



**GENERAL COMMITTEE CONFERENCE CALL**

**Thursday, June 28, 2018**  
3:00 PM to 3:30 PM

Healthcare Leadership Council

750 9th Street, NW, Suite 500 Washington, D.C. 20001

*Conference line: (857) 232-0157, 30-40-73#*

**1. Welcome and introductions**

**2. 42 CFR Part 2 Graphic**

**Attachment 1**

**3. House E & C and Senate HELP Cybersecurity Letter/PR to HHS**

**Attachments 2,3**

**4. Update on House E & C Legacy Technologies Letter**

**5. Additional Articles**

**Attachments 4,5,6**



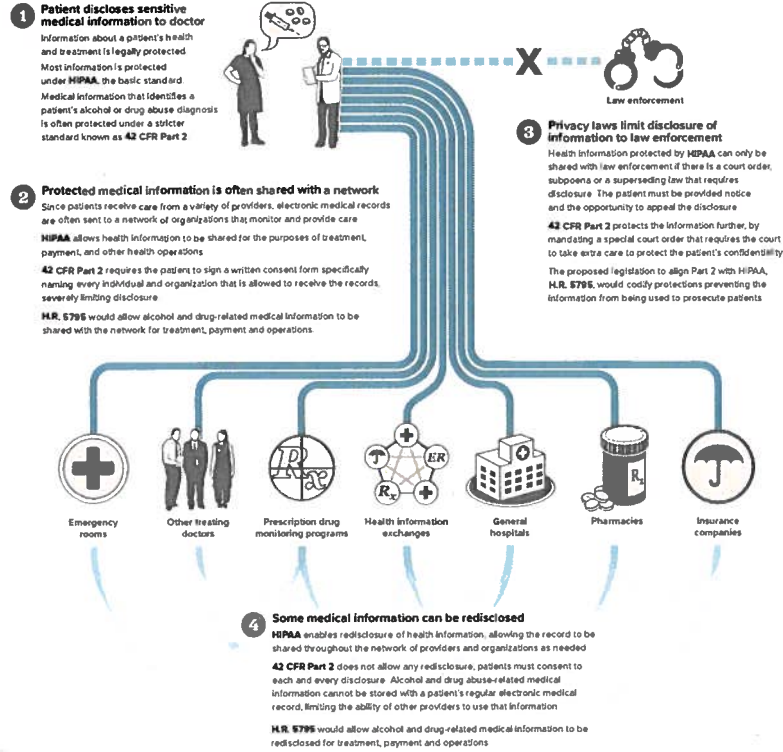
May 29, 2018

## Congress Considers Medical Privacy Overhaul to Combat the Opioid Epidemic

To protect individuals who seek medical treatment for alcohol and substance abuse problems, existing law strictly limits the sharing of alcohol and drug-related medical information under a statute known as 42 CFR Part 2. Lawmakers are worried that these legal protections are too cumbersome and have hampered the medical community's response to the opioid overdose epidemic.

To integrate alcohol and drug-related treatment with the rest of the medical system, House lawmakers have proposed legislation, H.R. 5795, that would align 42 CFR Part 2 with HIPAA — a more generally applicable law governing medical information sharing — for the purposes of treatment, payment and other operations. This would be an important change: HIPAA typically assumes that patients want their medical information shared with a network of providers, unless the patient says otherwise, whereas 42 CFR Part 2 assumes that patients do not want information shared without explicit consent.

### How legally protected medical information flows through a health care network



### Comparison of the major features of HIPAA and 42 CFR Part 2

	HIPAA	42 CFR Part 2
<b>General purpose</b>	<ul style="list-style-type: none"> <li>HIPAA establishes the minimum requirements for the protection of individuals' protected health information.</li> <li>Individuals have the right to access their records.</li> </ul>	<ul style="list-style-type: none"> <li>Part 2 creates stricter protections for medical records pertaining to alcohol and substance abuse, so that patients seeking treatment are not discouraged by potential legal and personal consequences.</li> <li>Programs have discretion to decide whether patients can view or obtain their records, unless state law says otherwise.</li> </ul>
<b>Entities governed</b>	<ul style="list-style-type: none"> <li>Applies to all health providers, health plans, clearing houses and any business associates that transmit any health information electronically.</li> </ul>	<ul style="list-style-type: none"> <li>Applies to any federally assisted program that provides alcohol or drug abuse diagnosis, treatment, or referral for treatment.</li> <li>A program is "federally assisted" if it: <ul style="list-style-type: none"> <li>Is federally authorized, licensed, certified or registered</li> <li>Receives any federal funding for any purpose</li> <li>Receives a grant of tax-exempt status or an allowance of tax deductions for contributions by the IRS</li> </ul> </li> </ul>
<b>Authorization for treatment and payment</b>	<ul style="list-style-type: none"> <li>Medical records governed by HIPAA can be disclosed without the patient's permission for treatment and payment procedures.</li> <li>Information shared with outside entities could be redisclosed to other parties for these purposes.</li> </ul>	<ul style="list-style-type: none"> <li>Individuals must authorize any disclosures with a written form that specifically names the persons or organizations that the records are being shared with.</li> <li>Information can not be redisclosed without specific authorization from the individual, except in the case of medical emergencies where the patient's life is clearly in danger.</li> </ul>
<b>Enforcement</b>	<ul style="list-style-type: none"> <li>Violators face civil fines enforced by the HHS Office for Civil Rights and state attorneys general.</li> <li>Further criminal penalties can be assessed on a case-by-case basis, especially if information is accessed under false pretenses or with malicious intent.</li> </ul>	<ul style="list-style-type: none"> <li>Violators are identified by the Substance Abuse and Mental Health Services Administration, and referred to the Justice Department for criminal charges.</li> </ul>
<b>Courts and law enforcement</b>	<ul style="list-style-type: none"> <li>Records can be shared without the individual's authorization in response to a court order or subpoena.</li> <li>The individual must be given notice and the opportunity to resist the disclosure with a protective order.</li> </ul>	<ul style="list-style-type: none"> <li>Records can not be disclosed without a special court order subject to additional confidentiality requirements under Part 2.</li> <li>A subpoena is not sufficient for disclosure; only a special court order under Part 2 rules can compel disclosure.</li> </ul>
<b>Public health reporting</b>	<ul style="list-style-type: none"> <li>As needed, information can be shared with public health authorities such as state and local health departments, FDA, CDC and the Occupational Safety and Health Administration.</li> </ul>	<ul style="list-style-type: none"> <li>Part 2 severely restricts the ability to share protected information with public health authorities. Any information that is shared must be stripped of information that could be used to identify a patient with an alcohol or substance abuse diagnosis.</li> </ul>

Note: This graphic does not constitute legal advice.

Sources: International Association of Privacy Professionals; Substance Abuse and Mental Health Services Administration; National Association for Addiction Professionals; By Tucker Duberry, POLITICO Pro DataPoint



PRESS RELEASE

## Bipartisan E&C, Senate HELP Leaders Press HHS for Answers on Health Care Cybersecurity Efforts

06.05.18

### Leaders Make Recommendations for Improvements, in Addition to Posing a Series of Questions

WASHINGTON, DC - Bipartisan and bicameral health care leaders today sent a letter to the Department of Health and Human Services (HHS) raising concerns about the department's implementation of a portion of the Cybersecurity Information Sharing Act (CISA) of 2015. The leaders requested information regarding the "Cyber Threat Preparedness Report" (CTPR), as well as other important status updates.

The letter was signed by Energy and Commerce Committee Chairman Greg Walden (R-OR), Senate Health, Education, Labor, and Pensions Committee Chairman Lamar Alexander (R-TN), Energy and Commerce Committee Ranking Member Frank Pallone, Jr. (D-NJ), and Senate Health, Education, Labor, and Pensions Committee Ranking Member Patty Murray (D-WA).

"While the CTPR provided a high-level overview of the cybersecurity responsibilities of each HHS office and operating division, the report omitted or lacked sufficient detail on many outstanding issues," wrote Walden, Pallone, Alexander, and Murray. "For example, HHS is both a regulator of the health care sector and the Sector Specific Agency (SSA) responsible for leading and providing guidance under the national critical infrastructure protection model. HHS must make clear how it plans to carry out this dual role and clearly communicate that plan to stakeholders, who must balance the need for support from HHS during cybersecurity incidents with the perceived risk that seeking support could lead to regulatory

enforcement actions. The CTPR did not mention this dual role or provide any clarification as to when HHS will act as a regulator or an SSA and how it will transition from one role to the other.”

**The bipartisan, bicameral leaders continued,** “Similarly, the CTPR failed to document HHS’s policies and procedures for responding to cybersecurity concerns or incidents that implicate multiple HHS operating divisions or offices. For example, a cybersecurity incident may initially affect a health care provider’s electronic health records, requiring a response from the Office of Civil Rights or the Office of the National Coordinator. If such an incident also compromised medical devices, the Food and Drug Administration likely would need to respond as well. The CTPR did not provide additional details or clarification as to how HHS would handle such an incident, when it would be appropriate for one HHS operating division or office to share information with another, or how such sharing would occur. This policy gap creates confusion for stakeholders and complicates the already difficult task of responding to cybersecurity incidents.”

The leaders also cited the Healthcare Cybersecurity and Communications Integration Center (HCCIC), and its omission from the CTPR, as well as other items of concern.

**The leaders detail some of those concerns, writing,** “Stakeholders have informed our staffs that they no longer understand whether the HCCIC still exists, who is running it, or what capabilities and responsibilities it has. Responses to committee requests to HHS for clarification on these questions remain vague at best, and the lack of documentation provided continues to undermine HHS’s efforts to address the HCCIC’s status.”

This letter follows one year of sustained oversight by Energy and Commerce of HHS’ health care cybersecurity. Those efforts include hearings by **#SubOversight**, as well as a series of letters.

Click **HERE** to read a copy of the letter.

###

**Congress of the United States**  
Washington, DC 20515

June 5, 2018

The Honorable Alex Azar  
Secretary  
U.S. Department of Health and Human Services  
200 Independence Avenue, S.W.  
Washington, DC 20201

Dear Secretary Azar:

We write to raise concerns regarding the Department of Health and Human Services' (HHS) implementation of Section 405 of the Cybersecurity Information Sharing Act of 2015 (CISA). Specifically, we request information regarding the "Cyber Threat Preparedness Report" (CTPR) required by 405(b) of the Act, as well as a status update regarding the alignment of "Health Care Industry Security Approaches" required by 405(d), and urge HHS to take prompt actions to address these outstanding issues. As cyber threats to the health care sector increase in frequency and severity, it is imperative that HHS provide clear and consistent leadership and direction to the sector regarding cyber threats.

