From Commercialization to Accountability: Responsible Health Data Collection, Use, and Disclosure for the 21st Century

Deven McGraw[1] Carolyn Petersen[2]

[1] Ciitizen Corp., Palo Alto, California, United States
[2] Division of Biomedical Statistics and Informatics, Mayo Clinic, Rochester, Minnesota, United States

Address for correspondence Carolyn Petersen, MS, MBI, FAMIA, Division of Biomedical Statistics and Informatics, Mayo Clinic, Rochester, MN, United States (e-mail: petersen.carolyn@mayo.edu).

Appl Clin Inform 2020;11:366–373.

Introduction

Proposed initiatives in the U.S. that require sharing of clinical health information and facilitate easier access to that information through open, standard digital interfaces raise risks that sensitive information may be shared more broadly outside of legal protections for health data and may be more readily commercialized, in addition to existing commercialization of health data by health care institutions allowed by federal privacy laws. Is commercialization truly health data's "boogeyman" or is the problem the sharing of health data without sufficient protections against harm or inappropriate use? Can privacy risks be mitigated while still enabling value to be gleaned through more widespread sharing of health information? In this editorial, we argue that the focus should not be on whether the entity is or is not currently covered by federal health privacy laws, or whether the data are or are not "commercialized." Instead, U.S. policies and practices should encourage (or outright require) (1) responsible use of data to improve health and health care, (2) greater transparency to and participation by patients and consumers, and (3) controls to minimize harm to individuals and populations.

Background

Since the passage of the Health Information Technology for Economic and Clinical Health Act in 2009 (HITECH),[1] a part of the American Recovery and Reinvestment Act of 2009, Congress and U.S. health administrative agencies have pursued policies to facilitate the adoption of electronic health records (EHRs), with the ultimate goal of improving individual and population health. Although the policies adopted in response to HITECH have facilitated widespread adoption of EHRs by health care providers, these policies did not result in the desired robust sharing of information for treatment, for population health, and for medical discovery.[2,3] In 2015, the U.S. Department of Health and Human Services (HHS) issued a report finding that entities and their EHR vendors too frequently refused to share (i.e., "blocked") information, even for routine treatment purposes, due in part to lack of business incentives to share data.[4]

Congress responded to that report with the 21st Century Cures Act, directing HHS to establish policies to promote "interoperability" of health information and to prohibit and penalize "information blocking" by health care providers and health information networks or exchanges.[5] In response, HHS proposed several bold initiatives to require data sharing, including with patients. Specifically, under its authority to define information blocking, the HHS Office of the National Coordinator (ONC) established rules (the "information blocking" rules) that would essentially require health care providers and health information networks to share identifiable health information for a broad range of purposes—both with patients and with others—unless a refusal to share information could be justified under one of eight exceptions.[6] ONC also finalized rules mandating that vendors of certified EHRs make data available to individuals and others via open standard application programming interfaces (APIs) (the "API rules"), with no fees to be charged to vendors of patient-facing applications or apps and, with respect to apps serving providers, under licensing and payment terms that are "reasonable and nondiscriminatory."[6] The Centers for Medicare and Medicaid Services now requires health plans under its oversight to share data with health plan beneficiaries using open, standard APIs and requiring hospitals to issue electronic alerts to physicians when patients are hospitalized.[7] Finally, the HHS Office for Civil Rights, the office responsible for the Health Insurance Portability and

received
March 27, 2020
accepted after revision
April 6, 2020

© 2020 Georg Thieme Verlag KG Stuttgart · New York

DOI https://doi.org/10.1055/s-0040-1710392.
ISSN 1869-0327.

This document was downloaded for personal use only. Unauthorized distribution is strictly prohibited.

Accountability Act (HIPAA) privacy and security regulations, launched an enforcement initiative focused on improving compliance with an individual's right to obtain copies of her health information pursuant to the HIPAA Privacy Rule.[8]

Opening the Door to Data Sharing for "Good" or "Bad"?

Data sharing initiatives—particularly the aspects that facilitate greater sharing of clinical health information with individuals (and with apps or services operating on their behalf)—are supported by many patient advocates and by technology companies seeking an opportunity to create markets for their services. However, some health care providers and EHR vendors have voiced resistance.[9,10] The proposed information blocking rules allow providers to decline sharing health information when necessary to protect privacy and security, and the proposed API rules include protections to assure that consumer applications requesting access to EHR data have been authorized by the consumer. Nevertheless, critics of the rules are worried about the lack of privacy protections for health information shared outside of HIPAA (e.g., when an individual downloads information into a medical application marketed to consumers), and the possibility of consumer technology companies' taking advantage of patients to sell and misuse data for the companies' commercial gain. HIPAA's coverage does not extend to entities outside of the traditional health care ecosystem, covering only health care providers who conduct electronic payment-related transactions with health plans, health plans, health care clearinghouses (which standardize electronic payment transactions), and vendors who work on providers' behalf (known as business associates).[11]

