Privacy of Digital Health Information

Amalia R. Miller (University of Virginia)

NBER Privacy Tutorial

October 14, 2022

The challenge

- Increased adoption and application of IT (inside and outside of healthcare provision) has generated unprecedented volume of digital records related to individual health that is controlled by companies
- The promise of these data and tools is immense, but unfettered access puts individual privacy in peril

- Is it possible to harness digital technology and data analytics in healthcare and still preserve privacy?
- What kind of policies do governments use to help preserve privacy while still reaping benefits of digitization? What are their effects?

This session

Goal is to raise conceptual and practical questions, motivate you to apply economic research methods to study health privacy.

1. How is health privacy special?
    - Theoretical costs and benefits of keeping health data private
    - Compare to other types of individual data
2. Can private markets allocate health privacy efficiently?
3. Regulating health privacy: key parameters
4. Regulating health privacy: empirical effects

1. How is health privacy special?

Special privacy rules for health

- Health information is subject to specific federal and state laws
- Key federal laws protecting health information:

1. 1996 Health Insurance Portability and Accountability Act (HIPAA)
    - Privacy Rule (45 CFR Parts 160 and 164, April 2003)
2. 2009 Health IT for Economic and Clinical Health (HITECH) Act
    - Created the Health Breach Notification Rule
3. Genetic Information Nondiscrimination Act of 2008 (GINA)

[*Also note*: 1978 Pregnancy Discrimination Act; 1990 ADA; 2010 ACA; 2016 Cures Act; 2021 proposed COVID-19 Public Health Emergency Privacy Act.]

Why stricter rules for health?

- Role for professional norms (Hippocratic Oath includes privacy) and policy context (healthcare is among most regulated sectors), but:
- Let’s take an economic perspective, consider costs and benefits
    - Think about *tradeoffs* instead of absolute *principles*
- Start by thinking of “health” information broadly, then get into categories later
- To be concrete, let’s consider: any piece of personal information that, on its own, or in combination with other information, can reveal something about your health status, medical diagnoses and conditions, medical care utilization and treatments, or health risk factors

Potential harms from lost (health) privacy?

Which are specific to (or higher for) (certain kinds of) health information?

Measuring harms from lost health privacy

- We know a little, but not much. It is complicated because:
- Can include both *direct* (primary, intrinsic) and *indirect* (secondary, instrumental) elements
- Some parts are subjective, based on preferences
  - No single unified theory of privacy; value depends in part on subjective, context-specific, contingent aspects (Acquisiti et al. 2016, 2015)
  - Intrinsic value of privacy low on average, but highly variable (Lin 2022)
- Even objective parts are contingent, depend on the category and content of the information, the subject and recipient, their situation, other information available them
- Harm primarily limited to subject of data, but spillovers possible

Benefits of health information use

- If respecting privacy means *not* collecting, storing, sharing, using health data, the cost of privacy is the foregone health data use
- Potential benefits are immense, across range of settings and uses.
- Digital health data can improve:
  - Healthcare delivery operations, processes (decision support), and incentives
  - Public health surveillance and operations (e.g., contact tracing, quarantine)
  - Medical and public health research and development
  - Development and administration of tailored (personalized/precision) treatments
  - Applications/devices for monitoring, managing health conditions or wellbeing
  - Targeted advertising – informative, useful

Distribution of benefits from health data use

- Private benefits to *individuals* whose data is being used and *companies* who collect, sell, use data
  - Impact of IT adoption on individual or firm outcomes (Bronsoler et al. 2022)
- External/social benefits (network effects, public health, research, innovation)
  - Personalized medicine (Miller and Tucker 2017); AI healthcare (Sanders et al. 2019, Yu et al. 2018, Bates and Syrowatka 2022)
- If privacy is about ownership (not just harm), then people might want to share in profit from sale, use of data *about them*
  - Can private markets for health data resolve privacy tradeoffs?

2. Can private markets allocate health privacy efficiently?

Market mechanisms for privacy allocation

- In principle, price mechanism and/or Coase-style private bargaining could resolve conflicts about optimal privacy of consumers and businesses – people pay to keep privacy or are paid for sharing data
- Similar for data security – people pay for safety or are paid for accepting risk or loss

But there are difficulties:

- With uncertain or unenforceable rights, how to trade over privacy?
- What about information limitations? Transaction costs? Spillovers?

Health privacy market failures

- Absent clear rules, property rights over health data are ambiguous
- Consumers may not be aware of privacy choices or understand impacts
  - Many consumers not well-equipped to understand and decide on privacy risks, which are complex, uncertain, and distant
- Transaction costs for individualized privacy agreements can be high
  - Set of privacy options can be limited by companies, foreclosing options
  - Companies with data not be limited to "first line" providers interacting with consumers
- Opacity and asymmetric information about data activity and uses hamper contracting and private enforcement of privacy agreements
- Data sharing can create *negative* spillovers when information is also about friends, coworkers, family members; *positive* spillovers from research

Role for public policy in health privacy

- Provide information, education about privacy to consumers
- Mandate information provision, disclosure by companies about privacy practices, events
- Assign clear property rights over personal health data to individuals or companies
- Enforce property rights through administrative agencies, courts
- Require that companies adopt certain technologies, practices in data collection, storage, transmission, use
- Restrict companies to prevent certain data uses, practices
- Encourage, enable public health and research uses of data