On April 27, 2017, HHS delivered the CTPR to the House Committee on Energy and Commerce and the Senate Committee on Health, Education, Labor & Pensions (collectively, the Committees).<sup>1</sup> This report was intended to clarify HHS's internal roles, responsibilities, and preparedness to address cyber threats in the health care sector.<sup>2</sup> Since the preparation and delivery of the CTPR, however, HHS has continued to alter its cybersecurity strategy.

While the CTPR provided a high-level overview of the cybersecurity responsibilities of each HHS office and operating division, the report omitted or lacked sufficient detail on many outstanding issues. For example, HHS is both a regulator of the health care sector and the Sector Specific Agency (SSA) responsible for leading and providing guidance under the national critical infrastructure protection model. HHS must make clear how it plans to carry out this dual role and clearly communicate to stakeholders, who must balance the need for support from HHS during cybersecurity incidents with the perceived risk that seeking support could lead to regulatory enforcement actions. The CTPR did not mention this dual role or provide any clarification as to when HHS will act as a regulator or an SSA and how it will transition from one role to the other.

---

<sup>1</sup> *HHS Cyber Threat Preparedness Report*, DEP'T OF HEALTH AND HUMAN SERV. (2017) (hereafter *CTPR*). The CTPR is on file with both Committees.

<sup>2</sup> Consolidated Appropriations Act, 2016, Pub. L. 114-113, 129 STAT. 2981-2984, 18 Dec. 2015, <https://www.gpo.gov/fdsys/pkg/PLAW-114publ113/pdf/PLAW-114publ113.pdf> (hereafter *CISA 2015*). The Cybersecurity Information Sharing Act of 2015 was passed as part of the larger bill, with the health care cybersecurity portions contained in Section 405.

Similarly, the CTPR failed to document HHS's policies and procedures for responding to cybersecurity concerns or incidents that implicate multiple HHS operating divisions or offices. For example, a cybersecurity incident may initially affect a health care provider's electronic health records, requiring a response from the Office of Civil Rights or the Office of the National Coordinator. If such an incident also compromised medical devices, the Food and Drug Administration likely would need to respond as well. The CTPR did not provide additional details or clarification as to how HHS would handle such an incident, when it would be appropriate for one HHS operating division or office to share information with another, or how such sharing would occur. This policy gap creates confusion for stakeholders and complicates the already difficult task of responding to cybersecurity incidents.

Most notably, the CTPR lacked information regarding the Healthcare Cybersecurity and Communications Integration Center (HCCIC). The HCCIC was announced during a panel appearance in April 2017 by the then-HHS Chief Information Security Officer, who stated, "HHS is building a health care information collaboration and analysis center, just like the [Department of Homeland Security's] NCCIC, only focused on health care."<sup>3</sup> Few additional details were provided, offering little clarity on how the HCCIC would fit into the larger health care cybersecurity picture and raising concerns that the HCCIC could duplicate work by entities such as the NCCIC or National Health-Information Sharing and Analysis Center (NH-ISAC).<sup>4</sup> Now a year after the announcement, the clearest public information regarding the HCCIC comes from written testimony submitted by HHS to the Energy and Commerce Committee for a June 2017 hearing.<sup>5</sup>

That testimony stated:

"HHS supports the [Healthcare and Public Health] sector through the establishment and operation of the [HCCIC]. The HCCIC has three high level goals:

- Strengthen engagement across HHS Operating Divisions;
- Strengthen reporting and increase awareness of the health care cyber threats across the HHS enterprise; and
- Enhance public-private partnerships through regular engagement and outreach."<sup>6</sup>

---

<sup>3</sup> Nicole Ogrysko, *HHS to stand up its own version of the NCCIC for health*, FEDERAL NEWS RADIO (Apr. 20, 2017), <https://federalnewsradio.com/health-it/2017/04/hhs-to-stand-up-its-own-version-of-the-nccic-for-health/>.

<sup>4</sup> Letter from the Hon. Ron Johnson and the Hon. Claire McCaskill, S. Comm. On Homeland Sec. and Gov't Affairs, to the Hon. Tom Price, Sec'y, US. Dep't of Health and Human Serv. (June 21, 2017).

<sup>5</sup> *Testimony from Emery Csulak, Steven Curren, and Leo Scanlon on Examining the Role of the Department of Health and Human Services in Health Care Cybersecurity before Committee on Energy and Commerce*, U.S. DEP'T OF HEALTH AND HUMAN SERV. (June 8, 2017), <https://www.hhs.gov/about/agencies/asl/testimony/2017-06/examining-role-department-health-and-human-services.html>.

<sup>6</sup> *Id.*



If HHS envisions the HCCIC as a mechanism to fulfill many of its cybersecurity goals and responsibilities, including those that HHS already assigned to various divisions and subdivisions, it is unclear why HHS omitted the HCCIC from the CTPR. The HCCIC was announced in April 2017 with the intention that it would be operational by June 2017. The absence of the HCCIC within the CTPR in May of 2017 renders the report outdated, incomplete, and inaccurate.

Further, there is significant confusion regarding the role and status of the HCCIC:

1. The global health care sector suffered a massive ransomware outbreak known as WannaCry in May 2017, which posed such a severe threat to the United States health care sector that HHS activated the HCCIC a month early.<sup>7</sup> The United States was ultimately spared the damage suffered by other countries, which media reports have attributed to the timely intervention of an unaffiliated security researcher, rather than specific actions taken by HHS or health care stakeholders.<sup>8</sup> HHS nonetheless credits the HCCIC and the capabilities it enabled for the relatively smooth sector response to the crisis.<sup>9</sup>
2. In September 2017, HHS temporarily reassigned two senior officials responsible for the day-to-day operation of the HCCIC to unrelated duties.<sup>10</sup> Memoranda provided to the affected officials stated the reassignments were to “permit the Agency time to review allegations raised against the Office of the Chief Information Officer (OCIO), Office of Information Security.”<sup>11</sup> HHS’s removal of senior HCCIC personnel has had undeniable impacts on HCCIC and HHS’s cybersecurity capabilities.

Stakeholders have informed our staffs that they no longer understand whether the HCCIC still exists, who is running it, or what capabilities and responsibilities it has. Responses to committee requests to HHS for clarification on these questions remain vague at best, and the lack of documentation provided continues to undermine HHS’s efforts to address the HCCIC’s status.<sup>12</sup>

Further, HHS’s private and public representation of the HCCIC as central to its cybersecurity efforts has confounded efforts to understand how HHS meets its obligations related to cybersecurity given the HCCIC’s instability. The HCCIC’s surprise announcement, initial

---

<sup>7</sup> Lily Hay Newman, *The Ransomware Meltdown Experts Warned About is Here*, WIRED, Mar. 12, 2017, <https://www.wired.com/2017/05/ransomware-meltdown-experts-warned/>.

<sup>8</sup> Lily Hay Newman, *How An Accidental ‘Kill Switch’ Slowed Friday’s Massive Ransomware Attack*, WIRED, May 13, 2017, <https://www.wired.com/2017/05/accidental-kill-switch-slowed-fridays-massive-ransomware-attack/>.

<sup>9</sup> *Examining the Role of the Department of Health and Human Services in Health Care Cybersecurity: Hearing Before the H. Comm. on Energy and Commerce*, 115th Cong. (June 8, 2017), <http://docs.house.gov/meetings/IF/IF02/20170608/106078/HHRG-115-IF02-Transcript-20170608.pdf> (See statements from Steve Curren and Leo Scanlon regarding HCCIC and the WannaCry outbreak).

<sup>10</sup> Letter from the Hon. Greg Walden, Hon. Frank Pallone, Jr., and Hon. Diana DeGette, H. Comm. on Energy and Commerce, to Eric Hargan, Acting Sec’y, Dep’t of Health and Human Serv. (Nov. 14, 2017), <https://energycommerce.house.gov/wp-content/uploads/2017/11/20171114HHS.pdf>.

<sup>11</sup> *Id.* at 1.

<sup>12</sup> Briefings with Committee staff.

success, and subsequent troubles, combined with the inadequacies in the CTPR, have exacerbated the very issues that CISA was intended to address. HHS's decision to present to our Committees a report that was outdated, incomplete, and inaccurate raises concerns about HHS's ability to address the growing number and severity of cyber threats facing the health care sector.

Additionally, 405(d) of CISA required HHS to establish a "collaborative process" with other government officials and health care industry stakeholders to align and publish "Health Care Industry Security Approaches." CISA was signed into law on December 18, 2015, but as of this writing, HHS still has not produced the "common set of voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes" required by the law.

Therefore, we respectfully suggest that HHS take the following actions:

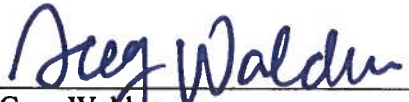
1. Update the CTPR to include any and all changes, modifications, and evolutions that have occurred in HHS cybersecurity strategies since its original drafting.
2. Include within the updated CTPR a detailed explanation of the HCCIC, its roles and responsibilities, how its work and operations intersect with the NCCIC and the NH-ISAC, and how it fits into HHS's broader cybersecurity capabilities and responsibilities.
3. Add sections to the CTPR specifically addressing:
  - a. The internal coordination between HHS offices and operating divisions that have regulatory authority with regards to health care cybersecurity, and how those offices will coordinate their efforts to provide a "whole-of-department" response to modern cybersecurity challenges;
  - b. The role of HHS, including the responsibility of HHS offices and operating divisions, in securing its own internal information systems as compared to its role in providing guidance, information, education, training, and assistance to the health care sector, and how it will differentiate between those two roles; and
  - c. The challenges HHS faces as both the regulator and the Sector Specific Agency for health care, including how it will differentiate and transition between these two roles.
4. Provide the date you expect to release the alignment of "Health Care Industry Security Approaches" required by 405(d) of CISA.


We appreciate your prompt attention to these suggested actions and request that HHS respond by no later than June 19, 2018. We look forward to working with you constructively to improve HHS cybersecurity efforts. If you have any questions regarding this request, please contact Jessica Wilkerson or Alan Slobodin of the House Committee on Energy and Commerce Majority staff at (202) 225-2927, Julie Babayan or Kevin McAloon of the House Committee on Energy and Commerce Minority staff at (202) 226-3400, Bobby McMillin of the Senate


Letter to the Honorable Alex Azar  
Page 5


Committee on Health, Education, Labor, and Pensions Majority staff at (202) 224-1284, and Elizabeth Letter of the Senate Committee on Health, Education, Labor, and Pensions Minority staff at (202) 224-0767.

