Rethinking Patient Data Privacy In The Era Of Digital Health

January 2020
National Academy of Medicine

Daniel P. O'Neill

@dp_oneill

dponeill.com

Background / conflicts

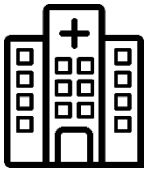
- 10+ years in health care technology and services, including:
  - Population health analytics
  - Ambulatory EHR vendor
  - Claims clearinghouse
- 2018 – 2019 RWJF Health Policy Fellow
  - Senate HELP Committee staff
- Co-author (with Lisa Bari):
  - *"Rethinking Patient Data Privacy In The Era Of Digital Health" (Health Affairs, December 2019)*

- No current conflicts

Agenda

1. What is happening
2. Why this is happening
3. Where we go from here

Traditional providers sharing data – at scale – with tech firms with checkered privacy record



BUSINESS | HEALTH CARE | HEALTH

Hospitals Give Tech Giants Access to Detailed Medical Records

Deals with Microsoft, IBM and Google reveal the power medical providers have in deciding how patients' sensitive health data is shared

Hospitals have granted Microsoft Corp
Machines Corp. and Amazon.com Inc.
patient information under deals to cru

◆ WSJ NEWS EXCLUSIVE | TECH

Google's 'Project Nightingale' Gathers Personal Health Data on Millions of Americans

Search giant is amassing health records from Ascension facilities in 21 states; patients not yet informed

Google is engaged with one of the U.S.'s largest health-care systems on a project to collect and crunch the detailed personal-health information of millions of people across 21 states.

The initiative, code-named "Project Nightingale," appears to be the biggest effort yet by a Silicon Valley giant to gain a toehold in the

"The data belongs to whoever has it."

-- Lisa Bari

Consumer health tools using patient health data to build enterprise businesses

Technology

Is your pregnancy app sharing your intimate data with your boss?

As apps to help moms monitor their health proliferate, employers and insurers pay to keep tabs on the vast and valuable data

By **Drew Harwell**
April 10, 2019

Like millions of women, Diana Diller was a devoted user of the pregnancy-tracking app Ovia, logging in every night to record new details on a screen asking about her bodily functions, sex drive, medications and mood. When she gave birth last spring, she used the app to chart her baby's first online medical data — including her name, her location and whether there had been any complications — before leaving the hospital's recovery room.

But someone else was regularly checking in, too: her employer, which paid to gain access to the intimate details of its workers' personal lives, from their trying-to-conceive months to early motherhood. Diller's bosses could look up aggregate data on how many workers using Ovia's

"…paid to gain access to…aggregate data on how many workers using Ovia's apps had faced high-risk pregnancies or gave birth prematurely… and how soon the new moms planned to return to work."

EHR vendors blur the lines between patient- and provider-controlled data to build advertising businesses

How private is your health data on "patient portal" websites used by hospitals and doctors' offices?

It's not as private as you might hope, despite a federal law known as HIPAA, short for the Health Insurance Portability and Accountability Act.

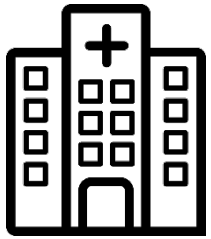
A reader from Silver Spring, Md., who asked me not to use her name, emailed me after reading the privacy policy in an external website used by her doctors at George Washington University Medical Faculty Associates. The patient portal FollowMyHealth.com reserves rights to use "personal health record" data for "marketing and advertising purposes, including sending you marketing and advertising communications whether on our behalf or on behalf of marketing partners."

When I contacted Follow My Health's corporate parent Allscripts, it painted a narrower picture of its practices — and claimed the site wasn't limited by HIPAA.

Tom Lynch, the company's director of marketing communications, said the site is "not disclosing identifiable patient data to third parties for any marketing purpose" — even though its privacy policy specifically reserves the right to "release" personal health data for marketing and advertising. (That policy was updated in August.)

