

Nicole Schneidman (SBN 319511)
PROTECT DEMOCRACY PROJECT
P.O. Box 341423
Los Angeles, CA 90034-9998
(202) 579-4582
nicole.schneidman@protectdemocracy.org
Attorney for Protect Democracy Project

Additional counsel listed on signature page

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA**

STATE OF CALIFORNIA, et al.,

Plaintiffs,

v.

U.S. DEPARTMENT OF HEALTH AND
HUMAN SERVICES, et al.,

Defendants.

3:25-cv-05536-VC

**UNOPPOSED MOTION FOR LEAVE
TO FILE AMICUS CURIAE BRIEF BY
ELECTRONIC FRONTIER
FOUNDATION, ELECTRONIC
PRIVACY INFORMATION CENTER,
AND PROTECT DEMOCRACY
PROJECT IN SUPPORT OF
PLAINTIFFS' MOTION FOR A
PRELIMINARY INJUNCTION**

Date: August 7, 2025

Time: 10:00 a.m.

Courtroom: Courtroom 4

Judge: Hon. Vince Chhabria

Trial Date: Not set

Action Filed: July 1, 2025

The Electronic Frontier Foundation, the Electronic Privacy Information Center, and the Protect Democracy Project move for leave to file the attached brief as amicus curiae in the above-captioned matter, in support of Plaintiffs' pending Motion for Preliminary Injunction (Dkt. 42-2, 43).

Proposed amici are non-profit legal advocacy organizations with missions dedicated, in whole or in part, to safeguarding privacy rights against digital intrusion. Their proposed brief explains the legal framework, the background of other data demands and disclosures undertaken by federal agencies in recent months, and the strong public interest in ensuring that federal agencies abide by applicable privacy requirements.

On July 17, 2025, the undersigned contacted counsel for all parties to seek their position on amici's filing. All parties consent to the Court's allowing filing of the brief.

A proposed order is attached.

Dated: July 18, 2025

Respectfully submitted,

PROTECT DEMOCRACY PROJECT

/s Nicole Schneidman
P.O. Box 341423
Los Angeles, CA 90034-9998
(202) 579-4582
nicole.schneidman@protectdemocracy.org
Attorney for Protect Democracy Project

ELECTRONIC FRONTIER FOUNDATION
Adam Schwartz (SBN 309491)
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
adam@eff.org
Attorney for Electronic Frontier Foundation

ELECTRONIC PRIVACY
INFORMATION CENTER
Alan Butler (SBN 281291)
1519 New Hampshire Ave, N.W.
Washington, D.C. 20036
(202) 483-1140
butler@epic.org
*Attorney for Electronic Privacy Information
Center*

Nicole Schneidman (SBN 319511)
PROTECT DEMOCRACY PROJECT
P.O. Box 341423
Los Angeles, CA 90034-9998
(202) 579-4582
nicole.schneidman@protectdemocracy.org
Attorney for Protect Democracy Project

Adam Schwartz (SBN 309491)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
adam@eff.org
Attorney for Electronic Frontier Foundation

Alan Butler (SBN 281291)
ELECTRONIC PRIVACY INFORMATION
CENTER
1519 New Hampshire Ave, N.W.
Washington, D.C. 20036
(202) 483-1140
butler@epic.org
*Attorney for Electronic Privacy Information
Center*

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

STATE OF CALIFORNIA, et al.,

Plaintiffs,

v.

U.S. DEPARTMENT OF HEALTH AND
HUMAN SERVICES, et al.,

Defendants.

3:25-cv-05536-VC

**BRIEF OF AMICI CURIAE
ELECTRONIC FRONTIER
FOUNDATION, ELECTRONIC
PRIVACY INFORMATION CENTER,
AND PROTECT DEMOCRACY
PROJECT IN SUPPORT OF
PLAINTIFFS' MOTION FOR
PRELIMINARY INJUNCTION**

TABLE OF CONTENTS

TABLE OF CONTENTS..... i

TABLE OF AUTHORITIES ii

INTEREST OF THE AMICI CURIAE 1

INTRODUCTION AND SUMMARY OF THE ARGUMENT 2

ARGUMENT..... 2

 I. The wrongful interagency disclosure of sensitive Medicaid data works a severe and concrete harm that courts may redress..... 2

 II. Courts may set aside unlawful transfers of personal information between federal entities, even in the absence of public disclosure..... 7