Sincerely,

  
\_\_\_\_\_  
Greg Walden  
Chairman  
Committee on Energy and Commerce  
U.S. House of Representatives

  
\_\_\_\_\_  
Lamar Alexander  
Chairman  
Committee on Health, Education, Labor,  
and Pensions  
U.S. Senate

  
\_\_\_\_\_  
Frank Pallone Jr.  
Ranking Member  
Committee on Energy and Commerce  
U.S. House of Representatives

  
\_\_\_\_\_  
Patty Murray  
Ranking Member  
Committee on Health, Education, Labor,  
and Pensions  
U.S. Senate



## Viewpoint

May 24, 2018

# HIPAA and Protecting Health Information in the 21st Century

I. Glenn Cohen, JD<sup>1</sup>; Michelle M. Mello, JD, PhD<sup>2</sup>

Author Affiliations [Article Information](#)

*JAMA*. Published online May 24, 2018. doi:10.1001/jama.2018.5630

In March 2018, the Trump administration announced a new initiative, MyHealthEData, to give patients greater access to their electronic health record and insurance claims information.<sup>1</sup> The Centers for Medicare & Medicaid Services will connect Medicare beneficiaries with their claims data and increase pressure on health plans and health care organizations to use systems that allow patients to access and send their health information where they like.

MyHealthEData is part of a broader movement to make greater use of patient data to improve care and health. The movement seeks to make information available wherever patients receive care and allow patients to share information with apps and other online services that may help them manage their health. At the population level, this approach may help identify optimal treatments and ways of delivering them and also connect patients with health services and products that may benefit them. Analysis of deidentified patient information has long been the foundation of evidence-based care improvement, but the 21st century has brought new opportunities. With developments in information technology and computational science that support the analysis of massive data sets, the “big data” era has come to health services research.

For all its promise, the big data era carries with it substantial concerns and potential threats. Part of what enables individuals to live full lives is the knowledge that certain personal information is not on view unless that person decides to share it, but that supposition is becoming illusory. The increasing availability and exchange of health-related information will support advances in health care and public health but will also facilitate invasive marketing and discriminatory practices that evade current antidiscrimination laws.<sup>2</sup> As the recent scandal involving Facebook and Cambridge Analytica shows, a further risk is that private information may be used in ways that have not been authorized and may be considered objectionable. Reinforcing such concerns is the stunning report that Facebook has been approaching health care organizations to try to obtain deidentified patient data to link those data to individual Facebook users using “hashing” techniques.<sup>3</sup>

Given these concerns, it is timely to reexamine the adequacy of the Health Insurance Portability and Accountability Act (HIPAA), the nation's most important legal safeguard against unauthorized disclosure and use of health information. Is HIPAA up to the task of protecting health information in the 21st century?

## HIPAA Framework for Information Disclosure

HIPAA was considered ungainly when it first became law, a complex amalgamation of privacy and security rules with a cumbersome framework governing disclosures of protected health information. HIPAA has been derided for being too narrow—it applies only to a limited set of “covered entities,” including clinicians, health care facilities, pharmacies, health plans, and health care clearinghouses—and too onerous in its requirements for patient authorization for release of protected health information. Over time, however, HIPAA has proved surprisingly functional. Particularly after being amended in the 2009 HITECH (ie, the Health Information Technology for Economic and Clinical Health) Act to address challenges arising from electronic health records, HIPAA has accomplished its primary objective: making patients feel safe giving their physicians and other treating clinicians sensitive information while permitting reasonable information flows for treatment, operations, research, and public health purposes.

HIPAA's Privacy Rule generally requires written patient authorization for disclosure of identifiable health information by covered entities unless a specific exception applies, such as treatment or operations. Researchers may obtain protected health information (PHI) without patient authorization if a privacy board or institutional review board (IRB) certifies that obtaining authorization is impracticable and the research poses minimal risk. The investigators can obtain a limited data set that excludes direct identifiers (eg, names, medical record numbers) without patient authorization if they agree to certain security and confidentiality measures. Importantly, data sets from which a broader set of 18 types of potentially identifying information (eg, county of residence, dates of care) has been removed may be shared freely for research or commercial purposes.

This has been a serviceable framework for regulating the flow of PHI for research, but the big data era raises new challenges. HIPAA contemplated that most research would be conducted by universities and health systems, but today much of the demand for information emanates from private companies at which IRBs and privacy boards may be weaker or nonexistent. Additionally, removing identifiers to produce a limited or deidentified data set reduces the value of the data for many analyses. Moreover, the increasing availability of information generated outside health care settings, coupled with advances in computing, undermines the historical assumption that data can be forever deidentified.<sup>4</sup> Startling demonstrations of the power of data triangulation to reidentify individuals have offered a glimpse of a very different future, one in which preserving privacy and the big data enterprise are on a collision course.<sup>4</sup>

It will be difficult to reconcile the potential of big data with the need to protect individual privacy. One reform approach would be data minimization (eg, limiting the upstream collection of PHI or imposing time limits on data retention),<sup>5</sup> but this approach would

sacrifice too much that benefits clinical practice. Another solution involves revisiting the list of identifiers to remove from a data set. There is no doubt that regulations should reflect up-to-date best practices in deidentification.<sup>2,4</sup> However, it is questionable whether deidentification methods can outpace advances in reidentification techniques given the proliferation of data in settings not governed by HIPAA and the pace of computational innovation. Therefore, expanding the penalties and civil remedies available for data breaches and misuse, including reidentification attempts, seems desirable.

## Limited Reach of HIPAA

HIPAA “attaches (and limits) data protection to traditional health care relationships and environments.”<sup>6</sup> The reality of 21st-century United States is that HIPAA-covered data form a small and diminishing share of the health information stored and traded in cyberspace. Such information can come from well-known sources, such as apps, social media, and life insurers, but some information derives from less obvious places, such as credit card companies, supermarkets, and search engines. For example, non–health information that supports inferences about health is available from purchases that users make on Amazon; user-generated content that conveys information about health appears in Facebook posts; and health information is generated by entities not covered by HIPAA when over-the-counter products are purchased in drugstores. Because HIPAA’s protection applies only to certain entities, rather than types of information, a world of sensitive information lies beyond its grasp.<sup>2</sup>

HIPAA does not cover health or health care data generated by noncovered entities or patient-generated information about health (eg, social media posts). It does not touch the huge volume of data that is not directly about health but permits inferences about health. For example, information about a person’s physical activity, income, race/ethnicity, and neighborhood can help predict risk of cardiovascular disease. The amount of such data collected and traded online is increasing exponentially and eventually may support more accurate predictions about health than a person’s medical records.<sup>2</sup>

Statutes other than HIPAA protect some of these non–health data, including the Fair Credit Reporting Act, the Family Educational Rights and Privacy Act of 1974, and the Americans with Disabilities Act of 1990.<sup>7</sup> However, these statutes do not target health data specifically; while their rules might be sensible for some purposes, they are not designed with health in mind. For instance, the Family Educational Rights and Privacy Act of 1974 has no public health exception to the obligation of nondisclosure.<sup>7</sup>

To ensure adequate protection of the full ecosystem of health-related information, a solution would be to expand HIPAA’s scope. However, the Privacy Rules’ design (ie, the reliance on IRBs and privacy boards, the borders through which data may not travel) is not a natural fit with the variety of nonclinical settings in which health data are collected and exchanged.<sup>8</sup>

The better course is adopting a separate regime for data that are relevant to health but not covered by HIPAA. One option that has been proposed is to enact a general rule protecting health data that specifies further, custodian-specific rules; another is to follow the European Union's new General Data Protection Regulation in setting out a single regime applicable to custodians of all personal data and some specific rules for health data. The latter has the appeal of reaching into non-health data that support inferences about health. Any new regulatory steps should be guided by 3 goals: avoid undue burdens on health research and public health activities, give individuals agency over how their personal information is used to the greatest extent commensurable with the first goal, and hold data users accountable for departures from authorized uses of data.

Rethinking regulation should also be part of a broader public process in which individuals in the United States grapple with the fact that today, nearly everything done online involves trading personal information for things of value. When such trades are made explicit, as when drugstores offered customers \$50 to grant expanded rights to use their health data, they tend to draw scorn.<sup>9</sup> However, those are just amplifications of everyday practices in which consumers receive products and services for free or at low cost because the sharing of personal information allows companies to sell targeted advertising, "deidentified" data, or both.

## Conclusions

Improved public understanding of these practices may lead to the conclusion that such deals are in the interest of consumers and only abusive practices need be regulated. Or it may create pressure for better corporate privacy practices. Some consumers may take steps to protect the information they care most about, such as purchasing a pregnancy test with cash. Shaping health information privacy protections in the 21st century requires savvy lawmaking as well as informed digital citizens.

[Back to top](#)

## Article Information

**Corresponding Author:** Michelle M. Mello, JD, PhD, Stanford Law School, 559 Nathan Abbott Way, Stanford, CA 94305 ([mmello@law.stanford.edu](mailto:mmello@law.stanford.edu)).

**Published Online:** May 24, 2018. doi:[10.1001/jama.2018.5630](https://doi.org/10.1001/jama.2018.5630)

**Conflict of Interest Disclosures:** Both authors have completed and submitted the ICMJE Form for Disclosure of Potential Conflicts of Interest. Dr Mello has served as a consultant to CVS/Caremark. No other conflicts were disclosed.

**Funding/Support:** Dr Cohen's research reported in this Viewpoint was supported by the Collaborative Research Program for Biomedical Innovation Law, which is a scientifically independent collaborative research program supported by Novo Nordisk Foundation (grant NNF17SA0027784).



**Role of the Funder/Sponsor:** The funder had no role in the preparation, review, or approval of the manuscript and decision to submit the manuscript for publication.