The concerns about lack of privacy protections outside of HIPAA are not unfounded.[12] Research shows that apps, including health apps, routinely share data with third parties, often for advertising, marketing, and other commercial purposes, without transparency to users.[13–15] Members of a Facebook social media group for individuals with the BRCA gene (which increases the risk of getting breast cancer) discovered that their "closed" peer support network—where they shared intimate details about medical treatments—was accessible to outsiders, in contravention of Facebook's stated policies.[16,17] Several technology companies' business models are based in part on their ability to mine consumers' digital activities and leverage that data to predict and shape human behavior for commercial gain.[18] Further, application developers stack the deck against individuals, who want to be careful about how they share their data, as technologies frequently are designed to maximize the likelihood individuals will consent to collection, uses, and disclosures of their personal information without fully realizing to what they are consenting.[19]

However, individuals' sharing of clinical data into spaces not covered by HIPAA is not the only cause for concern. Large technology companies have launched initiatives in health and are increasingly partnering with health care organizations, including partnerships that involve access to clinical health information. For example, Google has signed deals with Mayo Clinic and Ascension Health to use artificial intelligence (AI) help each of these entities make better use of their clinical data.[20] Microsoft is partnering with Providence St. Joseph Health to build a high-tech, hospital of the future in the Seattle area,[21] and the company also has partnered with Humana to develop technologies that deliver insights that will help the insurer better care for its senior health plan members.[22] These arrangements are covered by HIPAA if they involve the sharing of identifiable information. At the same time, the poor track record of some of these technology companies regarding their use of consumer data has caused many to question whether their motives are to improve health and wellness or to inject sensitive clinical data into advertising data pipelines—or both.[23] For example, HHS is investigating the arrangement between Google and Ascension to ensure that it complies with HIPAA.[24] It is unclear if other arrangements are under review.

Legal Protections for Health Data Outside of HIPAA

HIPAA does not cover all health data, but that does not mean that companies collecting health data outside of HIPAA can make unfettered use of it. Commercial companies can be held accountable by the Federal Trade Commission (FTC) under its Federal Trade Commission Act authority for "unfair" and "deceptive" trade practices "in or affecting commerce," and the FTC has used this authority to enforce expectations about how companies handle personal data. The FTC's enforcement actions regarding deception have been about more than broken privacy promises and extend to general deception in obtaining personal information through nontransparent, privacy-invasive activities. FTC's "unfairness" actions have addressed issues such as "retroactive policy changes, deceitful data collection, improper use of data, unfair design, and unfair information security practices."[25] The FTC's recent $5 billion settlement with Facebook, the largest penalty ever levied by the FTC against a company but diminutive compared with Facebook's total annual revenues, raised doubts about whether the FTC is up to the challenge of enforcing privacy in a modern data ecosystem.[26] Others have expressed concerns that FTC is underresourced, with respect to staff (numbers and expertise) and funding.[27] Even companies under FTC oversight have argued that the FTC needs more meaningful rulemaking authority, which could empower it to act more quickly to address emerging privacy and security risks in the marketplace.[28] Furthermore, FTC's authorities are grounded in what is "reasonable" behavior for a commercial company. Consequently, monetization of health data, if done in ways consistent with the context of the data collection, for purpose(s) related to the primary purpose of the data collection, and done with transparency to data subjects, would not necessarily be an unfair or deceptive act or practice.

States also have the power to regulate companies' collection of data on state residents. For example, the California Consumer Privacy Act (CCPA), which went into effect in 2020, covers companies' collecting large amounts of data (or monetizing data) about California residents.[29] CCPA has

This document was downloaded for personal use only. Unauthorized distribution is strictly prohibited.

exemptions for data covered by HIPAA or by the state's Confidentiality of Medical Information Act, which includes clinical information pulled from an EHR by a consumer app, but otherwise the reach of the CCPA is potentially broad. Because California authorities will not begin enforcing the law until June 2020, there is insufficient experience to gauge the impact it will have on the consumer data marketplace. Other states are also considering strong consumer privacy legislation, a development that has prompted technology companies to ask Congress to pass a federal data privacy law that would preempt (or supersede) state laws.[30] Bills have been introduced, and hearings have been held, but no bills have made substantial progress toward passage.

In response to proposed interoperability and information blocking rules, the American Medical Association[31] and Epic,[32] the largest EHR vendor, recommended that ONC require consumer apps seeking to connect to EHRs through APIs to be more transparent with users about their data practices. This action could help individuals make application choices that match their privacy tolerances. If ONC has legal authority to require or promote application transparency, this is a worthwhile suggestion. However, the rhetoric accompanying these recommendations aggressively warns about the "sale" and commercialization of health data by big technology companies. But does HIPAA sufficiently control for commercialization of health data by entities covered by its regulations? Is commercialization of health data always bad?

