a new health privacy agenda

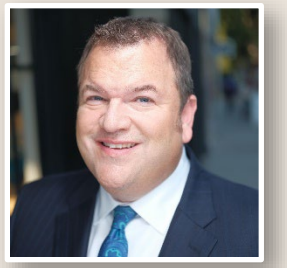
Revisiting privacy protections to build stronger legal infrastructure to protect health privacy

Educating consumers on “good hygiene” in health privacy--taking better care of where you input personal information, what you input, and how it’s used. Know and assert your rights. Review recommended steps for better protection: **https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/cell-phone-hipaa/index.html**

Need for providers – and consumer-focused platforms to be sensitized to potential threats to privacy -Policies/procedures – recordkeeping, responses to government

Test cases ahead: Stay tuned. This topic will need updating!

Questions? Comments? Grievances?



Harry Nelson
Founding Managing Partner
Nelson Hardiman LLP
Hnelson@nelsonhardiman.com

Trending Topics in Healthcare Privacy

1. **The Limits of HIPAA in Addressing Data Privacy Concerns in a Post-*Dobbs* World** Following the Supreme Court decision in *Dobbs* reversing *Roe v. Wade*, numerous states reinstated or implemented abortion bans and restrictions or began efforts to do so. A number of abortion restrictive states announced their intention to investigate and prosecute patients, providers, and even third parties (such as employer health plans) who facilitated out-of-state abortions in abortion-permissive states. These included the threat of using state criminal laws to override reproductive health privacy (*e.g.* by using patient medical records or health facility records to incriminate a patient or provider and by accessing information online to determine who has been seeking or offering abortion-related care. These efforts and the risks associated with health data highlighted the limits and gaps of HIPAA as a source of legal protection for provider-patient confidentiality, personal medical information and data privacy. In a June 2022 guidance statement, the Department of Health and Human Services was only able to concerned, out-of-state providers than a statement that HIPAA permitted but did not necessarily require them to disclose Protected Health Information (PHI) under HIPAA's exception allowing disclosure of "serious and imminent threat to the health or safety of a person or the public". Enacted in 1996, HIPAA was not designed for the modern health data environment. Among other limitations, HIPAA applies narrowly to healthcare providers who submit electronic claims to third party payers ("Covered Entities") and their contracted "Business Associates" who handle data on their behalf, and does not address other entities, leaving only the protections of state law (both state-specific health privacy laws and comprehensive consumer data privacy laws (thus far in California, Colorado, Connecticut, Virginia, Utah). The *Dobbs* decision and its aftermath raise multiple questions about health privacy, including how much patients and providers can "secure" it and prevent outside access, and where we may need new law to protect the social boundaries of health information we don't want others to know.

2. **The "Meta" Problem with Meta's Pixels:** A recent investigation by TheMarkup and STAT found that 33 of the top 100 American hospitals had an embedded "Meta Pixel" tracker on their public facing websites. These trackers were actively sending data packets to Facebook whenever patients logged in to schedule an appointment. Pixels, which are typically no more than a few lines of code, are used by social media companies like Facebook, Google, and Tiktok in order to quantify user traffic between their platforms and third-party sites. Additionally, pixels can record user activity, and pass this information back to the social media company. They can be used by healthcare organizations to target "lookalike" consumers as well as to rate the effectiveness of current advertising and conversion campaigns. While healthcare organizations are employing techniques to prevent consumer

emails and phone numbers from being linked to health data -- such as scrambling identifying data ("hashing") and/or inserting a string of random characters to obscure a user's identity ("salting") to protect patient privacy -- these efforts are routinely undermined by tech companies using algorithms that can work through de-identified data to learn as much as possible about individual users, and in the process connect consumers back to their individual data. Since social media companies are not subject to HIPAA, the sector is a frontier of enormous vulnerability for personal medical data. Of note, the California Consumer Privacy Act (CCPA) imposed requirements only on the "sale" of personal information; the new California Privacy Rights Act (CPRA) closes a legal gap by extending its overage to "sharing" of personal information.