## References

1. *Trump Administration announces MyHealthEData initiative at HIMSS18.* Centers for Medicare and Medicaid Services. <https://www.cms.gov/Newsroom/MediaReleaseDatabase/Fact-sheets/2018-Fact-sheets-items/2018-03-06.html>. Accessed April 3, 2018.
2. *Health information privacy beyond HIPAA: a 2018 environmental scan of major trends and challenges.* National Committee on Vital and Health Statistics. [https://www.ncvhs.hhs.gov/wp-content/uploads/2018/02/NCVHS-Beyond-HIPAA\\_Report-Final-02-08-18.pdf](https://www.ncvhs.hhs.gov/wp-content/uploads/2018/02/NCVHS-Beyond-HIPAA_Report-Final-02-08-18.pdf). Accessed April 3, 2018.
3. Farr C. *Facebook sent a doctor on a secret mission to ask hospitals to share patient data.* CNBC. <https://www.cnbc.com/2018/04/05/facebook-building-8-explored-data-sharing-agreement-with-hospitals.html>. Accessed April 10, 2018.
4. *Recommendations on de-identification of protected health information under HIPAA.* National Committee on Vital and Health Statistics. <https://www.ncvhs.hhs.gov/wp-content/uploads/2013/12/2017-Ltr-Privacy-Deidentification-Feb-23-Final-w-sig.pdf>. Accessed April 3, 2018.
5. Terry NP. Protecting patient privacy in the age of big data. *UMKC Law Rev.* 2012;81(2):385-415.[Google Scholar](#)
6. Terry NP. Big data proxies and health privacy exceptionalism. *Health Matrix Clevel.* 2014;24(1):65-108.[PubMedGoogle Scholar](#)
7. Riley MF. Big Data, HIPAA, and the Common Rule. In: Cohen IG, Lynch HF, Veyena E, Gasser U, eds. *Big Data, Health Law, and Bioethics*. New York, NY: Cambridge Univ. Press; 2018.
8. Terry NP. Regulatory disruption and arbitrage in health-care data protection. *Yale J Health Policy Law Ethics.* 2017;17(1):143-207.[Google Scholar](#)
9. Robbins R. *At Walgreens and CVS, a push to collect customer health data by dangling discounts.* STAT. <https://www.statnews.com/2015/11/23/pharmacies-collect-personal-data/>. Accessed May 14, 2018



## SPECIAL ARTICLE

# Clinical Trial Participants' Views of the Risks and Benefits of Data Sharing

Michelle M. Mello, J.D., Ph.D., Van Lieu, B.S.,  
and Steven N. Goodman, M.D., Ph.D.

---

**ABSTRACT**

---

**BACKGROUND**

Sharing of participant-level clinical trial data has potential benefits, but concerns about potential harms to research participants have led some pharmaceutical sponsors and investigators to urge caution. Little is known about clinical trial participants' perceptions of the risks of data sharing.

**METHODS**

We conducted a structured survey of 771 current and recent participants from a diverse sample of clinical trials at three academic medical centers in the United States. Surveys were distributed by mail (350 completed surveys) and in clinic waiting rooms (421 completed surveys) (overall response rate, 79%).

**RESULTS**

Less than 8% of respondents felt that the potential negative consequences of data sharing outweighed the benefits. A total of 93% were very or somewhat likely to allow their own data to be shared with university scientists, and 82% were very or somewhat likely to share with scientists in for-profit companies. Willingness to share data did not vary appreciably with the purpose for which the data would be used, with the exception that fewer participants were willing to share their data for use in litigation. The respondents' greatest concerns were that data sharing might make others less willing to enroll in clinical trials (37% very or somewhat concerned), that data would be used for marketing purposes (34%), or that data could be stolen (30%). Less concern was expressed about discrimination (22%) and exploitation of data for profit (20%).

**CONCLUSIONS**

In our study, few clinical trial participants had strong concerns about the risks of data sharing. Provided that adequate security safeguards were in place, most participants were willing to share their data for a wide range of uses. (Funded by the Greenwall Foundation.)

From the Department of Health Research and Policy, Stanford University School of Medicine (M.M.M., V.L., S.N.G.) and Stanford Law School (M.M.M.) — both in Stanford, CA. Address reprint requests to Dr. Mello at Stanford Law School, 559 Nathan Abbott Way, Stanford, CA 94305, or at [mmello@law.stanford.edu](mailto:mmello@law.stanford.edu).

N Engl J Med 2018;378:2202-11.  
DOI: 10.1056/NEJMsa1713258  
Copyright © 2018 Massachusetts Medical Society.

**W**E ARE RAPIDLY MOVING TOWARD A world in which broad sharing of participant-level clinical trial data is the norm.<sup>1-4</sup> The European Medicines Agency has implemented a policy to expand public access to data concerning products it approves,<sup>5,6</sup> the Food and Drug Administration is considering how to expand access to data pooled within a product class,<sup>7</sup> major research sponsors<sup>8-12</sup> and journal editors<sup>13</sup> have begun promoting data sharing, and lawmakers' interest<sup>14</sup> has resulted in legislation authorizing the National Institutes of Health to require all of its grantees to share data.<sup>15,16</sup> Pharmaceutical industry associations have committed to making data more accessible,<sup>17</sup> and several data platforms are now available.<sup>11,18-21</sup>

Previous work has identified diverse potential benefits of expanding access to participant-level data.<sup>1,4,22</sup> These benefits include deterring inaccurate reporting of trial results,<sup>4,23,24</sup> accelerating scientific discovery,<sup>25</sup> and exploring questions that are not answerable within individual trials.<sup>4,26</sup> In addition, data sharing helps fulfill the ethical obligation to make the most of research participants' contributions to science.<sup>13,27-30</sup>

Yet some investigators and industry sponsors of clinical trials have expressed hesitancy about the swift move toward broad data sharing. These groups have shifted from opposing data sharing to supporting it<sup>31,32</sup>; however, several concerns have led them to urge caution, limit what they share, and resist some initiatives as going too far.<sup>32,33</sup> Chief among these are concerns about potential harm to research participants.<sup>17,32,34,35</sup> Sponsors and investigators express worries that participants' privacy cannot be adequately protected, particularly in light of the fact that experts have demonstrated that it is possible to reidentify participant-level data.<sup>35-39</sup> Some pharmaceutical company representatives warn that the threat to privacy posed by data sharing will chill willingness to participate in trials, thereby delaying the availability of new therapies.<sup>36,38</sup>

It is unclear to what extent participants in clinical trials share these concerns. There is a large body of empirical literature concerning people's preferences related to biobanking<sup>40,41</sup> but not about clinical trials. When patient advocacy groups have spoken about data sharing, they have sometimes been challenged as parroting

the views of pharmaceutical companies that financially support them rather than conveying trial participants' views.<sup>42</sup> One commentator recently remarked that in debates about data sharing, "Both sides claim to have the patient's and the public's best interests at heart, but not many partisans of either camp have asked patients what those interests are."<sup>43</sup> To investigate this issue, we surveyed a large sample of participants in a diverse group of clinical trials.

---

## METHODS

---

### PARTICIPANTS

Survey participants had been enrolled, or were the parent or guardian of someone who had been enrolled, in an interventional clinical trial within the previous 2 years. We obtained agreement from nine principal investigators (PIs) in clinical trials at three academic medical centers to facilitate access to their trial participants, including one PI who provided access to all trials in the university's Clinical and Translational Science Institute.

We aimed for a broadly representative sample of trials that would be sufficient to provide at least 1200 potential survey participants. We selected the PIs we approached on the basis of personal contacts and stressed our interest in ensuring representation of racial and ethnic minority groups and persons with major health problems.

The final sample included both community-based trials (e.g., involving smoking cessation or diabetes prevention) and hospital-based trials (e.g., involving cancer or kidney disease). Within these trials, all the participants were eligible for the survey unless the trial team judged them as having cognitive impairment or being unable to respond to questions in English. The study was approved by the institutional review boards at Stanford and at the medical centers that provided access to the trial participants.

### QUESTIONNAIRE DEVELOPMENT

A 10-page structured survey questionnaire was used to elicit clinical trial participants' views on the sharing of data from clinical trials. Details of the survey development work, which included the use of focus groups, consultation with ex-

perts and community advisory boards, and pilot testing, are provided in Sections 2 and 5 in the Supplementary Appendix, available with the full text of this article at NEJM.org.

The questionnaire provided plain-English definitions of clinical trial, data sharing, and clinical trial data (Section 6 in the Supplementary Appendix). It included reminders that the survey was asking about sharing of individual-level information about trial participants, not research results, and that respondents should assume that the data were deidentified.

#### SURVEY ADMINISTRATION

Clinical trial PIs chose from among three methods of survey delivery: email, regular mail, or in-person distribution in study clinic waiting rooms. Four PIs chose regular mail, four chose the clinic, and one used both. All surveys were completed on paper, and the clinic staff's interaction with respondents was limited to a receptionist or research assistant handing out and collecting the questionnaires (Section 1 in the Supplementary Appendix).

The surveys were accompanied by informed consent information and a \$40 gift card. The responses were identified by participant identification number only.

#### STATISTICAL ANALYSIS

Responses were manually entered into a database in the Stanford University REDCap Survey system<sup>44</sup> and analyzed with the use of Stata software, version 13 (StataCorp). In addition to univariate statistics and cross-tabulations, multivariable logistic-regression models were run to identify predictors of the expression of negative views of data sharing. The following outcomes were modeled: perceiving the potential negative consequences of data sharing to outweigh the benefits (either strongly, moderately, or a little); being somewhat or very unlikely to allow one's own trial data to be shared with scientists in not-for-profit settings; and being somewhat or very unlikely to allow data to be shared with scientists in drug companies. To account for missing data, multiple imputation was performed with the Stata "mi" platform. Details of the model construction and regression results are provided in Sections 3 and 4 in the Supplementary Appendix.

## RESULTS

### SAMPLE CHARACTERISTICS

Completed surveys were received from 771 of the 978 invited trial participants (79%) and included 350 mailed surveys and 421 surveys completed in the clinic (Section 1 in the Supplementary Appendix). Respondents were fairly evenly distributed across the three academic medical centers (33%, 27%, and 40%) and were drawn from 119 different trials. Percentages based on the 771 respondents have a 95% confidence interval no wider than  $\pm 3.6$  percentage points.

Table 1, and Table S6 in the Supplementary Appendix, show the characteristics of the sample. Within the previous 2 years, 42% of the respondents had participated in a clinical trial as a person with the health condition being studied, 55% as a healthy volunteer or person at risk for the studied health condition, and 3% as both. The two most common topics studied in the trials were diabetes and issues related to nutrition, weight, and vitamin supplementation. A total of 90% of respondents were trial participants themselves, and 7% were parents of participants. More than 94% of the respondents reported having had positive experiences as clinical trial participants. Half were motivated to participate in the trial by the prospect of a health benefit, 33% by altruism, and 16% by other factors.

