Health Data Use for Marketing and Advertising: Privacy Risks and Patient Benefits

May 11, 2023

Nancy Perkins
Arnold & Porter

Melissa Goldstein
GW School of Public Health

Lyra Correa
Office for Civil Rights
U.S. Department of Health and Human Services

Tina Grande
Healthcare Leadership Council

Privacy+ Security Forum

HLC Confidentiality Coalition

Privacy + Security Forum

AdventHealth
Advocate Health
American Health Information Management Assoc.
America's Health Insurance Plans
American Hospital Association
American Pharmacists Association
American Society for Radiation Oncology
AmerisourceBergen
Amgen
AMN Healthcare
Anthem
Ascension
Association of American Medical Colleges
Association of Clinical Research Organizations
Augmedix
Bassett Healthcare Network
Baxter
Blue Cross Blue Shield Association
Blue Cross Blue Shield of North Carolina
Bristol Myers Squibb
Cardinal Health
CHIME
Cigna
City of Hope
College of American Pathologists
Connective Rx
Cotiviti
CVS Health
Datavant
Elevance
EMD Serono
Epic
Fairview Health Services
Federation of American Hospitals
Ferring Pharmaceuticals
Genentech
Genetic Alliance
Guardant Health
Healthcare Leadership Council
Intermountain Healthcare
IQVIA
Johnson & Johnson
Kaiser Permanente
Leidos
LifeScience Logistics
Marshfield Clinic Health System
Mayo Clinic
McKesson Corporation
Medical Group Management Association
Meharry Medical College
MemorialCare Health System
Merck
MetLife
Mount Sinai Health System
MRO
National Association of Chain Drug Stores
National Community Pharmacists
NewYork-Presbyterian Hospital
NorthShore University HealthSystem
Novartis Pharmaceuticals
Optum Insight
Oracle Health
Pfizer
Pharmaceutical Care Management Association
Premier
Senior Helpers
Stryker
Surescripts
Texas Health Resources
Tivity Health
United Health Group
Vizient
Wellvana
Workgroup for Electronic Data Interchange
ZS Associates

CONFIDENTIALITY COALITION

Overview of Key Issues

- What principles underlie the governance of outreach using personal health information?
- Who is regulating the use of personal health information for marketing purposes?
- What is “marketing” under laws that govern such use?
- Who benefits from marketing communications based on personal health information?
- What are the risks and how should they be addressed?

Underlying Principles

Privacy+ Security Forum

Right to Privacy

- Basic human right
- Negative and positive rights
  - Negative: right to be left alone
  - Positive: right to control access to information about yourself
- Right protected by common law, US Constitution, state constitutions

Ethical Justifications

- Grounded in principle of respect for autonomy and rule of fidelity
  - Respect for autonomy: consideration of an individual's capacity and desire for self-governance
  - Fidelity: promise keeping, loyalty, faithfulness in the health care provider-patient relationship

Health Information Privacy

- What is at stake? Unauthorized/erroneous disclosures
  - Embarrassment
  - Stigma
  - Discrimination in employment, insurance, government programs