3. Health Data or Consumer Data?

Beyond the issue of large social media platforms using third party identifiers to track clients and reconnect them to their health information, concerns are also growing more broadly with a general blurring of the lines between consumer information generally and health data. Consumers are often voluntarily providing all sorts of health information on different platforms -- a growing number of websites and smart phone applications that provide consumer services -- without any recognition by the receiving organizations that such data represents sensitive health information, let alone any commitment to health privacy protections. Examples of vulnerable information:

- Browsers (Google, Bing) for example, can collect and store information about a user's search history, which could potentially be used to identify individuals seeking information about health conditions or sensitive medical procedures.
- Posts in public online forums (Instagram, Facebook, may also be exposed to massive data mining, i.e. Cambridge Analytica 2016 scandal.) as individuals may unknowingly share personal and sensitive information on social media platforms, which could be used to identify them as individuals seeking abortions or other sensitive medical procedures.
- Personal Chat without end-to-end encryption can be intercepted and turned over with a valid warrant. (FB Messages used in Nebraska Abortion Case)
- Location tracking (Apple, FB, Cellphone providers, and countless apps) can reveal an individual's whereabouts, and used to place them at an abortion provider.
- Apps used to store health information or track a menstrual cycle for personal use, are not protected unless provided by a covered entity or its "business associate." These apps may not be subject to HIPAA regulations, leaving user's personal health information vulnerable to misuse or abuse.
- Wearable devices (*e.g.* Apple Watch, Fitbit) are not protected by HIPAA, whereas devices worn to supply info to covered entities are likely subject to HIPPA.
- Cloud storage (AWS, IBM Cloud, Azure) also may not be protected by HIPAA, leaving user's personal health information vulnerable to misuse or abuse.

- Voice assistants (Siri, Alexa) may not be protected by HIPAA, leaving user's personal health information vulnerable to misuse or abuse.
- ChatGPT: As a machine learning model it improves through data collection. Already there are numerous GPT apps (i.e. email assistants, document creation support, etc.). Stored data is not protected by HIPAA, potentially leaving user's personal health information vulnerable to misuse or abuse.
- Data brokers collect data across services and platforms, de-anonymize the data, and link it to specific users using a variety of methods. The sector is largely unregulated. (CRS Report)
- PHI on public facing websites. (Using Pixels, intake form data is sent to third-parties, such as Facebook or Tiktok without consumer authorization.)

As noted above, part of the challenge is that HIPAA relies upon a narrow definition of "covered entity" that is triggered by the submission of electronic claims for health insurance, and does not apply to direct-to-consumer services for which consumers pay directly. Similarly, state health privacy laws have tended to focus more narrowly on information in medical contexts, and not on the broader issue of health information being exchanged in consumer contexts.

4. Why Does My Therapist Sound Like a Robot? In December 2022, Koko, a behavioral health non-profit that uses AI to help spot individuals at risk of self-harm, conducted an experiment using OpenAI's GPT-3 technology. Over the course of several weeks, around 4,000 people received responses from Koko that were partially or entirely written by artificial intelligence. Unwitting users, many of whom were struggling with depression, PTSD, or anxiety, rated messages composed by the AI as being significantly better than those written solely by humans. However, when Koko revealed to users that the messages were composed by a machine, satisfaction plummeted. Koko's co-founder, Robert Morris, noted that "simulated empathy feels weird, empty." The company's revelation led to criticism and accusations of unethical behavior, as users felt they had been tricked into participating in the experiment. The experiment suggests that AI involvement in behavioral healthcare is likely to remain, raising a series of legal challenges, including:

- The absence of a clear legal framework to protect privacy;
- AI continuity of care requirements for verbatim preservation of sensitive chat conversations, entailing massive potential exposure to health data breach;
- Questions about machine learning platforms infringing on the territory of licensed health professions;
- Malpractice risk in scenarios where an AI provides inaccurate information or inadequate care; and
- Ethical concerns when individuals struggling with mental health challenges mistake the illusion of sentience for the real thing