### PERCEIVED RISKS OF DATA SHARING

For 9 of 11 potential consequences of data sharing, less than 10% of the respondents said they were "very concerned" and less than one third were "very" or "somewhat" concerned about the risk (Fig. 1). A total of 20% to 26% of the respondents were very or somewhat concerned about discrimination, reidentification, and exploitation of data for profit. Respondents were more concerned that data sharing could deter people from enrolling in clinical trials (37%), that companies might use the information for marketing purposes (34%), or that their data could be stolen (30%). Asked to select the most important potential risk, respondents expressed divergent views, with the most common choices being that the information might be stolen (15%) or used for marketing purposes (11%) and that others might be more reluctant to en-

roll in clinical trials if they knew their data would be shared (10%) (Table S7 in the Supplementary Appendix).

#### PERCEIVED BENEFITS OF DATA SHARING

Strong majorities of respondents (67% to 82%) believed that data sharing would yield “a great deal” or “a lot” of several benefits (Fig. 2). In contrast, 43% believed it would help lawyers prove their case in product liability lawsuits. When respondents were asked to choose the most important benefit of data sharing, the most popular choices were making sure people’s participation in clinical trials leads to the most scientific benefit possible (18%) and helping to get answers to scientific questions faster (17%) (Table S8 in the Supplementary Appendix). More than 85% of respondents expected that scientists in universities and other not-for-profit settings would benefit “a great deal” or “a lot” from data sharing; 81% of respondents had this expectation for physicians taking care of patients, 79% for companies developing medical products, and 72% for patients (Table S9 in the Supplementary Appendix).

#### OVERALL SUPPORT FOR DATA SHARING

In response to a question at the end of the survey, 82% of respondents indicated that they perceived that the benefits of data sharing outweighed the negative aspects, 8% felt the negative aspects outweighed the benefits, and 10% considered them equal (Table S10 in the Supplementary Appendix).

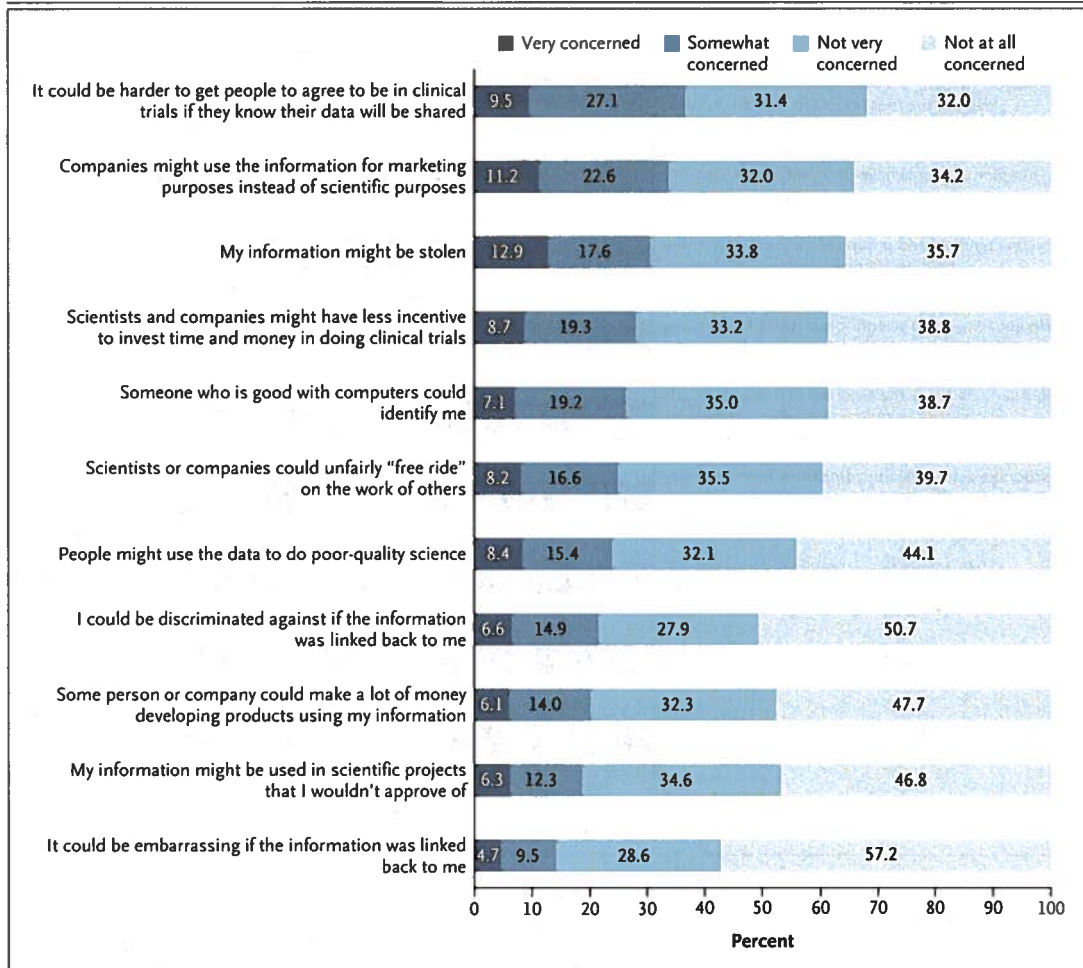
A total of 93% of respondents said they were very (69%) or moderately (24%) likely to allow their clinical trial data to be shared with scientists in universities and other not-for-profit organizations (Table 2), and 4% were very or somewhat unlikely to share. Although respondents had less trust in drug companies (18% trusted them a great deal or a lot) and health insurance companies (15%) than in universities (63%), 82% reported that they would be very or somewhat willing to share data with for-profit companies, whereas 8% were very or somewhat unwilling to share (Table 2, and Table S11 in the Supplementary Appendix).

Willingness to share data varied little according to the purpose for which it would be used — with the exception of its use in lawsuits, al-

**Table 1. Sample Characteristics as Reported in the Survey.\***

Characteristic	No. of Participants/ Total No. (%) (N = 771)
Female sex	380/762 (49.9)
Age	
<25 yr	63/762 (8.3)
25–44 yr	177/762 (23.2)
45–64 yr	286/762 (37.5)
≥65 yr	236/762 (31.0)
Hispanic ethnic group	101/759 (13.3)
Race	
White	518/768 (67.4)
Black or African American	113/768 (14.7)
American Indian or Alaskan Native	51/768 (6.6)
Asian	25/768 (3.3)
Other	61/768 (7.9)
Education	
Less than high school	40/752 (5.3)
High-school diploma	125/752 (16.6)
Some college	206/752 (27.4)
College degree	238/752 (31.6)
Graduate degree	143/752 (19.0)
Annual family income	
Less than \$15,000 to \$24,999	173/742 (23.3)
\$25,000 to \$54,999	206/742 (27.8)
\$55,000 to \$99,999	189/742 (25.5)
\$100,000 or higher	174/742 (23.5)
Health status	
Excellent	168/757 (22.2)
Good	420/757 (55.5)
Fair	156/757 (20.6)
Poor	13/757 (1.7)
Trial topic	
Nutrition, weight, or vitamins	172/771 (22.3)
Diabetes	172/771 (22.3)
Cardiovascular disease	71/771 (9.2)
Aging, neurodegenerative disease, or memory	64/771 (8.3)
Tobacco use	52/771 (6.7)
Liver disease	49/771 (6.4)
Mental illness	41/771 (5.3)
Cancer	39/771 (5.1)
Kidney disease	26/771 (3.4)
Other	85/771 (11.0)
Overall experience as a trial participant	
Very positive	573/752 (76.2)
Somewhat positive	136/752 (18.1)
Neither positive nor negative	34/752 (4.5)
Somewhat negative	9/752 (1.2)
Very negative	0

\* All characteristics with exception of trial topic were reported by the participant in the survey. Percentages may not total 100 because of rounding. Further details are provided in Section 6 in the Supplementary Appendix.



**Figure 1. Level of Concern about Potential Consequences of Data Sharing.**

Shown are the responses to an item worded as "How concerned are you about the following potential consequences of sharing *anonymous, individual* clinical trial data?" Numbers were rounded to the nearest tenth. The accuracy (95% confidence interval) of the percentages close to 50% is  $\pm 3.6$  percentage points, diminishing to  $\pm 2.2$  percentage points for percentages close to 10%.

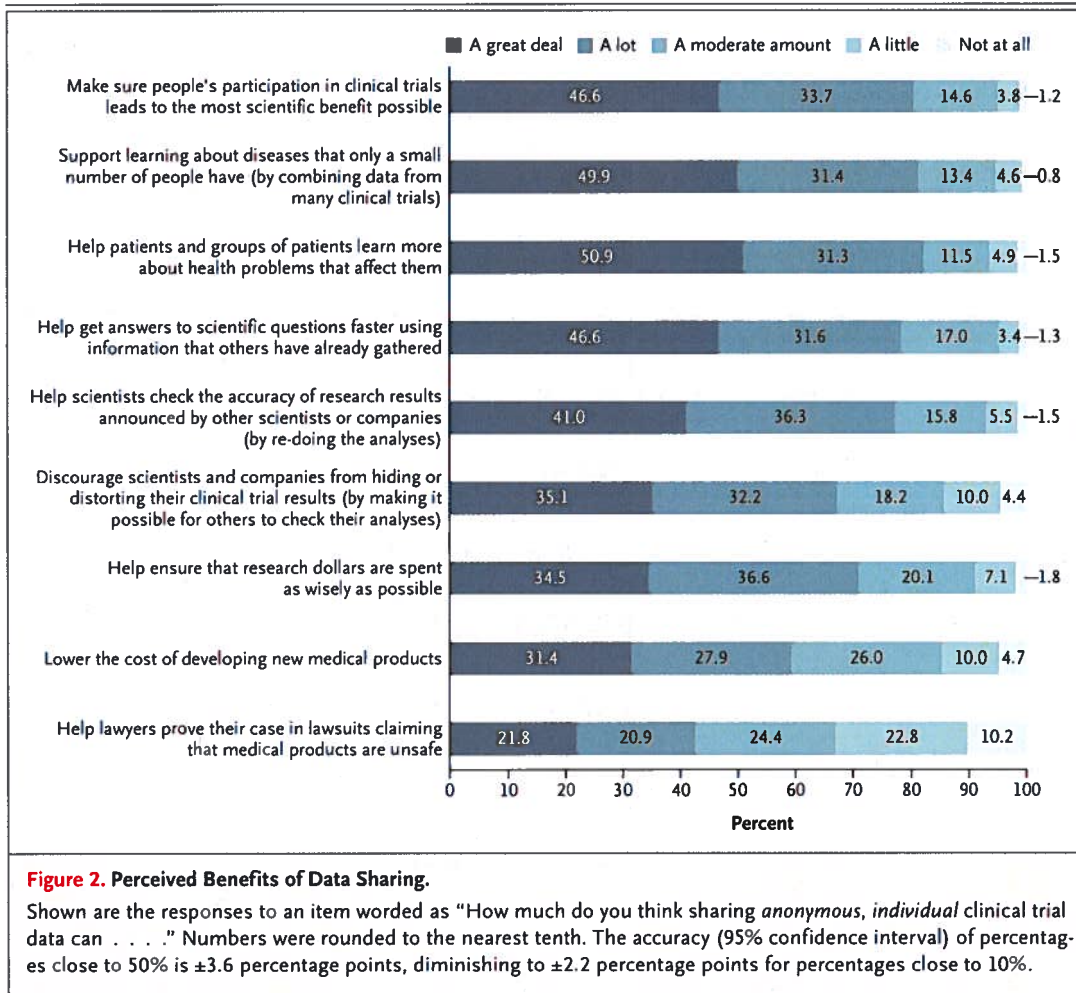
though a majority of respondents were still willing to share even for that purpose (Table 2). No appreciable differences were found between uses that did and uses that did not benefit the participant directly or between uses for verifying previous research results and uses for making new discoveries.