Privacy preferences and paternalism

- If people are not able to make informed choices about privacy, then (the right) government restrictions can improve outcomes
- But significant variation in individual preferences for privacy (e.g., Lin 2022) presents difficulty with setting universal privacy policy
- Government policy that severely restricts options for private market contracting may preclude efficient contracts that would be preferred by consumers and businesses
- Variation in privacy preferences also suggests distributional effects from privacy rules – could help people with high tastes but hurt those who prefer to trade information for better prices, tools, convenience

Health privacy and discrimination

- Privacy rules that limit flow or use of information to a market intersect with Civil Rights anti-discrimination law
    - e.g., GINA; ACA ban on pre-existing conditions; pregnancy discrimination act
- These rules have *distributional* effects (*ex post*) and insurance effects (*ex ante*)
    - Distributional effects can diverge across consumers; blocking information improves market access for people with risk factors but raises prices others.
    - Could serve social insurance goal of helping people with negative shocks
    - Could harm efficiency by increasing info asymmetry -> adverse selection -> lemons problem
- *Also*: blocking specific types of info could increase use of proxies

Aside: privacy from government

- Our focus is on companies, but government operations also involve vast amounts of data on citizens, residents, businesses; including health data from insurance programs, health systems, regulatory enforcement
- People want privacy, confidentiality and security from government too
- Government agencies bound by HIPAA for healthcare data
- Federal agencies also covered by federal Privacy Act (1974), not specific to health

3. Regulating health privacy: key parameters

Parameters of health privacy policy

Health privacy rules need to set some key parameters:

1. What counts as health information?
2. What counts as sensitive health information?
3. What counts as personal information?
4. What entities should be covered (type of business, relationship to consumer)?
5. What uses, practices should be covered, proscribed, or mandated?
6. What penalties for violations, enforcement mechanisms?

Health privacy protection from other rules

- Significant gaps in coverage of health privacy under federal rules
- State health privacy rules can exceed the floor set by federal law
- State privacy rules that are not focused on health generally include health data
- Absent a federal data privacy rule, FTC relies on other consumer protection rules (deception, fraud) for privacy cases
- Other uses of health-related data fall outside of regulation

4. Regulating health privacy: empirical effects

Privacy and electronic medical records (EMRs)

- Miller and Tucker (2009) asks if legal protection of health data increases or decreases adoption of digital health records at US hospitals
- Does legal reassurance increase willingness of patients to share data? Or do restrictions on data flow reduce the value of digitization?
- We find the latter; hospitals usually increase adoption in response to adoption by other local hospitals, but this is eliminated by strict privacy laws
- Miller and Tucker (2011) replicates this over longer time period and further shows cost of delayed EMR adoption: higher infant mortality

Health data security and encryption

- Miller and Tucker (2011) studies health data security and breaches.
- Show greater digitization increases loss of patient data
- Show increased use of encryption (overall or induced by state data breach notification rules that exempt encrypted data) does not decrease publicized data loss
- Instead, encryption increases loss from internal fraud and lost equipment
- Highlights challenge in data security policy and practice – human element is key; focus on technological can undermine it

Information blocking: access to records

- Privacy laws aim at empowering individuals; not always about reducing information flow
- Jones and Tonetti (2020) argue that giving consumer’s ownership of data can reduce inefficient data hoarding by companies
    - E.g., Miller and Tucker (2014) on hospital system data silos
- Health privacy rules often have caps on charges healthcare providers can impose for copies of paper records
    - Baker et al. (2015) find these caps increased hospital adoption of EMRs
- 21st Century Cures Act of 2016 (Cures Act) went into effect April 2021
    - Raises concerns about emotional impact of electronic delivery of health information

Privacy, personalized medicine, genetic data

- Genetic data have significant privacy risks (Hellman 2003, Oster et al. 2010):
    - Reveal a lot about a person – current and future health status, other traits
    - Can also reveal a lot about biological relations
    - Are persistently informative (over a lifetime and for future generations)
    - Implications and meanings develop and change as science progresses
- Genetic data can also be a key input into personalized medicine.
    - Genetic cancer risk can be used to target monitoring, preventive treatment
- Lack of privacy protection can make people reluctant to take genetic tests (and create data outside their control), while strict protections may limit social value of data (and lower supply)

Genetic privacy policy

- Miller and Tucker (2017) studies impact of 3 dimensions of genetic privacy policy on rates of genetic testing for cancer risk
- Find different effects of different dimension:
    1. Notification of privacy risk lowers rates of testing
    2. Consent requirement for re-disclosure (ownership) increases it
    3. Restrictions on downstream data uses (anti-discrimination) has no effect
- Implication: greater consumer control does not always slow adoption (can reassure or increase value)
- Signs of information limitations: notification rule affected behavior (could be efficient or salience), lack of discrimination law impact could signal difficulties with detection and enforcement

What can you do?

- Recent growing interest from economists
- This is good for policy and science
- Theory models are useful for formalizing ideas about incentives, tradeoffs, mapping out equilibrium, welfare and distributional effects
- Empirical work needed to assess ground reality as it unfolds, guide policy
- Still huge open questions, quickly changing technology and policy world, lots of opportunity