5. Genomic Analytics The use of predictive health analytics, particularly in the area of cancer, has the potential to revolutionize the way medical professionals diagnose and treat

the disease. However, the use of genomically-derived data in these analytics raises important privacy concerns. Current health privacy were not designed specifically with genetic data in mind and may not provide adequate protection for this type of information. California has been among the states that have sought to address this regulatory gap by enacting legislation, such as CA's Genetic Information Privacy Act (GIPA), that would make biometric collection and storage more transparent. There remains a great deal of ambiguity around what constitutes "health data" when it comes to genetic information, such that sensitive information can be used and shared inappropriately. Lastly, in the realm of gene-based diagnostics or predictive analyses, dataset bias can lead to inferior outcomes when the medical statistics used to train AI models includes genomic information from one particular ethnicity or age range to the exclusion of others.

6. FTC. v. Kochava

On August 27, 2022, The Federal Trade Commission (FTC) filed suit against data broker Kochava Inc. for allegedly selling geolocation data from hundreds of millions of mobile devices. The data can be used to trace the movements of individuals to and from sensitive locations such as reproductive health clinics, places of worship, homeless shelters, and addiction recovery facilities. The FTC claims that by selling data tracking information, Kochava is enabling others to identify individuals and expose them to threats of stigma, stalking, discrimination, job loss, and even physical violence. The FTC's lawsuit seeks to halt Kochava's sale of sensitive geolocation data and require the company to delete the sensitive geolocation information it has collected. (Source FTC Press Release) The basis of the lawsuit is Section 5(a) of the FTC Act, 15 U.S.C. § 45(a)(n), which prohibits "unfair or deceptive acts or practices in or affecting commerce." Should the FTC prevail in court, there will be enormous repercussions for internet commerce and communication technologies.

Key Recent Developments in Health Privacy Law

- Title 42 CFR Part 2 governs certain Substance User Disorder Treatment Records. Enacted in the 1970s, it predates and is inconsistent with many HIPAA requirements (requiring additional protections that often get in the way of information sharing needed for care coordination. In **November 2022**, the Office of Civil Rights and the Substance Abuse and Mental Health Services Administration (SAMHSA) issued a Notice of Proposed Rulemaking (NPRM) that would align Part 2 and HIPAA, including:
    - Single patient consent for all future uses and disclosures of SUD records for treatment, payment, and healthcare operations.
    - Permitted to redisclose SUD records in accordance with the HIPAA Privacy Rule
    - Enable patients to obtain accounting of disclosures of SUD records and request restrictions on disclosures
    - Expansion of prohibitions on the use and disclosure of Part 2 records in civil, criminal, administrative, and legislative proceeding

- Part 2 programs must establish a complaints process about Part 2 violations and must not require patients to waive the right to file a complaint as a condition of providing treatment, enrollment, payment, or eligibility for services.
- The HHS will be able to impose civil money penalties for violations of Part 2, in line with HIPAA and HITECH.
- Final Rule expected in 2023.

- The Confidentiality of Medical Information Act (CMIA) is California's state health privacy law.
  - **AB 1184:** In July 2022, CMIA was amended to prohibit the disclosure of medical information related to sensitive services (mental or behavioral health, sexual and reproductive health, sexually transmitted infections, substance use disorder, gender-affirming care, and intimate partner violence). The amendment prohibits the disclosure of medical information to anyone other than the enrollee without the individual's express written authorization, including the policyholder or parent of a minor patient. Under the amendment, a patient can request "confidential communications" for all communications re: the individual's medical information and applies to communications that disclosure: (1) medical information; or (2) provider name and address related to receipt of medical services by the individual requesting the confidential communication.
  - **AB 2089:** In September 2022, CMIA was amended to include "mental health application information" in its new expanded definition of "medical information," and imposes additional obligations for businesses offering a mobile-based application or online "mental health digital service" to a consumer for the purpose of allowing the consumer to manage their own information, or for the diagnosis, treatment or management of a medical condition. AB 2089 creates a new disclosure obligation regarding data breaches for certain businesses, specifically, that any entity required to make a security breach notification pursuant to CCP § 1798.82 to more than 500 California residents as a result of a single breach of the security system must now electronically submit a single sample copy of that security breach notification (excluding personally identifiable information) to the Attorney General.