HIPAA and "Sale" of Data

The HIPAA Privacy Rule prohibits "sales" of protected (identifiable) health information without the express authorization of the individual, but there are several exceptions to this prohibition. For example, a sale of a medical practice to another physician, which would include all of the records, would not constitute a "sale of data" requiring authorization from each patient.[33] Arrangements between covered entities and vendors, which are business associates, also would not constitute a sale of data as long as the reimbursement from the covered entity to the business associate is for the provision of services (even if data are shared as part of that service).

However, data that are "de-identified" in accordance with HIPAA standards are no longer regulated by HIPAA and thus can be sold without limitation. The de-identification legal standard is "no reasonable basis" to believe the information can be re-identified. The Privacy Rule provides two methodologies for achieving de-identification. The safe harbor, or "cookbook" method, first established in 2001, requires the removal of 18 categories of identifiers and no actual knowledge that the data can be re-identified. (This is a high bar—it is actual knowledge, not mere suspicion.) Many have criticized this method as being insufficient to protect individuals from being re-identified given the greater amount of data in the ecosystem that can be used to potentially identify individuals.[34] The other methodology, the expert or statistician method, requires a statistician to attest that the data—in the hands of the recipient (and taking into account other information the recipient has access to)—is at "very low risk" of re-identification. Once information is de-identified per HIPAA standards, it is no longer covered by HIPAA's rules.

Consequently, sales of de-identified data do not have to be tracked or reported, but crucially, they appear to be ubiquitous.[35] In *Our Bodies, Our Data*, Adam Tanner reported on robust sales of detailed health profiles of individuals, all created with HIPAA de-identified data.[36] The entities that can "sell" de-identified data are not limited to covered entities like doctors and hospitals or health plans. Their contractors/business associates can also de-identify and sell data as long as their business associate agreements with covered entities expressly allow them to do this.[37] In many cases, the business associate considers this contractual permission to be part of the deal, with the ability to sell de-identified data reflected in the price of the services. The Meaningful Use-certified electronic medical record PracticeFusion is free to physicians who agree to view advertising when using the record; physicians also give permission for PracticeFusion to sell de-identified patient record data.[38] Omny Health, a health technology startup that facilitates provider sales of their data, was voted by the audience as the most promising new technology at the Health 2.0 conference in 2019.[39] Legally, sales of de-identified data can occur without transparency to patients or the public, without patient consent, and even over a patient's objection.

Sale of de-identified data arrangements are increasingly being subjected to scrutiny and legal challenge. In January 2020, patients at the University of Pittsburgh Medical Center (UPMC) filed a class action lawsuit alleging that information gathered from patients via UPMC's Web site (including via its patient portal) was disclosed to third parties for commercial gain without the consent of the patients.[40] In June 2019, a patient filed a class action lawsuit against the University of Chicago and Google after University of Chicago Medical Center sold supposedly "de-identified" medical record data to Google to enable the company to create AI tools to sell to physicians and hospitals.[41] In 2018, The New York Times and ProPublica reported on an arrangement between Memorial Sloan Kettering Cancer Center (MSKCC) and Paige.AI, a technology startup in which MSKCC and key executives were investors. Paige.AI had an "exclusive deal" to use cancer tissue slides from MSKCC and from decades of work by its pathologists. Physicians and staff at the hospital questioned the arrangement, noting that patients were concerned about their health data being commercialized.[42] In February 2020, the HHS Office of the Inspector General found that some pharmacies had unlawfully provided marketers with the pharmacies' credentials for querying information about beneficiary eligibility for the Medicare Part D program.[43]

What's the Harm?

Much has been written about the potential and actual harms of unauthorized disclosures of personal data.[44,45] Data shared with employers or insurers, or in financial contexts (such as to lenders) can lead to discrimination which, even if the data are anonymized or de-identified, could be used in ways that negatively affect populations. People already can become

This document was downloaded for personal use only. Unauthorized distribution is strictly prohibited.

easy targets for potentially harmful health misinformation because health status can be inferred from nonhealth information collected online and through daily activities. This could be exacerbated if actual clinical data can be added to these data profiles. Data collection and uses that are "creepy" (i.e., go beyond social norms) generate strong public backlash.[46] Individuals may become fearful of using services, including social media, to share information and obtain support for self-management of health concerns, and thereby experience poorer quality of life.[12] Survey data shows that individuals practice "privacy protective" behaviors, such as not seeking care, selecting the few remaining providers without EHRs, or lying about health conditions, if they have doubts about whether health information will remain confidential and not misused.[47] Minorities admit to privacy protective behaviors in greater numbers,[48] and are far less likely to utilize consumer tools such as portals,[49] suggesting that the failure to address these issues could exacerbate racial and ethnic health disparities. Consequently, concerns about how health information can be accessed, used, and disclosed has the potential to undermine public trust in digital innovation, whether in the form of digital tools to improve individual health or with respect to access to health data by technology companies. Such loss of public trust also has the potential to undermine the federal government's substantial investment of taxpayer dollars in health information technology.

