National Academy of Medicine -Digital Learning Collaborative
Patient Ownership of Health Data:
Implications for a Learning Health System
June 28, 2018

Panel 3 - Ethical and Financial Implications of Patient Data Ownership

Barbara J. Evans, Ph.D., J.D., LL.M.
Alumnae College Professor of Law
Professor, Electrical and Computer Engineering
Director, Center for Biotechnology & Law
University of Houston
bjevans@central.uh.edu ● 713-446-7576

Acknowledgments & Disclosures

My work has received support from

- US National Institutes of Health/National Human Genome Research Institute/National Cancer Institute R01HG008605, R01HG008918, UO1HG006507, U01HG007307

with additional support from Robert Wood Johnson Foundation, the Greenwall Foundation, and the US Food & Drug Administration via Mini-Sentinel/Sentinel subcontracts

No conflicts to disclose

Views expressed are my own and are not positions of the State of Texas (my employer) or my funders

A Note on Terminology

As used here:

- “My data” means “data that describe me,” not “data I own”
- “Their data” means “data that describe them,” not “data that they own”

et cetera

Realities of Legal Data Ownership

1. **Property law is a creature of state, not federal, law**

   – exception: patent law, where the U.S. Constitution expressly gave Congress power to legislate

   – implications: Federal regulations like the Common Rule and HIPAA Privacy Rule do not preempt more stringent state laws. State data ownership laws, if they existed, would take precedence over these regulations, creating a non-uniform patchwork of data access rules

2. **Law offers many different forms of ownership. Proposed data ownership laws are vague whether they mean:**

   – *Fee simple* ownership (example: a house or car)
   – Joint ownership or tenancy in common (multiple owners)
   – Copyright (time-limited ownership, with a “fair use” override)
   – Trusts (which split nominal ownership from beneficial ownership)
   – Future interests
   – Riparian ownership (rights in a river that runs by land you own)
   – and many others

3. **Individual data ownership would not provide the exclusive control that proponents seem to desire**
   - **Property law balances the interests of owners and the public**
   - **Eminent Domain/"Takings" -** The government – or a private agent it authorizes – can take your house without your consent for "public benefit," subject to paying "just compensation," which may be zero
   - **Police Power -** The government can take your house without compensation for law enforcement, public health and safety purposes
4. **Ownership requires administrative infrastructure and high transaction costs ("tragedy of the anti-commons")**
   - example: county records to trace titles, convey and record deeds, courts to resolve ownership disputes and enforce owners' rights
5. **Ownership does not ensure an enduring access right**
   - Access rights run with the property. You lose access if you sell or transfer the property to a new owner.
   - You can't go sit in your living room, after you sell your house!
6. **Data ownership does not protect privacy and security**
   - A house you own can still be robbed

Three Different Mechanisms for protecting the interests of data subjects

1. **Bioethical rights**
2. **Rights incident to property ownership**

   e.g., ingress/egress/access, right to eject trespassers, right to use and enjoy your property, right to sell or transfer your ownership, right to alter or improve your property, etc. – the specific “bundle of rights” and the duties of ownership are defined by property law

3. **Civil rights (enforceable rights created by law)**

Example: **Access rights - Don't Mix Them Up!**

Return of incidental findings and return of research results: unenforceable bioethical rights

Access incident to ownership: goes away if you transfer the property

Civil Rights: individual access rights under privacy laws: enforceable civil rights, *e.g.*

1970 US Fair Credit Reporting Act
1973 US HEW Fair Information Practices
1974 US Federal Privacy Act (government-held data)
(resulting in Privacy Protection Study Comm'n)
1996 - 2000 US HIPAA statute & HIPAA Privacy Rule
2008 US Genetic Information Nondiscrimination Act
(resulting in 2014 changes to HIPAA Privacy Rule)
2016 EU GDPR Art. 15 (effective May 2018)

Prior to the late 1970s, there was no norm of informed consent for research with preexisting data in the U.S.

The U.S. National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research

As of 1978 - Consent was widely viewed as unnecessary for studies "based exclusively upon existing records, data or materials gathered for other purposes." *43 Fed. Reg. 56174, 56188 (Nov. 30, 1978)*

U.S. Privacy Protection Study Commission ("PPSC")

As of 1977 - "Federal rules governing the funding of medical research require the informed consent of individuals who participate in it as research subjects, but do not require their consent when medical records are reviewed and abstracted for retrospective epidemiological research studies." *Personal Privacy in an Information Society 280 (July 1977)*

1977 Privacy Protection Study Comm'n recommended:

Research uses of data generally should require consent

Unconsented disclosures of identifiable personal data can sometimes be ethically justified, but should require:

1. Transparency entitlements for the data subjects
   - Individual data access
   - Accounting for disclosures
   - Right of explanation (for decisions based on the data that may affect individual rights)
2. A "minimum necessary" standard
3. A "public benefit" standard – the use must offer social benefit
4. Restrictions on downstream reuse and re-disclosure

1997 – The Balance of Individual and Public Interests in U.S. Federal Privacy Law*

"A Federal health privacy law should permit limited disclosures of health information without patient consent for specifically identified national priority activities. We have carefully examined the many uses that the health professions, related industries, and the government make of health information, and we are aware of the concerns of privacy and consumer advocates about these uses. The allowable disclosures and corresponding restrictions we recommend reflect a balancing of privacy and other social values."*

* U.S. Dep't of Health & Human Servs., Confidentiality of Individually-Identifiable Health Information: Recommendation of the Secretary of HHS Pursuant to Sec. 264 of the Health Insurance Portability and Accountability Act of 1996 (Sept. 11, 1997)

U.S. HIPAA's individual access right

45 C.F.R. §164.524

Designated Record Set (DRS) includes:

- Data *actually maintained* at time of request, if data can be identified as pertaining to the individual
- Medical, insurance, billing records plus data used *in whole or in part* to make decisions (*medical* or *non-medical*) about individuals (*any* individual)
  65 Federal Register at 82,606
- No duty to provide interpretive assistance to requesting individual

2016 HHS/OCR Guidance interprets this as including uninterpreted genomic data + test reports

Art. 15 EU GDPR
Right of access by the data subject

The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

- the purposes of the processing;

- the categories of personal data concerned …

The new U.S. Common Rule § 46.104(d)(4)(iii)(4)

Effective January 21, 2019, secondary data uses will not be subject to the Common Rule if:

> "The research involves only information collection and analysis involving the investigator's use of identifiable health information when that use is regulated under 45 CFR parts 160 and 164, subparts A and E, for the purposes of 'health care operations' or 'research' as those terms are defined at 45 CFR 164.501 or for 'public health activities and purposes' as described under 45 CFR 164.512(b) . . . ."

Where things stand

U.S. federal law and the law of other major jurisdictions such as the E.U. rightly rejected data ownership in favor of a civil rights model for protecting the rights of people whose data are taken into medical and genomic information commons.

There are many legal, practical, financial, and other drawbacks to individual data ownership, and legal data ownership would not provide as much protection as its proponents hope it will.

The current civil rights framework fails to cover all the health-relevant data that now exists (e.g., non-HIPAA-covered direct-to-consumer test results, data from mobile and wearable sensors, data stored by FDA-regulated medical device manufacturers, etc.)

Moreover, the current package of civil rights is incomplete. Further civil rights protections are needed in order to make the U.S. federal framework credible and worthy of public trust.