- The Genetic Information Privacy Act (effective 1/1/2022): GIPA requires Direct-to-Consumer companies to obtain a consumer's express consent for various uses, including:
  - Use of genetic data collected through a genetic testing product or service offered by the DTC Company. The consent must describe who has access to genetic data, how genetic data may be shared, and the specific purposes for which it will be collected, used, and disclosed.

- Storage of a consumer's biological sample after the consumer's initial testing has been completed.
- Each use of the consumer's genetic data or biological sample beyond uses associated with the primary purpose of the genetic testing or service.
- Each transfer or disclosure of the consumer's genetic data or biological sample to a third party other than to a service provider.
- Consent must include the name of the third party to which the consumer's genetic data or biological sample will be transferred or disclosed.
- Marketing directed towards a consumer based on the consumer's genetic data, or the company's facilitation of marketing by a third party based on the consumer's order, purchase, or use of a DTC Company's genetic testing product or service.
- Straightforward methods of revoking their consent to the actions listed above at any time

Harry Nelson is the co-founder and managing partner of Nelson Hardiman, LLP, a Los Angeles-based healthcare and life sciences law firm, where he advises on regulatory risks and strategy (including health data privacy and security), reimbursement, licensing, risk management and innovation issues, from structuring healthcare ventures to responding to crises. He is the author of The United States of Opioids: A Prescription for Liberating a Nation in Pain (2019), addressing solutions for the Opioid Crisis, and co-author of the From Obamacare to Trumpcare: Why You Should Care (2017), an analysis of the past, present, and future of U.S. health policy. Harry has served as an educator and advocate for improving the quality and safety of addiction treatment and behavioral health. He has also served in leadership roles in ventures related to healthcare investment, compliance, and e-learning.

hnelson@nelsonhardiman.com
www.nelsonhardiman.com
310.203.2800

- FTC Health Breach Notification Rule
  - https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-318

- FTC Mobile Health App Tool
  - https://www.ftc.gov/business-guidance/resources/mobile-health-apps-interactive-tool

- FTC – Flo Health Action and Consent Order
  - https://www.ftc.gov/system/files/documents/cases/192_3133_flo_health_complaint.pdf
  - https://www.ftc.gov/system/files/documents/cases/192_3133_flo_health_decision_and_order.pdf

- FTC – Kochava Complaint and FTC Press release
  - https://www.ftc.gov/system/files/ftc_gov/pdf/1.%20Complaint.pdf
  - https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other

- FTC – Good RX Action and Consent Order, with Consumer Reports article referenced by FTC:
  - https://www.ftc.gov/system/files/ftc_gov/pdf/goodrx_complaint_for_permanent_injunction_civil_penalties_and_other_relief.pdf
  - https://www.ftc.gov/system/files/ftc_gov/pdf/goodrx_stipulated_order_for_permanent_injunction_civil_penalty_judgment_and_other_relief.pdf
  - https://www.consumerreports.org/health-privacy/goodrx-saves-money-on-medsit-also-shares-data-with-google-facebook-and-others-a6177047589/

- Federal Court complaint regarding health care providers use of Meta Pixel violating various privacy laws
  - https://regmedia.co.uk/2022/06/20/meta_class_action_propsoed_suit.pdf

- HHS January 2023 report re Reproductive Health Care (which includes guidance for application of HIPAA in the wake of Dobbs Supreme Court decision)
  - https://www.hhs.gov/sites/default/files/roe-report.pdf

- HHS Guidance for health care providers in wake of Dobbs (July 2022)
  - https://www.cms.gov/files/document/faqs-part-54.pdf

- California Confidentiality of Medical Information Act (CMIA)
  - https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB2089 - 2022 Amendment to cover mental health application information
  - https://oag.ca.gov/news/press-releases/attorney-general-bonta-emphasizes-health-apps-legal-obligation-protect - California AG Emphasis about Health Apps Compliance with CMIA