It is not clear, however, whether there are potential harms from "commercialization" of health information that are distinct from these general data-sharing harms, or distinct from general concerns that the U.S. health care system may prioritize revenue over people. Research on the potential harms of "commercialization" of research may shed light on potential harms unique to health data commercialization. Such harms include skewing of research toward projects with commercial potential; withholding data for competitive advantage; science "hype" (exaggerated representations of the state of the science); premature implementation before the science is fully developed in a rush to get to market; and erosion of public trust.[50] With respect to health data commercialization, the harms arguably can be quite similar: prioritization of data initiatives with the greatest potential for monetization (at the expense of data projects that could serve an important population or public health need but for which potential for commercialization is less clear); marginalization of populations absent from databases used for decision-making; use of data intended to identify costs and negative outcomes in populations that have been less able to prevent unwanted data collection and that may subsequently be further discriminated against; use of data to support nonhealth-care-related forms of bias such as discrimination in housing and employment; overhype of data initiatives with the greatest commercial potential; decisions made prematurely based on incomplete or biased data; and erosion of public trust.

Protecting Data and Supporting Progress

Commercialization has had some positive impacts on research —for example, providing incentives for investment in research and supporting translation of research into beneficial products and therapies.[50] The entry of technology companies—with their expertise, resources, and computing power—into the health care space could help us solve seemingly intractable problems of cost and quality in U.S. health care.[51] Advertising supports a free Internet and mobile services used by individuals; the problem is not necessarily that information is shared with advertisers but that the tradeoff is not made sufficiently transparent to consumers; that current data profiling is beyond the knowledge and comfort level of most consumers; and that consumers seeking to be more private with their data have few, if any, options. Is it possible to glean the benefits from greater health data sharing while minimizing the harms, even in a health care system in which revenue is a key driver of decisions?

Despite these technical, political, and legal challenges, some potential areas for action emerge:

Eliminate the distinction between HIPAA- and non-HIPAA-covered data and between "Big Technology" and traditional health care entities. Given that commercial interests motivate behavior of entities both inside and outside of HIPAA, drawing policy lines based on HIPAA coverage makes little sense. Prohibiting commercial and/or "Big Tech" companies from acquiring health data altogether is a blunt instrument that likely is infeasible and sacrifices any potential benefits. A more nuanced approach that supports innovation while controlling for inappropriate, unexpected, and/or potentially harmful uses of data better—if achievable—has greater potential to advance the public interest.

Don't overrely on informed consent to protect privacy. The use of informed consent has been a foundational principle of health care research for decades, but its ability to adequately control the flow of data pushes the burden of protecting privacy to the individual and remains challenging for technological, political, and practical reasons.[52,53] Although the use of dynamic consent (the use of health information technology to support opting out of data sharing at a granular level) holds potential for research,[54] it is less clear how well it can be implemented across the range of health data sources for multiple, potentially valuable uses (not all of which can be anticipated at the time of data collection). However, providing individuals with some choices with respect to their health information is critical, particularly in circumstances where the collection, use, and disclosure of their data are beyond what reasonably would be expected given the context. The "no surprises" principle—a principle that no one should ever be surprised by the collection, use, transmission, or disclosure of their personal information—offers an approach that builds and supports the trust individuals seek when making decisions about secondary uses of their data.[55] In addition, U.S. policymakers should explore policies that allow people to opt out of data collection and to have their data deleted from databases (commonly referred to as the "right to be forgotten"[56]), in circumstances when these actions do not impair the utility of the database for individual or population health uses.

Treat transparency to patients and consumers as a fundamental value and a primary obligation.

This document was downloaded for personal use only. Unauthorized distribution is strictly prohibited.

Transparency is an underrated—and underutilized—fair information practice principle. Users may be uninterested in reading long Terms of Service or other agreements, but that does not mean they do not care to know when and how their data will be used, and whether there is commercial gain from such activities. Providing more transparency to data flows so that consumers understand how their data are collected, used, and shared is paramount to building a trustworthy ecosystem for health data. Greater transparency to the public, plus other requirements for accountability such as ethics review boards for data uses,[57] should be explored and implemented.