Privacy and Health Generally

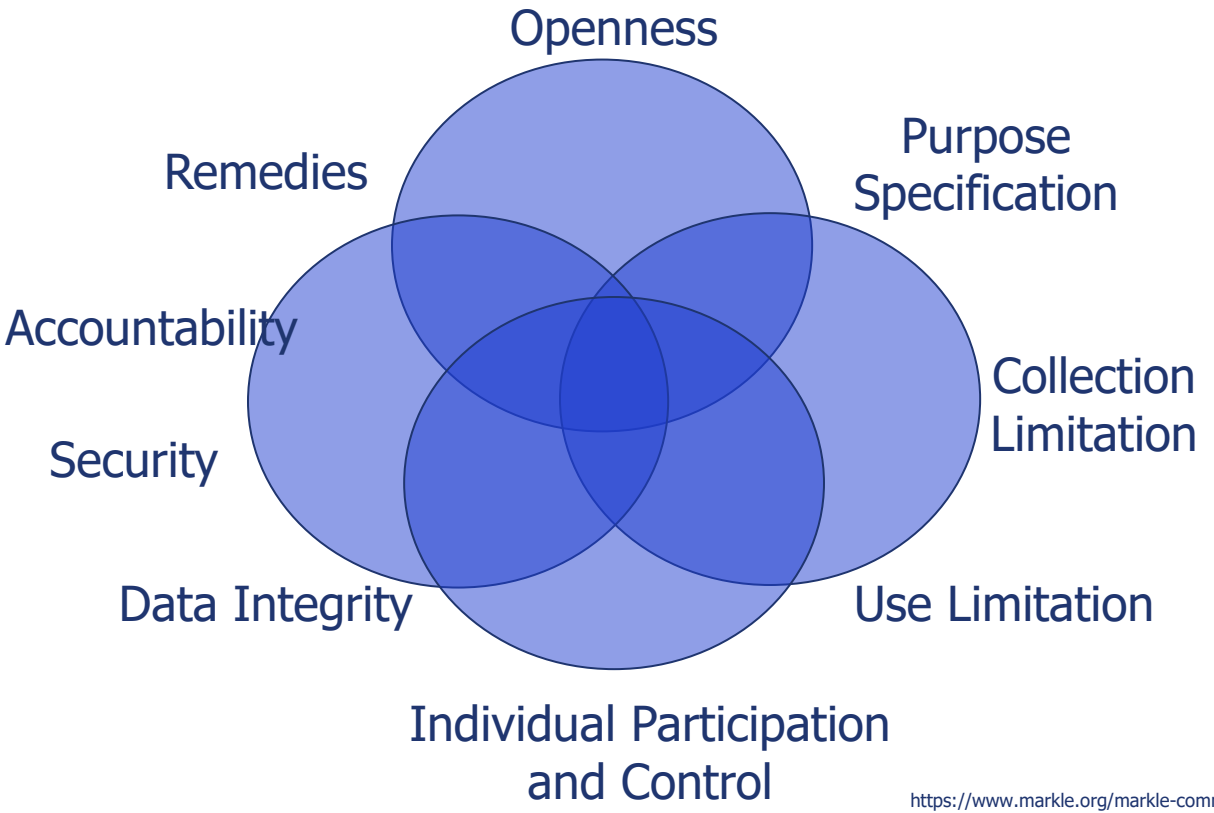
- Individuals' privacy must be balanced with the value of important uses of health information (*e.g.*, research, public health)
- Infringing too much on privacy could reduce people's willingness to seek medical care or to cooperate with public health authorities
- Demands systemized privacy protection (fair information practices) to mitigate risks and establish trust

Fair Information Practice Principles

Principle	Description
Transparency	Organizations should be transparent and notify individuals regarding collection, use, dissemination, and maintenance of personally identifiable information (PII).
Individual participation	Organizations should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. Organizations should also provide mechanisms for appropriate access, correction, and redress regarding use of PII.
Purpose specification	Organizations should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.
Data minimization	Organizations should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).
Use limitation	Organizations should use PII solely for the purpose(s) specified in the notice. Sharing PII should be for a purpose compatible with the purpose for which the PII was collected.
Data quality and integrity	Organizations should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.
Security	Organizations should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
Accountability and auditing	Organizations should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use

United States Department of Homeland Security. https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf

Privacy in a Networked Health Environment



https://www.markle.org/markle-common-framework-connecting-professionals

Regulatory Framework

Who is Regulating?

Privacy + Security Forum

STATES

EXEMPLARY STATES:

- California
- Texas
- Washington

DEPARTMENT OF HEALTH & HUMAN SERVICES (HHS)

- Health Insurance Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Health (HITECH) Act

FEDERAL COMMUNICATIONS COMMISSION (FCC)

- Telephone Consumer Protection Act (TCPA)

  (telemarketing, including text messaging)

FEDERAL TRADE COMMISSION (FTC)

- Section 5 of FTC Act
- Telemarketing and Consumer Fraud and Abuse Prevention Act
- Fair Credit Reporting Act

HIPAA Privacy Rule “Marketing” Prohibition

- Covered entities may not use protected health information (“PHI”) for marketing purposes without a written authorization from the individual to whom the information pertains.
  - Exception for face-to-face communications
- “Marketing”:

  > “making a communication about a product or service that encourages recipients to purchase or use the product or service”

Exclusions from “Marketing” Definition

- It is NOT “marketing” if:
  - A health care provider communicates with a patient for treatment purposes, including to recommend alternative treatments and therapies
  - A health plan communicates with plan beneficiaries about products/services available under the plan
  - A covered entity contacts patients with information about treatment alternatives for case management/care coordination

  BUT ONLY if there is no remuneration for making the communication
- Refill reminders may be made with remuneration *at cost*