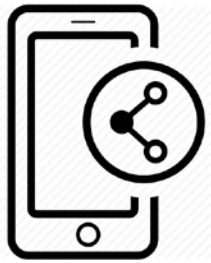
"…using 'information about patients to alert them to certain goods and services…'"

Recap: For good or ill, more patient data is flowing across organizational & regulatory boundaries



Traditional **healthcare providers** (aka HIPAA covered entities) are pursuing business opportunities which rely on patient data, often in partnership with non-traditional actors

- Generally in aggregated, de-identified form



Digital health services (not covered entities) are collecting data directly from consumers, but then using it to build new revenue streams from employers, insurers, drugmakers etc

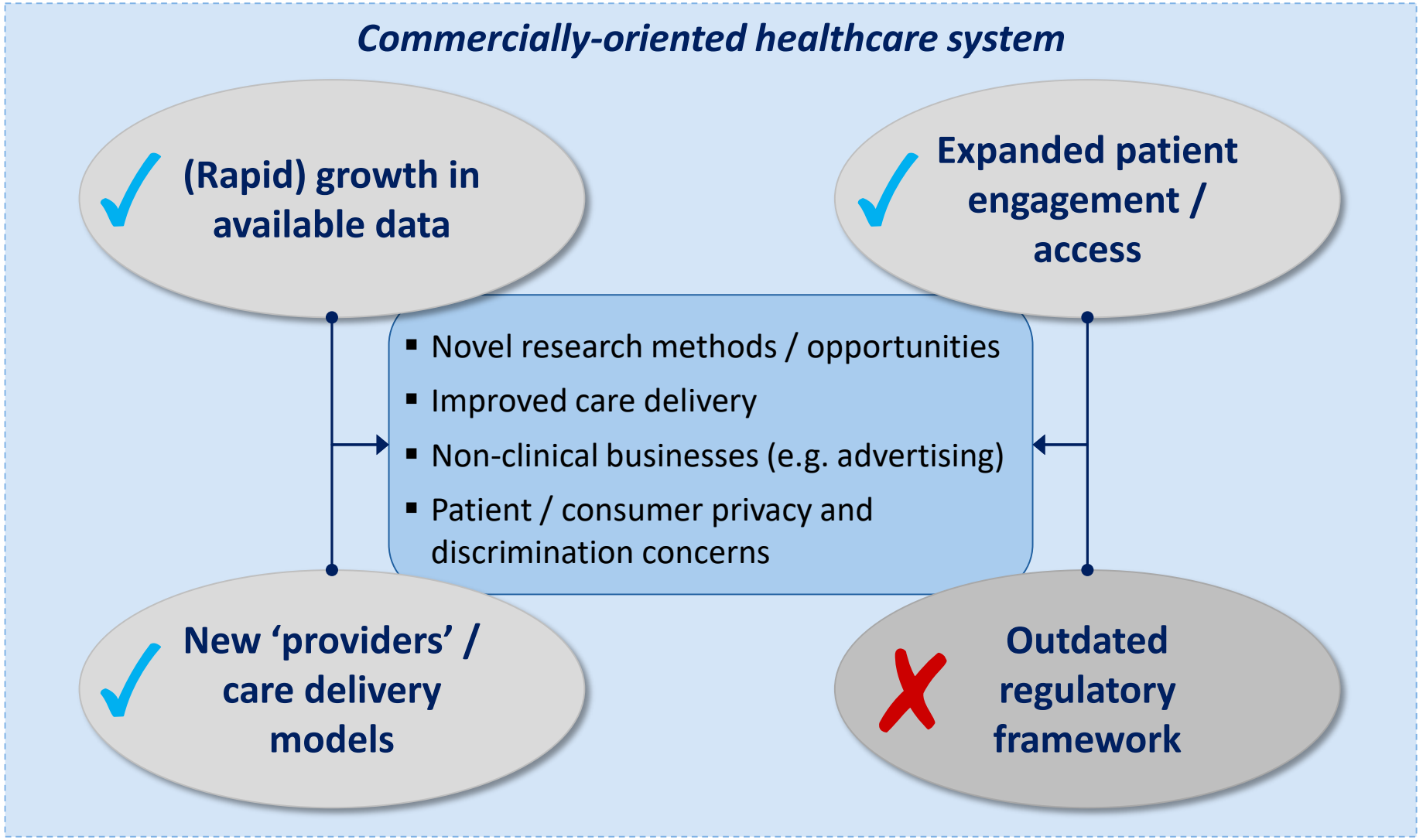
Electronic health records (aka HIPAA business associates) are working to shift health data from a provider-controlled to a patient-directed regulatory regime, to open up new business opportunities


"In the future, everyone
will want to be anonymous
for fifteen minutes." Bankzy

Agenda

1. What is happening
2. Why this is happening
3. Where we go from here

Digital health brings opportunities for research and care delivery, but with acute privacy risks



HIPAA's data protections revolve around entities, not the data itself

HIPAA's conceptual structure (simplified!)