Develop a policy framework that will allow commercial companies to utilize data in ways that could improve health and health care while minimizing harms to individuals and to populations. The pursuit of profit through data commercialization as an end in itself is unsupportable within health care. However, profit as a byproduct of data use that has the potential to support health and improved health outcomes should be encouraged. A privacy policy framework that delineates how data may be used other than for direct treatment purposes would establish guardrails for commercial users and help restore confidence in the health care system.[58] Such policies should include real consequences for data collection, uses, or disclosures that harm individual or populations (including criminal penalties for intentional misuses or abuses of data).

Explore new forms of benefits that accrue to patients and consumers whose data are collected, used, and shared. The idea that patients should share in any profits generated as a result of discoveries based upon individuals' personal information is not new.[59,60] Patients also are concerned about being unable to access treatments that are developed using their data while others profit.[61] Although the value of innovation can be measured through sales receipts, the financial value of personal data used in product development is more difficult to assess because individuals value privacy and compensation differently based upon personal circumstances. Because the economic value of health records is highly variable—from $1 to $1,000 per record, depending upon completeness of record and whether it is sold singly or as part of a database[62]—financial compensation for access to personal health information can be challenging to calculate and distribute. Thus, other forms of recompense to individuals for use of their data are needed. Such benefits could include, but are not limited to, expanded access to care and opportunities to partner with commercial entities to facilitate research in the interests of patients.[63–65] At a minimum, individuals should have the right to obtain health and health-related information collected about them, enabling them to use it and share it as they see fit. For example, return of personalized, actionable information (e.g., a report showing times of day when blood glucose levels are most often outside the ideal range) to individuals could support appropriate changes in diet and meal management. Health systems can use individuals' data to identify relevant services and help individuals access that care, as well as alleviate individuals' concerns about the quality of care.[66]

Conclusion

Ultimately, our federal health data "policy" today reflects more of a laissez-faire approach that undermines both public trust and our ability to leverage data to improve individual and population health. We need policies and practices that focus less on eliminating the "boogeyman" and instead help ensure that broader sharing of health data—both inside and outside of HIPAA coverage—is transparent, trustworthy, and accountable *and* improves access to care and health outcomes, reduce disparities, and makes health affordable.

Clinical Relevance Statement

This works describes the lack of accountability surrounding the sale of health data and identifies actions that can mitigate the problems resulting from commercialization of health data.

Multiple Choice Questions

1. The following group(s) support greater sharing of clinical health information with individuals:
   a. Technology companies.
   b. Patient advocates.
   c. Insurance companies and patient advocates.
   d. Technology companies and patient advocates.

   Correct Answer: The correct answer is option d. Technology companies and patient advocates support the use of health information technology to make patient information more accessible to patients on demand across a broad range of platforms.

2. Actions that could result in more patient- and consumer-friendly data protection and sharing include:
   a. Treat HIPAA-covered and non-HIPAA-covered data the same under the law.
   b. Value and act as though transparency to patients is a fundamental value and an obligation.
   c. Develop new benefits for patients and consumers whose data are collected, used, and shared.
   d. All of the above.

   Correct Answer: The correct anwer is option d. Treating HIPAA-covered and non-HIPAA-covered data the same, establishing transparency as a fundamental value and obligation, and creating new benefits for those who share data about them are all activities that could result in more patient- and consumer-friendly data protection and sharing.

Authors' Contributions

D.M. and C.P. wrote the first draft and revised the manuscript.

Protection of Human and Animal Subjects

This work involved no humans or animals, and so was not subject to institutional review board oversight.

This document was downloaded for personal use only. Unauthorized distribution is strictly prohibited.

Funding
None.

Conflict of Interest
None declared.