Among the write-in comments, the most dominant theme was the need to help others as much as possible. Many commenters expressed confidence in the deidentification of data. Several urged greater cooperation and less competition among scientists.

**PREDICTORS OF ATTITUDES**

In multivariable modeling, the likelihood that a respondent would feel that the negative aspects of data sharing outweighed the benefits was significantly higher among those who felt that other people generally could not be trusted (odds ratio, 2.3; 95% confidence interval [CI], 1.2 to 4.6) and among those who were concerned about the risk of reidentification (odds ratio, 2.4; 95% CI, 1.2 to 4.5) or about information theft (odds ratio, 2.2; 95% CI, 1.2 to 4.1) (Section 4 in the Supplementary Appendix). The only other significant predictor was having a

TRIAL PARTICIPANTS' VIEWS OF DATA SHARING



college degree, which was associated with a lower likelihood of feeling that the negative aspects of data sharing outweighed the benefits (odds ratio, 0.27; 95% CI, 0.2 to 0.5).

A low level of trust in people was also a significant predictor of being somewhat or very unlikely to share one's own data with scientists in not-for-profit contexts (odds ratio, 3.7; 95% CI, 1.6 to 8.3) or drug companies (odds ratio, 2.5; 95% CI, 1.3 to 4.8). Low trust in drug companies was a significant predictor of unwillingness to share data with drug-company scientists (odds ratio, 2.4; 95% CI, 1.4 to 4.2). Having a college degree was associated with a significantly lower likelihood of refusing to share data with not-for-profit scientists (odds ratio, 0.28; 95% CI, 0.10 to 0.78).

DISCUSSION

In this study assessing the views of clinical trial participants on the sharing of participant-level clinical trial data beyond genomic information, several key messages emerged. First, most of the clinical trial participants in our study believed that the benefits of data sharing outweighed the potential negative aspects and were willing to share their data. Their willingness to share was high regardless of the way in which the data would be used, with the exception of litigation, and it extended to uses that involved no prospect of direct benefit to themselves or their family members. Despite low levels of trust in pharmaceutical companies, most trial participants were willing to share their data with them.



**Table 2. Willingness of Clinical Trial Participants to Share Their Data, According to Type of Use and Recipient.\***

Type of Use or Recipient	Very Likely	Somewhat Likely	Neither Likely nor Unlikely	Somewhat Unlikely	Very Unlikely
	<i>percent of respondents</i>				
<b>Type of use</b>					
To help patients and groups of patients learn more about health problems that affect them	77.8	18.8	2.6	0.4	0.4
To do research on health problems that affect my family or me	78.3	17.1	3.2	1.1	0.5
To do research that will help others	79.9	17.1	2.0	0.4	0.7
To help get answers to scientific questions faster using information that others have already gathered	72.2	22.6	3.4	1.2	0.5
To help scientists check the accuracy of research results announced by other scientists or companies (by re-doing the analyses)	70.9	22.6	3.8	1.5	1.2
To learn more about diseases that only a small number of people have (by combining data from many clinical trials)	69.1	22.1	5.9	1.7	1.2
To help lawyers prove their case in lawsuits claiming that medical products are unsafe	27.9	24.5	26.9	12.7	8.0
<b>Recipient</b>					
Scientists in universities and other not-for-profit organizations	69.2	24.0	3.3	1.7	1.8
Scientists in companies developing medical products, such as prescription drugs	53.4	28.5	10.6	5.4	2.1

\* Shown are the responses to items worded as “How likely would you be to allow your *anonymous, individual* clinical trial data to be used in the following ways?” (for type of use) or “How likely would you be to allow your *anonymous, individual* clinical trial data to be shared with . . .” (for recipient). Numbers were rounded to the nearest tenth. The accuracy (95% confidence interval) of percentages close to 50% is ±3.6 percentage points, diminishing to ±2.2 for percentages close to 10%.

The respondents’ lack of differentiation among different data users and uses contrasts with previous study findings related to biobank participation. Those studies consistently showed substantially less willingness to share biospecimens with researchers in for-profit companies than with university researchers.<sup>45-53</sup> One study showed the same effect for sharing information from electronic health records (EHRs) for research purposes.<sup>54</sup>

The willingness of the respondents in our study to share clinical trial data was greater than that found in many previous studies that involved participants’ attitudes toward research use of biospecimens or EHR data.<sup>40,41,54-56</sup> Expanding access to clinical trial data shares some ethical complexities with biobanking, such as how to obtain meaningful informed consent,

but genetic information raises special concerns.<sup>45,57</sup> On the other hand, clinical trial data include information from medical records and questionnaires that reveals much more about participants than biospecimens. Some such information — for example, sexual orientation or substance use — may carry serious social risks.<sup>38</sup> A further consideration is that with rare exceptions,<sup>58</sup> biobanking studies presume that an institutional review board will approve future uses of the data — a safeguard that may not be present for sharing of clinical trial data. Finally, biobanking and EHR studies have generally presumed that the data would be used by qualified researchers, but some proposals for “open access” data sharing are not so limited.<sup>1,4</sup>

The values and concerns of clinical trial participants may differ from those of the general

public, patients in general, or other populations surveyed in biobanking and EHR studies. Clinical trial participants typically constitute a small proportion of the people who are eligible for participation and may represent those who are least bothered by data sharing and most enthusiastic about contributing to science. Their familiarity with physician-researchers may impart especially high trust in research and researchers.<sup>59</sup> Indeed, nearly all of our respondents reported very positive experiences as trial participants.

Our findings are broadly consistent with other literature on engagement in clinical trials in underscoring the idea that altruism as well as self-regarding motivations influence participation decisions.<sup>60,61</sup> In write-in comments, many respondents expressed the view that agreeing to broad use of their data was inherent in agreeing to participate in research.

A second finding of our study is that even when presented with a list of negative potential consequences, most trial participants do not express substantial concern about the risks of data sharing. On average, across the negative consequences they considered, approximately 8% of respondents were very concerned and 17% somewhat concerned. However, a substantial minority of respondents did express some concern, especially about discouraging others from volunteering for trials (37% somewhat or very concerned), having information used for marketing (34%), and having information stolen (31%). Many potential harms that trial sponsors and investigators worry a great deal about, such as reidentification and discrimination, were not of great concern to a sizable majority of participants, a finding that differs from surveys about biobanking that highlight these issues as leading concerns.<sup>62</sup>

Third, multivariable analysis revealed few differences in views across participant subgroups. Despite concern that distrust in research among African Americans may extend to data sharing,<sup>1,46,58,63</sup> we found no significant differences according to race. Because few of our respondents expressed negative views of data sharing, only large subgroup differences were detectable.

Our study had limitations. The respondents

were relatively healthy: approximately a quarter characterized their health status as fair or poor. Although health status was not a significant predictor of attitudes in our models, a less healthy group of respondents might have reported different views. Our response rate was high, but we cannot exclude the possibility of nonresponse bias. Some people may decline to enroll in clinical trials out of concern that their data might be shared, and they are not represented in our sample. The survey concepts were complex, and although we conducted pilot work to clarify questions, some respondents may have had comprehension difficulties or lacked sufficient understanding of data sharing to meaningfully assess the potential consequences. Finally, respondents' actual willingness to share their data might be lower than their hypothetical willingness. Previous research on genomic data, however, has shown the reverse.<sup>59,62</sup>

Our findings suggest that concerns about trial participants' attitudes toward data sharing invoked by companies and investigators who caution against it may be exaggerated. Participants perceive data sharing to have many benefits, and most are willing to share their data. Finally, participants' concern about the use of their data for marketing is worth addressing. Data repositories could require data requesters to attest that no marketing use will occur, and consent documents could offer assurances about this requirement.

Reaching a world in which the sharing of clinical trial data is routine requires surmounting several challenges — financial, technical, and operational. But in this survey, participants' objections to data sharing did not appear to be a sizable barrier.

Supported by a grant from the Greenwall Foundation. Research information technology used in the study was funded by a grant from the National Center for Research Resources, National Institutes of Health (Clinical and Translational Sciences Award UL1 TR001085, to Stanford University).

Disclosure forms provided by the authors are available with the full text of this article at [NEJM.org](http://NEJM.org).

We thank the clinical trial principal investigators and teams for their generosity in facilitating access to the trial participants and administering the survey; Harry Selker, Edward Kuczynski, Anantha Shekhar, Laurie Trevino, and Brenda Hudson for connecting us with the trial teams; Sayeh Fattahi, Cynthia Rinaldo, and Quinn Walker for research assistance; and Jon Krosnick, Eric Campbell, Joe Ross, Jennifer Miller, Randy Stafford, and members of Dr. Stafford's American Indian Community Action Board for feedback on earlier drafts of the survey questionnaire.