CA Confidentiality of Medical Information Act

- "Marketing" means "to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service."
- "Marketing" does ***not*** include:
  - Communications for which the communicator does not receive direct or indirect remuneration from a third party for making the communication
  - Communications current health plan enrollees about products or services covered by the plan or describing the availability of more cost-effective pharmaceuticals
  - Communications tailored to the circumstances of a particular individual to educate or advise the individual about treatment options, and otherwise maintain the individual's adherence to a prescribed course of medical treatment

Telephone Consumer Protection Act

- "Telemarketing":
  - Initiating a telephone call or message to encourage the purchase of property, goods, or services
- Any telemarketing calls using a prerecorded message or artificial voice, and any autodialed telemarketing calls to cell phones, require *prior express **written** consent.*
- Limited exceptions for:
  - Emergency calls
  - Calls by tax-exempt nonprofits
  - Certain HIPAA-covered health care calls

FCC HIPAA-Related Exemption

- In recognition of the exemption of "health care management/treatment" communications from the HIPAA Privacy Rule's requirement for an authorization to make marketing communications, the FCC decided to give special leeway for certain calls that:
  - describe a health-related product or service
    AND
  - are made by a HIPAA covered entity or business associate.

- There are nuances and those create significant risk

Conditions for “Healthcare” Calls/Text Messages

- Must be from a HIPAA covered health care provider or its business associate
- Must provide a “treatment” message
- Must be free to the recipient of the call (typically a patient)
- Must be made only to the number provided by the patient
- Must state the name and contact information for the provider
- Must be concise
  - Cannot exceed 1 minute (call) or 160 characters (text message)
- Must be infrequent
  - One call per day / three per week
- Must include an easy means to opt out
- Opt-out requests must be honored immediately.

Health Plan Calls/Text Messages

- Health plans did not get the same exemption
- This led to concerns about liability for MCOs that assist states with Medicaid enrollment
- Unwinding of PHE and Medicaid re-determination
- CMS urged FCC to provide exemption; FCC responded:
  - "Enrollee's provision of phone number on Medicaid application constitutes prior express consent to be contacted at that number regarding enrollment eligibility because the purpose of those texts is related to the purpose for which the enrollees provided their numbers."

Online Health Data Uses: Regulation and Enforcement

Privacy+ Security Forum

FTC Act Enforcement: 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."

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

CMIA Enforcement: Glow Case

- Glow 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 found Glow violated the CMIA by sharing users' sensitive health information without authorization; settlement in 2020

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.

BetterHelp Consent Order (2023)

- Monetary penalty: $7.8 Million
- Injunctive relief -- BetterHelp must:
  - cease sharing 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

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

Online Tracking Technologies & HIPAA

- In December 2022, OCR released a bulletin highlighting the obligations of covered entities and business associates under HIPAA when using online tracking technologies
- Bulletin addresses:
  - What is a tracking technology
  - How do the HIPAA Rules apply
  - HIPAA compliance obligations
  - Resources

What are tracking technologies?

- A script or code used to gather information about users as they interact with a website or mobile app.
- Script or code is not readily apparent to website or app users.
- Tracking technologies on websites: cookies, web beacons or tracking pixels, session replay scripts, and fingerprinting scripts.
- Tracking technologies on mobile apps: a tracking code is embedded within the app to collect information provided by the user and a user's mobile device-related information.

Third party tracking technologies

- Tracking technologies developed by third parties:
  - Send information directly to the third parties who developed such technologies
  - May continue to track users and gather information about them even after they navigate away from the original website to other websites.
- There is a risk information may be sold or disclosed to other third parties and used to promote misinformation, identity theft, stalking, or harassment

When do the HIPAA Rules apply?

- Is a HIPAA covered entity or business associate using tracking technologies?
  - Tracking technology vendors are HIPAA business associates if they create, receive, maintain, or transmit PHI on behalf of a regulated entity for a covered function (e.g., health care operations) or provide certain services to or for a covered entity (or another business associate) that involve the disclosure of PHI
- Is protected health information being disclosed through the tracking technology?
  - Ex: IP Address, dates of appointments, other identifying information that the individual provides when interacting with the webpage or app

How do the HIPAA Rules apply?