References

1 United States Congress. Health Information Technology (HITECH Act). United States Congress; 2009. Available at: https://www.healthit.gov/sites/default/files/hitech_act_excerpt_from_arra_with_index.pdf. Accessed February 16, 2020
2 Sheikh A, Sood HS, Bates DW. Leveraging health information technology to achieve the "triple aim" of healthcare reform. J Am Med Inform Assoc 2015;22(04):849–856
3 Lehmann CU, Kressly S, Hart WWC, Johnson KB, Frisse ME. Barriers to pediatric information exchange. Pediatrics 2017;139(05):e20162653
4 Office of the National Coordinator for Health Information Technology. Report on Health Information Blocking. Department of Health and Human Services; 2015. Available at: https://www.healthit.gov/sites/default/files/reports/info_blocking_040915.pdf. Accessed February 16, 2020
5 United States Congress. Public Law 114–255. United States Congress; 2016. Available at: https://www.congress.gov/114/plaws/publ255/PLAW-114publ255.pdf. Accessed February 16, 2020
6 Department of Health and Human Services. 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program. Department of Health and Human Services; 2019. Available at: https://www.healthit.gov/sites/default/files/cures/2020-03/ONC_Cures_Act_Final_Rule_03092020.pdf. Accessed March 24, 2020
7 Department of Health and Human Services. Medicare and Medicaid Programs; Patient Protection and Affordable Care Act; Interoperability and Patient Access for Medicare Advantage Organization and Medicaid Managed Care Plans, State Medicaid Agencies, CHIP Agencies and CHIP Managed Care Entities, Issuers of Qualified Health Plans in the Federally-Facilitated Exchanges and Health Care Providers. Department of Health and Human Services; 2019. Available at: https://www.cms.gov/files/document/cms-9115-f.pdf. Accessed March 24, 2020
8 Office for Civil Rights. OCR Settles First Case in HIPAA Right of Access Initiative. Department of Health and Human Services; 2019. Available at: https://www.hhs.gov/about/news/2019/09/09/ocr-settles-first-case-hipaa-right-access-initiative.html. Accessed February 16, 2020
9 Kent J. AMA calls for more data privacy in proposed health IT rules. Health IT Analytics; 2019. Available at: https://healthitanalytics.com/news/ama-calls-for-more-data-privacy-in-proposed-health-it-rules. Accessed February 16, 2020
10 Farr C. Epic's CEO is urging hospital customers to oppose rules that would make it easier to share medical info. CNBC; 2020. Available at: https://www.cnbc.com/2020/01/22/epic-ceo-sends-letter-urging-hospitals-to-oppose-hhs-data-sharing-rule.html. Accessed February 16, 2020
11 Department of Health and Human Services. Covered Entities and Business Associates. Department of Health and Human Services; 2017. Available at: https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html. Accessed February 16, 2020
12 Petersen C, Lehmann CU. Social media in health care: time for transparent privacy policies and consent for data use and disclosure. Appl Clin Inform 2018;9(04):856–859
13 Huckvale K, Torous J, Larsen ME. Assessment of the data sharing and privacy practices of smartphone apps for depression and smoking cessation. JAMA Netw Open 2019;2(04):e192542
14 Grundy Q, Chiu K, Held F, Continella A, Bero L, Holz R. Data sharing practices of medicines related apps and the mobile ecosystem: traffic, content, and network analysis. BMJ 2019;364:l920
15 ForbrukerRådet. Out of Control: How Consumers Are Exploited by the Online Advertising Industry. Available at: https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf. Accessed March 22, 2020
16 Trotter F, Harlow D, Patient A, et al. FTC Complaint: Multiple Ongoing Patient Privacy Breaches in the Facebook PHR (Groups Product). 2018. Available at: https://missingconsent.org/downloads/SicGRL_FTC_Compliant.pdf. Accessed February 16, 2020
17 Davis J. Facebook accused of exposing user health data in complaint to FTC. Health IT Security; 2019. Available at: https://healthitsecurity.com/news/facebook-accused-of-exposing-user-health-data-in-ftc-complaint. Accessed February 16, 2020
18 Zuboff S. 'Surveillance capitalism' has gone rogue. We must curb its excesses. Washington Post; 2019. Available at: https://www.washingtonpost.com/opinions/surveillance-capitalism-has-gone-rogue-we-must-curb-its-excesses/2019/01/24/be463f48-1ffa-11e9-9145-3f74070bbdb9_story.html. Accessed February 16, 2020
19 Hartzog W. Privacy's Blueprint: The Battle to Control the Design of New Technologies. Cambridge, MA: Harvard University Press; 2018
20 Japsen B. Mayo Clinic, Google partner on digital health analytics. Forbes; 2019. Available at: https://www.forbes.com/sites/brucejapsen/2019/09/10/mayo-clinic-google-partner-on-digital-health-analytics/#5320766a36e7. Accessed February 16, 2020
21 Farr C. Microsoft joins hospital chain Providence to build 'hospital of the future'. CNBC; 2019. Available at: https://www.cnbc.com/2019/07/09/microsoft-and-providence-medical-building-hospital-of-the-future.html. Accessed February 16, 2020
22 Thorne J. Microsoft lands another healthcare partnership, this time with Humana to take care of aging seniors. GeekWire; 2019. Available at: https://www.geekwire.com/2019/microsoft-lands-another-healthcare-partnership-time-humana-take-care-aging-seniors/. Accessed February 16, 2020
23 Dorsch A. The intrusion of big tech into healthcare threatens patients' rights. The Health Care Blog; 2019. Available at: https://thehealthcareblog.com/blog/2019/12/24/the-intrusion-of-big-tech-into-healthcare-threatens-patients-rights/. Accessed February 16, 2020
24 Wehrwein P. HHS investigating Google, Ascension's 'Project Nightingale' for HIPAA violations. Managed Care; 2019. Available at: https://www.managedcaremag.com/dailynews/20191113/hhs-investigating-google-ascensions-project-nightingale-hipaa-violations. Accessed February 16, 2020
25 Solove DJ, Hartzog W. The FTC and the new common law of privacy. Columbia Law Rev 2011;114(03):583–676
26 Olen H. Why Facebook's $5 billion settlement with the FTC won't change a thing. Washington Post; 2019. Available at: https://www.washingtonpost.com/opinions/2019/07/25/why-facebooks-billion-settlement-with-ftc-wont-change-thing/. Accessed February 16, 2020
27 Rich J. Give the F.T.C. some teeth to guard our privacy. The New York Times; 2019. Available at: https://www.nytimes.com/2019/08/12/opinion/ftc-privacy-congress.html. Accessed February 16, 2020
28 Propes A. Privacy & FTC rulemaking authority: a historical context. iab; 2018. Available at: https://www.iab.com/news/privacy-ftc-rulemaking-authority-a-historical-context/. Accessed March 22, 2020
29 State of California Department of Justice. California Consumer Privacy Act (CCPA). State of California Department of Justice; 2018. Available at: https://oag.ca.gov/privacy/ccpa. Accessed February 16, 2020