1. **Establish a list of "Covered entities"**
   - Providers (hospitals, physician practices, etc)
   - Health plans (insurers and ERISA plans)
   - Clearinghouses

2. **Define a category of data**
   - Individually identifiable health information (IIHI)
   - "information…that relates to the individual's past, present or future physical or mental health…the provision of health care to the individual, or… payment for the provision of health care to the individual"

3. **Assign data protection obligations to those entities**
   - Conditions for sharing or disclosure ("payment, treatment or operations," "minimum necessary" etc)
   - Patient access rights (often ignored)
   - Breach notification & security rules

Siloed HIPAA framework opens door to regulatory arbitrage and the erosion of public trust

Not an exhaustive list

Shift the source → Change the rules

Given HIPAA's entity orientation, data collected from a patient (or derived from patient-sourced data) lacks equivalent privacy and security protections

Shift "control" → Change the rules

Provider-sourced clinical data shifted to patient's control can free the data (and the entity that holds the data) from HIPAA protections and access rights

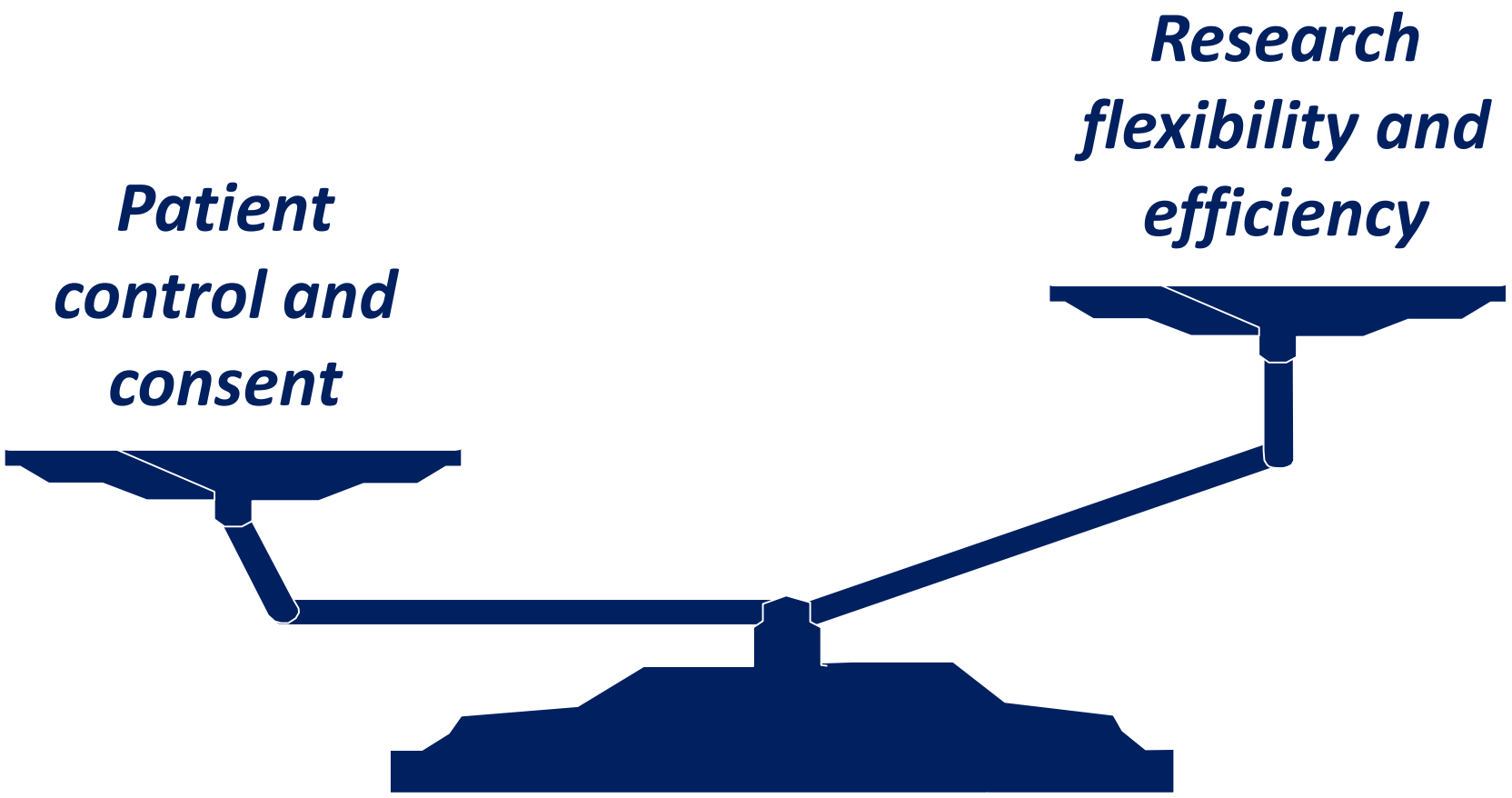
"De-identify" → Change the rules

De-identified data is no longer deemed "individually identifiable," hence is not "protected" and hence no longer subject to the same protections and consent requirements

Money in ~~politics~~ healthcare is like water on pavement…
…It finds every crack and crevice.

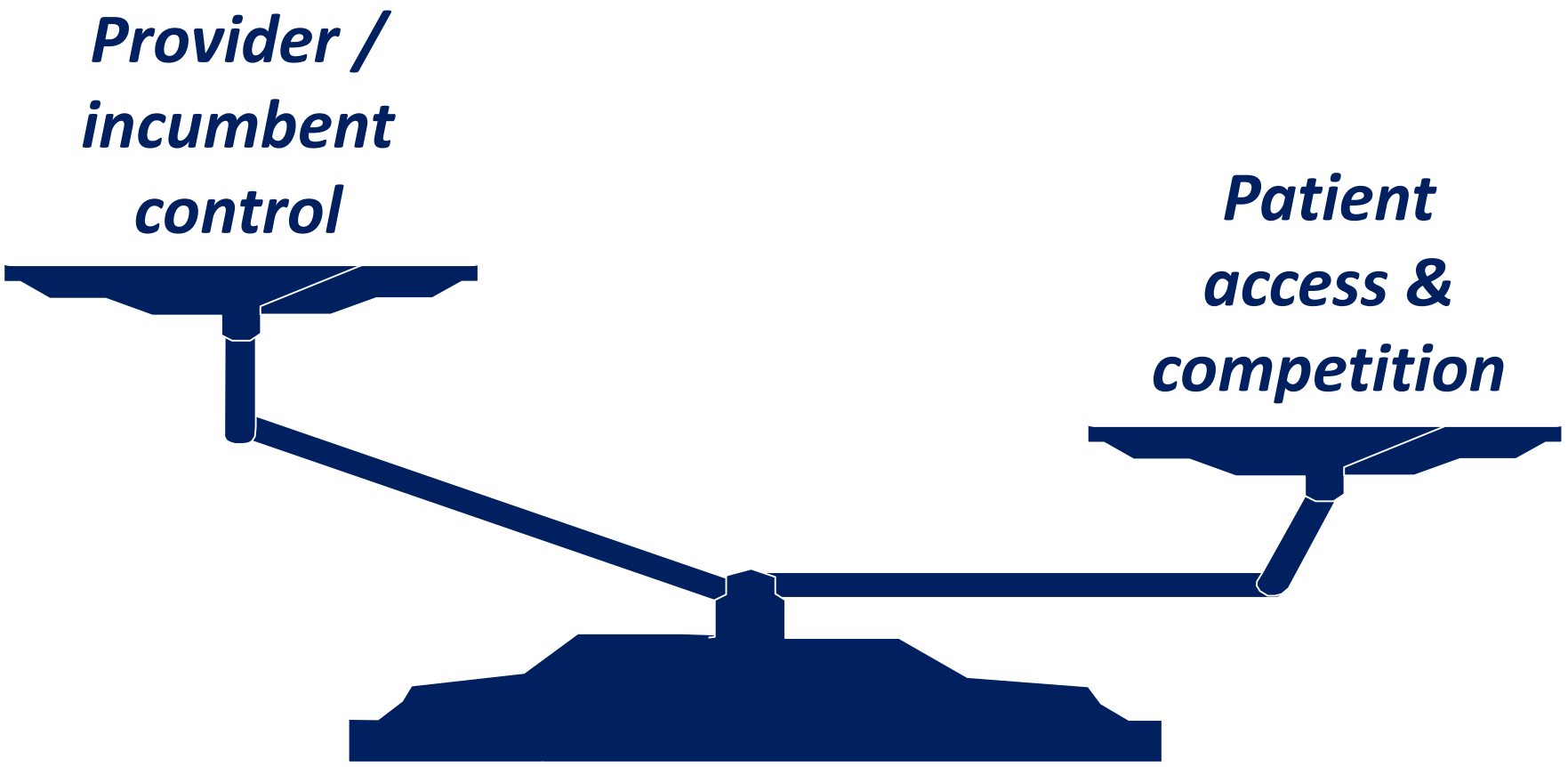
Some of these exploitable “loopholes” also serve systemic goals with clear social benefit