## REFERENCES

- Institute of Medicine. Sharing clinical trial data: maximizing benefits, minimizing risk. Washington, DC: National Academies Press, 2015.
- Zarin DA. Participant-level data and the new frontier in trial transparency. *N Engl J Med* 2013;369:468-9.
- Loder E. Sharing data from clinical trials: where we are and what lies ahead. *BMJ* 2013;347:f4794.
- Mello MM, Francer JK, Wilenzick M, Teden P, Bierer BE, Barnes M. Preparing for responsible sharing of clinical trial data. *N Engl J Med* 2013;369:1651-8.
- European Medicines Agency. Clinical data publication ([http://www.ema.europa.eu/ema/curi=pages/special\\_topics/general/general\\_content\\_000555.jsp](http://www.ema.europa.eu/ema/curi=pages/special_topics/general/general_content_000555.jsp)).
- Davis AL, Miller JD. The European Medicines Agency and publication of clinical study reports: a challenge for the US FDA. *JAMA* 2017;317:905-6.
- Food and Drug Administration. Availability of masked and de-identified non-summary safety and efficacy data: request for comments. *Fed Regist* 2013;78(107):33421-3 (<https://www.federalregister.gov/articles/2013/06/04/2013-13083/availability-of-masked-and-de-identified-non-summary-safety-and-efficacy-data-request-for-comments>).
- Coady SA, Wagner E. Sharing individual level data from observational studies and clinical trials: a perspective from NHLBI. *Trials* 2013;14:201.
- Walport M, Brest P. Sharing research data to improve public health. *Lancet* 2011;377:537-9.
- Jumbe NL, Murray JC, Kern S. Data sharing and inductive learning — toward healthy birth, growth, and development. *N Engl J Med* 2016;374:2415-7.
- Krumholz HM, Waldstreicher J. The Yale Open Data Access (YODA) Project — a mechanism for data sharing. *N Engl J Med* 2016;375:403-5.
- Green AK, Reeder-Hayes KE, Corty RW, et al. The Project Data Sphere initiative: accelerating cancer research by sharing data. *Oncologist* 2015;20(5):464-e20.
- Taichman DB, Sahni P, Pinborg A, et al. Data sharing statements for clinical trials — a requirement of the International Committee of Medical Journal Editors. *N Engl J Med* 2017;376:2277-9.
- Warren E. Strengthening research through data sharing. *N Engl J Med* 2016;375:401-3.
- 21st Century Cures Act, Pub. L. No. 114-255 § 2014 (2016).
- Majumder MA, Guerrini CJ, Bollinger JM, Cook-Deegan R, McGuire AL. Sharing data under the 21st Century Cures Act. *Genet Med* 2017;19:1289-94.
- PhRMA, EfPIA. Principles for responsible clinical trial data sharing. 2014 (<http://www.phrma.org/sites/default/files/pdf/PhRMAPrinciplesForResponsibleClinicalTrialDataSharing.pdf>).
- Rockhold F, Nisen P, Freeman A. Data sharing at a crossroads. *N Engl J Med* 2016;375:1115-7.
- Krumholz HM, Gross CP, Blount KL, et al. Sea change in open science and data sharing: leadership by industry. *Circ Cardiovasc Qual Outcomes* 2014;7:499-504.
- Bierer BE, Li R, Barnes M, Sim I. A global, neutral platform for sharing trial data. *N Engl J Med* 2016;374:2411-3.
- Strom BL, Buysse ME, Hughes J, Knoppers BM. Data sharing — is the juice worth the squeeze? *N Engl J Med* 2016;375:1608-9.
- Eichler HG, Pétavy F, Pignatti F, Rasi G. Access to patient-level trial data — a boon to drug developers. *N Engl J Med* 2013;369:1577-9.
- Shining a light on trial data. *Nat Biotechnol* 2012;30:371.
- Krumholz HM, Ross JS. A model for dissemination and independent analysis of industry data. *JAMA* 2011;306:1593-4.
- Whitty CJ, Mundel T, Farrar J, Heymann DL, Davies SC, Walport MJ. Providing incentives to share data early in health emergencies: the role of journal editors. *Lancet* 2015;386:1797-8.
- Eichler HG, Abadie E, Breckenridge A, Leufkens H, Rasi G. Open clinical trial data for all? A view from regulators. *PLoS Med* 2012;9(4):e1001202.
- Göttsche PC. Why we need easy access to all data from all clinical trials and how to accomplish it. *Trials* 2011;12:249.
- Lemmens T. Pharmaceutical knowledge governance: a human rights perspective. *J Law Med Ethics* 2013;41:163-84.
- Bauchner H, Golub RM, Fontanarosa PB. Data sharing: an ethical and scientific imperative. *JAMA* 2016;315:1237-9.
- Bertagnolli MM, Sartor O, Chabner BA, et al. Advantages of a truly open-access data-sharing model. *N Engl J Med* 2017;376:1178-81.
- PhRMA statement on clinical trials and *Bad Pharma*. Press release of PhRMA, February 5, 2013 (<http://www.phrma.org/press-release/phrma-statement-on-clinical-trials-and-bad-pharma>).
- Rathi V, Dzara K, Gross CP, et al. Sharing of clinical trial data among trialists: a cross sectional survey. *BMJ* 2012;345:e7570.
- Statement on European General Court decision on EMA. Press release of PhRMA, April 30, 2013 (<http://www.phrma.org/press-release/phrma-statement-on-decision-of-the-european-general-court-on-ema-disclosure-of-company-data>).
- Berlin JA, Morris S, Rockhold F, Askie L, Ghersi D, Waldstreicher J. Bumps and bridges on the road to responsible sharing of clinical trial data. *Clin Trials* 2014;11:7-12.
- Kaye J. The tension between data sharing and the protection of privacy in genomics research. *Annu Rev Genomics Hum Genet* 2012;13:415-31.
- Castellani J. Are clinical trial data shared sufficiently today? Yes. *BMJ* 2013;347:f1881.
- Homer N, Szelinger S, Redman M, et al. Resolving individuals contributing trace amounts of DNA to highly complex mixtures using high-density SNP genotyping microarrays. *PLoS Genet* 2008;4(8):e1000167.
- Rosenblatt M, Jain SH, Cahill M. Sharing of clinical trial data: benefits, risks, and uniform principles. *Ann Intern Med* 2015;162:306-7.
- Alemayehu D, Anziano RJ, Levenstein M. Perspectives on clinical trial data transparency and disclosure. *Contemp Clin Trials* 2014;39:28-33.
- Garrison NA, Sathe NA, Antommarrina AHM, et al. A systematic literature review of individuals' perspectives on broad consent and data sharing in the United States. *Genet Med* 2016;18:663-71.
- Shabani M, Bezuidenhout L, Borry P. Attitudes of research participants and the general public towards genomic data sharing: a systematic literature review. *Expert Rev Mol Diagn* 2014;14:1053-65.
- Sample I. Big pharma mobilising patients in battle over drugs trials data. *The Guardian*. July 21, 2013 (<https://www.theguardian.com/business/2013/jul/21/big-pharma-secret-drugs-trials>).
- Haug CJ. Whose data are they anyway? Can a patient perspective advance the data-sharing debate? *N Engl J Med* 2017;376:2203-5.
- Harris PA, Taylor R, Thielke R, Payne J, Gonzalez N, Conde JG. Research electronic data capture (REDCap) — a meta-data-driven methodology and workflow process for providing translational research informatics support. *J Biomed Inform* 2009;42:377-81.
- Pentz RD, Billot L, Wendler D. Research on stored biological samples: views of African American and White American cancer patients. *Am J Med Genet A* 2006;140:733-9.
- Kaufman DJ, Murphy-Bollinger J, Scott J, Hudson KL. Public opinion about the importance of privacy in biobank research. *Am J Hum Genet* 2009;85:643-54.
- Helft PR, Champion VL, Eckles R, Johnson CS, Meslin EM. Cancer patients' attitudes toward future research uses of stored human biological materials. *J Empir Res Hum Res Ethics* 2007;2:15-22.

48. Beskow LM, Dean E. Informed consent for biorepositories: assessing prospective participants' understanding and opinions. *Cancer Epidemiol Biomarkers Prev* 2008;17:1440-51.
49. Gornick MC, Ryan KA, Kim SY. Impact of non-welfare interests on willingness to donate to biobanks: an experimental survey. *J Empir Res Hum Res Ethics* 2014;9:22-33.
50. Trinidad SB, Fullerton SM, Bares JM, Jarvik GP, Larson EB, Burke W. Genomic research and wide data sharing: views of prospective participants. *Genet Med* 2010;12:486-95.
51. Rogith D, Yusuf RA, Hovick SR, et al. Attitudes regarding privacy of genomic information in personalized cancer therapy. *J Am Med Inform Assoc* 2014;21(e2):e320-e325.
52. Long MD, Cadigan RJ, Cook SF, et al. Perceptions of patients with inflammatory bowel diseases on biobanking. *Inflamm Bowel Dis* 2015;21:132-8.
53. Hapgood R, McCabe C, Shickle D. Public preferences for participation in a large DNA cohort study: a discrete choice experiment. HEDS discussion paper 04/05. 2004 (<http://eprints.whiterose.ac.uk/10939/>).
54. Grande D, Mitra N, Shah A, Wan F, Asch DA. Public preferences about secondary uses of electronic health information. *JAMA Intern Med* 2013;173:1798-806.
55. Truven Health Analytics, National Public Radio. Health poll: data privacy. November 2014 ([https://truvenhealth.com/Portals/0/NPR-Truven-Health-Poll/NPRPulseDataPrivacy\\_Nov2014.pdf](https://truvenhealth.com/Portals/0/NPR-Truven-Health-Poll/NPRPulseDataPrivacy_Nov2014.pdf)).
56. Luchenski SA, Reed JE, Marston C, Papoutsis C, Majeed A, Bell D. Patient and public views on electronic health records and their uses in the United Kingdom: cross-sectional survey. *J Med Internet Res* 2013;15(8):e160.
57. Melas PA, Sjöholm LK, Forsner T, et al. Examining the public refusal to consent to DNA biobanking: empirical data from a Swedish population-based study. *J Med Ethics* 2010;36:93-8.
58. Storr CL, Or F, Eaton WW, Ialongo N. Genetic research participation in a young adult community sample. *J Community Genet* 2014;5:363-75.
59. Johnsson L, Helgesson G, Rafnar T, et al. Hypothetical and factual willingness to participate in biobank research. *Eur J Hum Genet* 2010;18:1261-4.
60. Stunkel L, Grady C. More than the money: a review of the literature examining healthy volunteer motivations. *Contemp Clin Trials* 2011;32:342-52.
61. Truong TH, Weeks JC, Cook EF, Joffe S. Altruism among participants in cancer clinical trials. *Clin Trials* 2011;8:616-23.
62. Oliver JM, Slashinski MJ, Wang T, Kelly PA, Hilsenbeck SG, McGuire AL. Balancing the risks and benefits of genomic data sharing: genome research participants' perspectives. *Public Health Genomics* 2012;15:106-14.
63. Sanderson SC, Brothers KB, Mercaldo ND, et al. Public attitudes toward consent and data sharing in biobank research: a large multi-site experimental survey in the US. *Am J Hum Genet* 2017;100:414-27.