This document was downloaded for personal use only. Unauthorized distribution is strictly prohibited.

30 Kuraitis V, McGraw D. For your radar – huge implications for healthcare in pending privacy legislation. The Health Care Blog; 2020. Available at: https://thehealthcareblog.com/blog/2019/02/20/for-your-radar-huge-implications-for-healthcare-in-pending-privacy-legislation/. Accessed February 16, 2020

31 American Medical Association. Letter. American Medical Association; 2019. Available at: https://searchusan.ama-assn.org/undefined/documentDownload?uri=%2Funstructured%2Fbinary%2Fletter%2FLETTERS%2F2019-5-31-Letter-to-Dr-Rucker-re-ONC-NPRM-Comments.pdf. Accessed February 16, 2020

32 Jason C. Epic leads almost 60 health systems against interoperability rule. EHR Intelligence; 2020. Available at: https://ehrintelligence.com/news/epic-leads-almost-60-health-systems-against-interoperability-rule. Accessed February 16, 2020

33 Office for Civil Rights. HIPPA Administrative Simplification Regulation Text: 45 CFR Parts 160, 162, and 164 (Unofficial Version, as amended through March 26, 2013). Department of Health and Human Services; 2013. Available at: https://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf. Accessed February 16, 2020

34 McGraw D. Building public trust in uses of Health Insurance Portability and Accountability Act de-identified data. J Am Med Inform Assoc 2013;20(01):29–34

35 Arndt RZ. How third parties harvest health data from providers, payers and pharmacies. Modern Healthcare; 2018. Available at: https://www.modernhealthcare.com/article/20180407/NEWS/180409938/how-third-parties-harvest-health-data-from-providers-payers-and-pharmacies. Accessed February 16, 2020

36 Tanner A. Our Bodies, Our Data: How Companies Make Billions Selling our Medical Records. Boston: Beacon Press; 2017

37 Department of Health and Human Services. May a Health Information Organization (HIO), Acting As a Business Associate of a HIPAA Covered Entity, De-identify Information and Then Use It For Its Own Purposes? Department of Health and Human Services; 2008. Available at: https://www.hhs.gov/hipaa/for-professionals/faq/544/may-a-health-information-organization-de-identify-information/index.html. Accessed March 22, 2020

38 Quora. What is Practice Fusion's business model? Quora.com; 2015. Available at: https://www.quora.com/What-is-Practice-Fusions-business-model. Accessed February 16, 2020

39 HIMSS TV. How Health 2.0 Launch! Winner is tapping the value of supply chain data. MobiHealthNews; 2019. Available at: https://www.mobihealthnews.com/video/how-health-20-launch-winner-tapping-value-supply-chain-data. Accessed February 16, 2020

40 Court of Common Pleas of Alleghany County. Pennsylvania. Civil Action: Jane Doe I and Jane Doe II, on behalf of themselves and all others similarly situated v. UPMC. 2020. Available at: https://higherlogicdownload.s3-external-1.amazonaws.com/AMIA/UPMC%20Jane%20Doe%20Privacy%20Complaint.pdf?AWSAccessKeyId=AKIAVRDO7IEREB57R7MT&Expires=1581928998&Signature=ezkWpx2OhfxuxXg7p7GufzHe4sg%3D. Accessed February 16, 2020

41 Wakabayashi D. Google and the University of Chicago are sued over data sharing. The New York Times; 2019. Available at: https://www.nytimes.com/2019/06/26/technology/google-university-chicago-data-sharing-lawsuit.html. Accessed February 16, 2020

42 Thomas K, Ornstein C. Memorial Sloan Kettering's season of turmoil. The New York Times; 2018. Available at: https://www.nytimes.com/2018/12/31/health/memorial-sloan-kettering-conflicts.html?searchResultPosition=1. Accessed February 16, 2020