 III. Defendants have ignored the public’s statutorily protected interests in data sharing transparency..... 9

CONCLUSION..... 13

TABLE OF AUTHORITIES

Cases

| | |
|--|---------|
| <i>AFL-CIO v. Dep’t of Labor</i> , No. 25-cv-339, 2025 WL 1129227 (D.D.C. April 16, 2025) | 4, 5, 6 |
| <i>All. For Ret. Ams. v. Bessent</i> , 770 F.Supp.3d 79 (D.D.C. 2025) | 4 |
| <i>Am. Fed’n of Gov’t Emps., AFL-CIO v. Off. of Personnel Mgmt.</i> , No. 1:25-cv-1237, 2025 WL 996542 (S.D.N.Y. Apr. 3, 2025) | 4 |
| <i>Am. Fed’n of State, Cnty. & Mun. Empls., AFL-CIO v. SSA</i> , No. 25-cv-596, 2025 WL 1206246 (D. Md. Apr. 17, 2025) | 4, 5, 7 |
| <i>Am. Fed’n of State, Cnty. & Mun. Empls., AFL-CIO v. SSA</i> , 771 F.Supp.3d 717 (D. Md. 2025) | 4 |
| <i>Bennett v. Spear</i> , 520 U.S. 154 (1997) | 8 |
| <i>Eichenberger v. ESPN, Inc.</i> , 876 F.3d 979 (9th Cir. 2017) | 7 |
| <i>Garey v. James S. Farrin, P.C.</i> , 35 F.4th 917 (4th Cir. 2022) | 4 |
| <i>In re Ambry Genetics Data Breach Litigation</i> , 567 F.Supp.3d 1130 (C.D. Cal. 2021) | 3 |
| <i>In re Nickelodeon Consumer Privacy Litig.</i> , 827 F.3d 262 (3d Cir. 2016) | 7 |
| <i>Jeffries v. Volume Servs. Am.</i> , 928 F.3d 1059 (D.C. Cir. 2019) | 5, 6 |
| <i>Lujan v. Defenders of Wildlife</i> , 504 U.S. 555 (1992) | 2, 6 |
| <i>Nayab v. Capital One Bank (USA), N.A.</i> , 942 F.3d 480 (9th Cir. 2019) | 4 |
| <i>Perry v. Cable News Network, Inc.</i> , 854 F.3d 1336 (11th Cir. 2017) | 7 |
| <i>Randolph v. ING Life Ins. & Annuity Co.</i> , 973 A.2d 702 (D.C. 2009) | 3 |
| <i>Spokeo v. Robbins</i> , 578 U.S. 330 (2016) | 3, 6 |
| <i>Swenson v. U.S. Postal Serv.</i> , 890 F.2d 1075 (9th Cir. 1989) | 12 |
| <i>TransUnion LLC v. Ramirez</i> , 594 U.S. 413 (2021) | 2, 3, 4 |

Statutes

| | |
|--|---|
| Children’s Online Privacy Protection Act of 1998, 15 U.S.C. § 6501 | 9 |
|--|---|