- Bulletin addresses how the HIPAA Rules apply to:
  - Tracking on user-authenticated webpages
  - Tracking on unauthenticated webpages
  - Tracking within mobile apps

Compliance Obligations

- Examples include:
  - Ensuring all disclosures of PHI are specifically permitted by the Privacy Rule
  - Putting a business associate agreement in place if vendor meets the definition of business associate
  - Addressing use of tracking technologies in Security Rule risk analysis and risk management processes
  - Providing notification in the case of breach of unsecured PHI

Looking Forward: Policy Decisions

Privacy+ Security Forum

Emerging State Health Data Privacy Laws

- **New Washington State "My Health Data Act"**
  - Could presage new wave of state health data-specific privacy regulation
- As of March 31, 2024, applies to any legal entity that:
  - conducts business in Washington *or* produces/provides products or services that are targeted to consumers in the state, and
  - alone or with others determines the purpose and means of processing "consumer health data."
- *Consumer health data*: PI that "identifies a consumer's past, present, or future physical or mental health status."
  - *Consumer*: Washington state resident *or* a person whose consumer health data is collected in the state.
- Requires explicit consent to collect or share consumer health data other than as needed to provide a requested product or service to the consumer
- Prohibits "geofencing" (creating a virtual boundary around) an entity that provides in-person health care if the geofence is used to:
  - Identify or track consumers seeking health care services;
  - collect consumer health data from consumers; or
  - send notifications, messages, or advertisements to consumers related to their consumer health data or health care services.

FTC Anticipated Privacy and Security Regulations

- August 2022: FTC published Advance Notice of Proposed Rulemaking on "Commercial Surveillance" and Data Security.
  - "Commercial surveillance": the collection, aggregation, analysis, retention, transfer, or monetization of consumer data and the direct derivatives of that information."
- Sought input on questions such as:
  - Should the FTC limit healthcare companies from engaging in any specific commercial surveillance practices like personalized or targeted advertising?
    - If so, how?
    - What would the relative costs and benefits of such a rule be, given that consumers generally pay zero dollars for services that are financed through advertising?
  - To what alternative advertising practices, if any, would companies turn in the event new rules somehow limit first- or third-party targeting?

FTC and Congress

- **FTC FY 2024 budget request to Congress**
  - $160 million increase from FY 2023
  - Additional FTEs for the Office of the Chief Privacy Officer to support increased workload
  - Strengthen ability to take on bigger and more complex cases related to health privacy

- **Statement of justification:**
  - “Additional staff will allow the agency to investigate and litigate more and increasingly complex matters, such as those involving health privacy.”

Congressional Proposals

- **American Data Privacy and Protection Act (ADPPA) – H.R. 8152**
  - Comprehensive federal consumer privacy framework - addresses state preemption and private right of action
  - Bipartisan, Bicameral
  - Passed full committee on House side 53-2
  - Waiting on the Senate…

- **UPHOLD Act, S. 631 – March 2023**
  - Sponsors: Amy Klobuchar (D-MN), Elizabeth Warren (D-MA), Mazie Hirono (D-HI)
  - Prevent companies from monetizing identifiable health data for advertising purposes
    - Bans use of data collected from any source, including data from users, medical centers, wearable fitness trackers, and web browsing histories
  - Allow consumers greater access to and ownership of their personal health information
  - Restrict companies' ability to collect/use information about personal health without consent
  - Ban data brokers from selling location data

Congressional Concern About Health Data Use

- **Senators' letters to Cerebral, Monument and Workit Health – February 2023**
  - Cantwell (D-WA), Collins (R-ME), Klobuchar (D-MN), Lummis (R-WY)
  - Letters to CEOs expressing concern over tracking and sharing of customers' identifiable health data with social media platforms for advertising
- **Stop Commercial Use of Health Data Act, S.4738 – August 2022**
  - Amy Klobuchar (D-MN) and Sheldon Whitehouse (D-RI)
  - Restrict companies from monetizing identifiable health data for advertising purposes

Consideration of Patient Benefits and Risks

- **Online Activity**
  - Monitoring social media sites
  - Participating in patient advocacy groups
  - Tracking patient online queries
- **Clinical trial recruitment**
  - Study subject selection
  - Rare disease populations
- **Targeted Treatment or Cost-Coverage Information**
  - Medicaid redetermination
  - Availability of patient support programs
  - Options for co-pay prescription drug coverage
  - Locations of nearby clinics

Nancy L. Perkins

Arnold & Porter
Nancy.Perkins@arnoldporter.com
(202) 942-5065

Tina Grande

Healthcare Leadership Council
tgrande@hlc.org
(202) 452-8700

Melissa Goldstein

Milken Institute School of Public Health
mgoldste@gwu.edu
(202) 994-4235

Lyra Correa

Office for Civil Rights
Department of Health and Human Services
Lyra.Correa@hhs.gov
(800) 368-1019