Example:



Meanwhile, some providers lean on “privacy” to serve business objectives at variance with patient interests

Example:



Agenda

1. What is happening
2. Why this is happening
3. Where we go from here

“…Adapt and extend the familiar HIPAA framework, and some of the fiduciary principles embedded in that framework, for a new era of digital-first health care.”

Contrast with more recent privacy law – GDPR & CCPA – highlights HIPAA gaps

	HIPAA (current)	GDPR	Adapted / extended HIPAA (proposed)
Health data in scope	Individually identifiable health information (IIHI), relating to individual health (physical or mental), provision of care or payment for provision of care, *when that IIHI is held or transmitted by a covered entity or its business associate*	"Personal data" which includes direct or indirect identifiers and "expresses the physical, physiological, genetic, mental, commercial, cultural or social identity" individuals. Health data is a special category with heightened protection.	IIHI relating to an individual health (physical or mental), provision of care, or payment for provision of care, regardless of who collects, holds, processes or transmits that data
Regulated entities	*Covered entities (CEs)* – Health plans, health care providers and health care clearinghouses *Business associates* – person or organization performing functions on behalf of (or providing services to) a CE	*Controller* – Any person or organization which determines the purposes or means of processing personal data *Processor* – person or organization processing data on behalf of controller	*Custodian* – Any person or organization collecting or holding IIHI, or controlling the processing thereof *Processor* – person or organization processing data on behalf of custodian
Permitted uses of personal health data	Health care treatment, payment and operations	Treatment, public health, research, judicial proceedings, substantial public interest, by informed consent, or when processing is in the "vital interests" of person unable to consent	Health care treatment, payment and operations, regardless of the entities involved in those activities, when appropriately disclosed to the individual. All other uses require consent.
Security standards	✓	✓	✓
Breach notification requirements	✓	✓	✓
Individual right to: Access | Amend | Delete	✓ | ✓ | ✗	✓ | ✓ | ✓	✓ | ✓ | ✓

Source: Author summary, based in part on information from The U.S. Department of Health and Human Services (https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html), GDPR text available from Intersoft Consulting (https://gdpr-info.eu/) and analysis by Laura Jehl and Alan Friel of Baker Hostetler LLP (https://www.bakerlaw.com/webfiles/Privacy/2018/Articles/CCPA-GDPR-Chart.pdf) and Pathak et al of Microsoft and Polsinelli P.C. (http://download.microsoft.com/download/B/B/F/BBFC0412-E610-49D9-AF83-D76DE35259F7/GDPR_Implementation_and_HIPAA_Compliance_EN_US.pdf)

Five key steps to modernize HIPAA for the era of digital health

1. Define **individually-identifiable health information (IIHI) as an inherently protected class of data**, regardless of who holds or processes the data

2. Create new definitions of IIHI **"custodians" and "processors"** – analogous to (but broader than) HIPAA's covered entities and business associates

3. Establish **individuals' right to access, amend and delete** IIHI, and to consent to or decline participation in aggregated data sets

4. Codify **permitted uses** of IIHI, rooted in fiduciary principle

5. Specific parameters for **consumer-friendly and revocable consent**, for any use or disclosure beyond narrow permitted uses

Discussion