Copyright © 2018 Massachusetts Medical Society.

**SPECIALTIES AND TOPICS AT NEJM.ORG**

Specialty pages at the *Journal's* website (NEJM.org) feature articles in cardiology, endocrinology, genetics, infectious disease, nephrology, pediatrics, and many other medical specialties.



**shots**

HEALTH NEWS FROM NPR

# When Scientists Develop Products From Personal Medical Data, Who Gets To Profit?

May 31, 2018

Heard on [All Things Considered](#)



**RICHARD HARRIS**  
[Twitter](#)



*Katherine Streater for NPR*

If you go to the hospital for medical treatment and scientists there decide to use your medical information to create a commercial product, are you owed anything as part of the bargain?

That's one of the questions that is emerging as researchers and product developers eagerly delve into digital data such as CT scans and electronic medical records, making artificial-intelligence products that are helping doctors to manage information and even to help them diagnose disease.

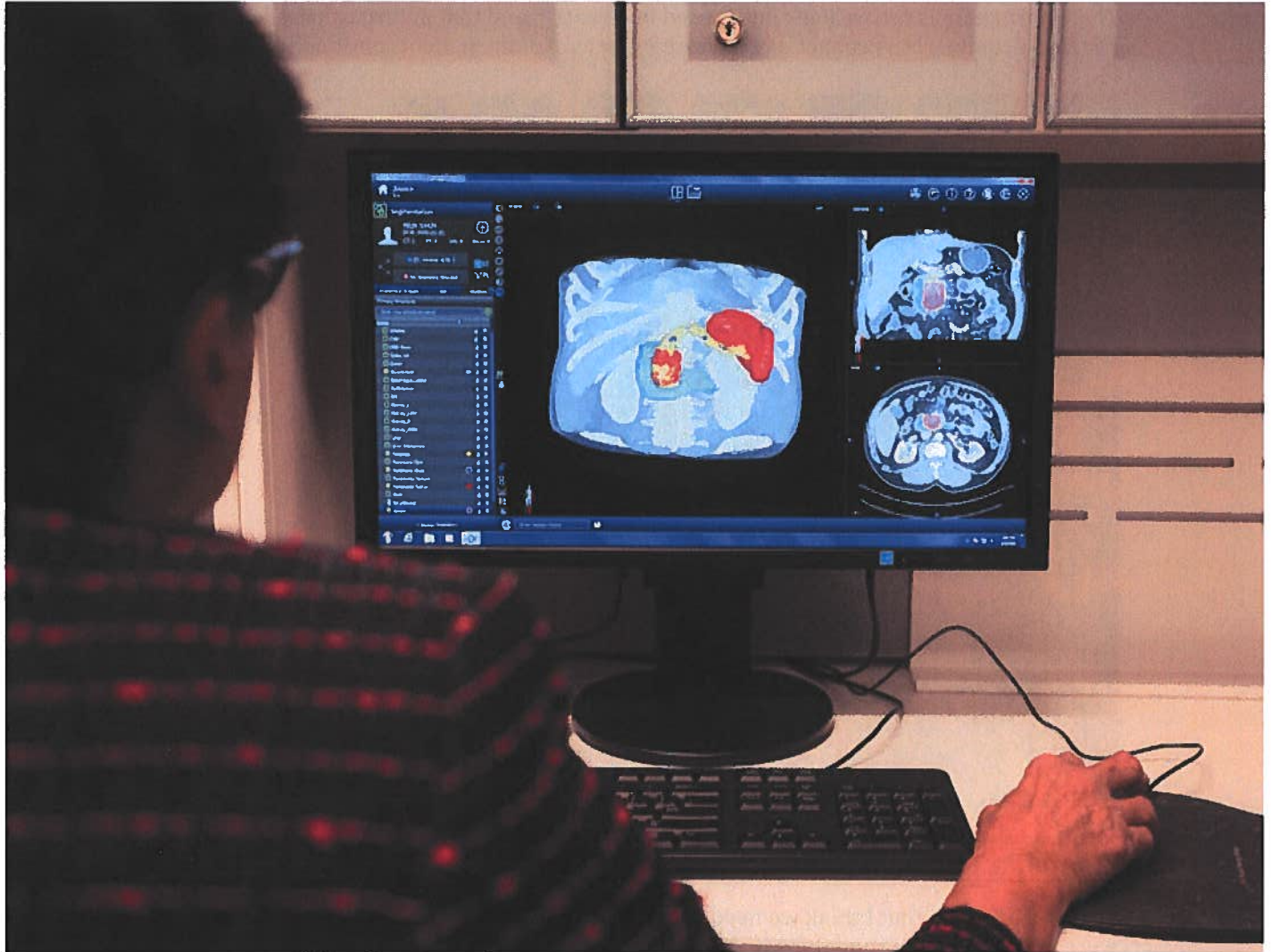
This issue cropped up in 2016, when Google DeepMind decided to test an app that measures kidney health by gathering 1.6 million records from patients at the Royal Free Hospital in London. The British authorities found [this broke patient privacy laws](#) in the United Kingdom. (*Update on June 1 at 9:30 a.m. ET: DeepMind [says](#) it was able to deploy its app despite the violation.*)

But the rules are different in the United States. The most notable cases have involved living tissue, but the legal arguments apply to medical data as well. One of the best examples dates back to 1976, when John Moore went to UCLA to be treated for hairy cell leukemia.

[Prof. Leslie Wolf](#), director of the Center for Health, Law and Society at the Georgia State University College of Law, says Moore's doctors gave him good medical care, "but they also discovered there was something interesting about his cells and created a cell line from his cells without his knowledge," she says.

"And what complicated things even more is they asked Mr. Moore to travel down from his home in Seattle to L.A. multiple times, for seven years, to get additional cells without telling him they had this commercial interest in his cells."

Moore sued. In 1990, The California Supreme Court [decided that he did not own his cells](#), but found his doctors had an obligation to inform him that his tissue was being used for commercial purposes and to give him a chance to object. Moore reached a settlement following his court battle, "but Mr. Moore certainly felt betrayed through the process," Wolf says.



Scientists are training a computer to detect pancreatic tumors from CT scans at Johns Hopkins Medicine in Baltimore, Md. The project uses anonymized patient CT scans to build a system that can recognize tumors.

*Meredith Rizzo/NPR*

The most famous case of this nature involves a Maryland woman, Henrietta Lacks. Back in 1951, doctors at the Johns Hopkins hospital in Baltimore collected cells from her cervical cancer and turned them into the world's first immortal cell line, which grows perpetually in the lab and is used widely in research. As documented in Rebecca Skloot's [book](#) and an HBO biopic starring Oprah Winfrey, the family learned only much later what had transpired and received no compensation. In 2013, the National Institutes of Health [came to an agreement with her family](#) guiding the use of her genetic information, but the family [has continued to raise the issue](#).

While those fights were about living tissue, "in a certain sense whether it's cells or [digital] bits and bytes, it's all information about an individual, at some level," says [Dr. Nabile Safdar](#), a radiologist at Emory University and author [of a recent paper discussing the issue](#) of patients' rights as it pertains to their medical scans.

This information is increasingly being used in research, and that in turn can easily end up being used to develop a commercial product that's worth millions. Are the patients entitled to a cut?



## FINE ART

### [Henrietta Lacks' Lasting Impact Detailed In New Portrait](#)

"That's a question that I think we need to figure out," Safdar says. "And if were a patient and my data were used to develop something that was being shared outside as a product, I'd want to know."

That's not how it's usually done. At many research hospitals, patients routinely sign a paper, in that huge stack of admission paperwork, giving permission for the institution to use their personal data for research.

"For someone to sign away the rights in perpetuity for their data to be used for all possible research applications in the future, that's something I think would deserve a lot of scrutiny, and that's not something I would agree with," Safdar says.

Here's a current example. Researchers at Johns Hopkins Medicine [are mining years of CT scans](#) that were performed initially to care for patients. Those patients signed a form saying it was okay to use that data for research. And the research has been approved by the university's institutional review board, which is charged with weighing the ethics of research projects, says [Dr. Karen Horton](#), director of radiology.

Horton is now using some of this data to teach computers how to recognize pancreatic cancer. She says part of their agreement is that the data are stripped of all information that could identify an individual patient, "so there's no [privacy] risk to a patient to have their images used to train the computer."



And Horton says technically, the data don't belong to the patients. "Right now as the law defines it, your medical images are property of the health system," she says. "You don't own the image."

But Wolf, the law professor and ethicist at Georgia State, says she's not sure that's a strong argument. "Yes, they [the doctors] created the scans," she says, "but certainly the patient has rights related to the scans," such as the right to view them and of course to decide at the outset whether they can be used in research.

It generally takes thousands of scans from many individuals to develop a commercial product, so no single person's data is especially valuable on its own. Overall, Wolf says, patients don't have much of a legal argument here, but there is an ethical issue.

"My own concern is not that it is problematic *per se*," she says. But, "I don't think we've done a really good job of letting people know that this is in fact what we do with their data." She [cites lawsuits](#) where blood samples that had been taken at birth ended up being used for research. "One of the moms in the case said if 'I had been asked I think I would have said yes,' but it was the sense of not even being asked, and having the data used," Wolf says. "People generally will agree, but they want to be asked, at least at some level."

And Safdar says there are times when people might, indeed, want to object to how their data are being used.

"There's a wealth of information in a CT scan or an MRI," Safdar says. Looking at features such as liver fat, artery clogs and brain atrophy, researchers might calculate a probability for how long that person is likely to live.

These algorithms are generally called "black boxes," because there's no way to know how they reach their conclusions. And if the computer algorithm "spits out that you have two months to live, there are implications for employment, for insurability, for all kinds of things that impacts that person's daily life," Safdar says. "That worries me a little bit, especially when it's not clear how that black box is making those decisions."

And what if the algorithm has actually baked in an unconscious prejudice of some sort, he asks, such as about race, age or sex?

"When that same model, when trained [to work] on a specific group of people, is now applied to a totally different group of people, it could make totally erroneous decisions."

These issues are becoming more pressing as these AI-based products start coming to market.

You can contact Richard Harris at [rharris@npr.org](mailto:rharris@npr.org).