43 Office of the Inspector General. The Majority of Providers Reviewed Used Medicare Part D Eligibility Verification Transactions for Potentially Inappropriate Purposes. Department of Health and Human Services. Available at: https://oig.hhs.gov/oas/reports/region5/51700020.pdf. Accessed February 16, 2020

44 Dimick C. No harm done? Assessing risk of harm under the federal breach notification rule. J AHIMA 2010;81(08):20–25

45 Institute of Medicine. Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research. Institute of Medicine; 2009. Available at: https://www.nap.edu/catalog/12458/beyond-the-hipaa-privacy-rule-enhancing-privacy-improving-health-through. Accessed March 22, 2020

46 Tene O, Polonetsky J. A theory of creepy: technology, privacy, and shifting social norms. Yale J Law Technol 2014;16(01):59–102

47 McGraw D, Dempsey JX, Harris L, Goldman J. Privacy as an enabler, not an impediment: building trust into health information exchange. Health Aff (Millwood) 2009;28(02):416–427

48 California Health Care Foundation. Americans Have Acute Concerns about the Privacy of Personal Health Information. California Health Care Foundation; 2005. Available at: https://www.chcf.org/press-release/americans-have-acute-concerns-about-the-privacy-of-personal-health-information/. Accessed March 22, 2020

49 Cohen JK. Black, older patients less likely to use hospital patient portals. Modern Healthcare; 2019. Available at: https://www.modernhealthcare.com/information-technology/black-older-patients-less-likely-use-hospital-patient-portals. Accessed March 22, 2020

50 Caulfield T, Ogbogu U. The commercialization of university-based research: balancing risks and benefits. BMC Med Ethics 2015;16(01):70

51 Wachter RM, Cassel CK. Sharing health care data with digital giants: overcoming obstacles and reaping benefits while protecting patients. JAMA 2020. Doi: 10.1001/jama.2019.21215

52 Savage L. Why we must remember where informed consent comes from. IAPP; 2018. Available at: https://iapp.org/news/a/why-we-must-remember-where-informed-consent-comes-from/. Accessed March 22, 2020

53 Nissenbaum H. A contextual approach to privacy online. Daedalus 2015;140(04):32–48

54 Spencer K, Sanders C, Whitley EA, Lund D, Kaye J, Dixon WG. Patient perspectives on sharing anonymized personal health data using a digital system for dynamic consent and research feedback: a qualitative study. J Med Internet Res 2016;18(04):e66

55 Baker DB, Kaye J, Terry SF. Governance through privacy, fairness, and respect for individuals. EGEMS (Wash DC) 2016;4(02):1207

56 Information Commissioner's Office. Right to Erasure. Information Commissioner's Office; [No date]. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/. Accessed March 22, 2020

57 Parasidis E, Pike E, McGraw D. A Belmont Report for health data. N Engl J Med 2019;380(16):1493–1495

58 Bechtel C, Ricciardi L, deBronkart D, Quinlan C, Cryer D. Why aren't more patients electronically accessing their medical records (yet)? Health Aff (Millwood) blog January 13, 2020. Available at: https://www.healthaffairs.org/do/10.1377/hblog20200108.82072/full/. Accessed April 16, 2020

59 van Roessel I, Reumann M, Brand A. Potentials and challenges of the health data cooperative model. Public Health Genomics 2017;20(06):321–331

60 Hafen E, Kossmann D, Brand A. Health data cooperatives - citizen empowerment. Methods Inf Med 2014;53(02):82–86

61 NICE Citizens Council. What Ethical and Practical Issues Need to Be Considered in the Use of Anonymised Information Derived from Personal Care Records as Part of the Evaluation of treatments and Delivery of Care? NICE Citizens Council; 2015. Available at: https://www.ncbi.nlm.nih.gov/books/NBK401705/pdf/Bookshelf_NBK401705.pdf. Accessed March 22, 2020

62 Stack B. Here's how much your personal information is selling for on the Dark Web. Experian Blog; 2017. Available at: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/. Accessed March 22, 2020

63 Petersen C. Patient informaticians: Turning patient voice into patient action. JAMIA Open 2018;1(02):130–135

64 Petersen C, Austin RR, Backonja U, et al. Citizen science to further precision medicine: from vision to implementation. JAMIA Open 2019. Doi: 10.1093/jamiaopen/ooz060

This document was downloaded for personal use only. Unauthorized distribution is strictly prohibited.

65 Borda A, Gray K, Fu Y. Research data management in health and biomedical citizen science: practices and prospects. JAMIA Open 2019. Doi: 10.1093/jamiaopen/ooz052

66 Singh K, Meyer SR, Westfall JM. Consumer-facing data, information, and tools: self-management of health in the digital age. Health Aff (Millwood) 2019;38(03):352–358

This document was downloaded for personal use only. Unauthorized distribution is strictly prohibited.