| | |
|---|------------------|
| E-Government Act of 2002, 44 U.S.C. § 3601 <i>et seq.</i> | 9 |
| Federal Information Security Modernization Act (FISMA), 35 U.S.C. § 350 | 5 |
| Paperwork Reduction Act of 1980, 44 U.S.C. § 3501 <i>et seq.</i> | 9, 10 |
| Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (Dec. 31, 1974) | 8 |
| Privacy Act of 1974, 5 U.S.C. § 552a | 7, 9, 10, 11, 12 |
| Privacy Act of 1974, 5 U.S.C. § 704 | 8 |
| Trade Secrets Act, 18 U.S.C. § 1905 | 9 |
| Other Authorities | |
| Arek Sarkissian, ‘There was a lot of anxiety’: Florida’s immigration crackdown is causing patients to skip care, <i>Politico</i> (Feb. 14, 2024), https://www.politico.com/news/2024/02/14/florida-immigration-crackdown-healthcare-00141022 | 12 |
| CMS, <i>T-MSIS Data Guide (Ver. 3.38.0)</i> , https://www.medicaid.gov/tmsis/dataguide/v3/ (last visited July 17, 2025) | 4 |
| Danielle Keats Citron & Daniel J. Solove, <i>Privacy Harms</i> , 102 B.U.L. Rev. 793 (2021) | 6 |
| Executive Order 14243, 90 Fed. Reg. 13681 (Mar. 20, 2025) | 11 |
| Peter Sangeyup Yun, Lindsey Williams & Janice Blanchard, <i>Legislating Fear: How Immigration Status Mandates Threaten Public Health</i> , <i>Western Journal of Emergency Medicine: Integrating Emergency Care with Population Health</i> (Mar. 24, 2025) | 12 |
| Priscilla Alvarez et al., <i>DOGE is building a master database for immigration enforcement, sources say</i> , CNN (April 25, 2025), https://www.cnn.com/2025/04/25/politics/doge-building-master-database-immigration . | 11 |
| Restatement (Second) of Torts § 652B (A.L.I. 1977) | 3, 5 |
| S. Comm. on Gov’t Operations & H. Comm. on Gov’t Operations, 94th Cong., 2d Sess., <i>Legislative History of the Privacy Act of 1974</i> (Comm. Print. 1976) | 8 |
| Samuel D. Warren & Louis D. Brandeis, <i>The Right to Privacy</i> , 4 Harv. L. Rev. 193 (1890) | 8 |
| Sheera Frenkel & Aaron Krolic, <i>Trump Taps Palantir to Compile Data on Americans</i> , N.Y. Times (May 30, 2025) | 11 |
| U.S. Department of Justice, Overview of the Privacy Act of 1974 (2020 ed.), https://www.justice.gov/Overview_2020/dl?inline | 9 |

INTEREST OF THE AMICI CURIAE

Amici are non-profit legal advocacy organizations with missions dedicated, in whole or in part, to safeguarding privacy rights against digital intrusion. They share an interest in the proper development of the law under the Privacy Act, Paperwork Reduction Act, related federal statutes, and the constitutional privacy interests on which they all rest.

The Electronic Frontier Foundation (EFF) works to ensure that technology supports freedom, justice, and innovation for all the people in the world. EFF is a non-profit with more than 30,000 members. EFF regularly advocates in courts and legislatures for data privacy, among many other digital rights.

The Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, D.C., established in 1994 to protect privacy, freedom of expression, and democratic values in the information age.

Protect Democracy Project's mission is to prevent our democracy from declining into a more authoritarian form of government. As part of that mission, Protect Democracy Project engages in various forms of advocacy and litigation aimed at preventing abuses of executive power, including by unlawful capture of private information and unlawful sharing of that data within and beyond government.

EPIC and Protect Democracy are counsel to plaintiffs, and EPIC is itself a plaintiff, in *Pallek v. Rollins*, No. 1:25-cv-1650 (D.D.C. 2025), a case raising similar Privacy Act and other challenges to an unlawful data sharing project the U.S. Department of Agriculture is executing for state data acquired for the Supplemental Nutrition Assistance Program (SNAP).

INTRODUCTION AND SUMMARY OF THE ARGUMENT

The plaintiff states convincingly explain why their legal arguments are likely to succeed on the merits and why the states face imminent and meaningful harm from Defendants’ unlawful requisitioning of sensitive Medicaid patient data. Amici curiae, nonprofit advocacy organizations with missions and expertise involving statutory privacy protections, write to provide the Court with additional arguments from the perspective of the broader public interest in this case. This brief explains the legal framework, the background of other data demands and disclosures undertaken by federal agencies in recent months, and the strong public interest in ensuring that federal agencies abide by applicable privacy requirements. Amici argue (1) that the exposure of sensitive Medicaid data works a severe and redressable harm to the affected individuals; (2) that federal courts are empowered under the Administrative Procedure Act (APA) to set aside unlawful sharing of information between federal government entities; and (3) that federal law recognizes a public interest in the transparency of government use of sensitive data that has been absent in Defendants’ sharing of Medicaid data. Together these points amplify Plaintiffs’ showing that the public interest favors preliminary relief.

ARGUMENT

I. The wrongful interagency disclosure of sensitive Medicaid data works a severe and concrete harm that courts may redress.

HHS’s unlawful disclosure of sensitive health and health-related records from millions of Medicaid beneficiaries to DHS causes a concrete injury in fact that the Court may redress. *See TransUnion LLC v. Ramirez*, 594 U.S. 413, 425 (2021); *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992). While economic and physical harms constitute cognizable injuries under Article III, harms need not be tangible to qualify as concrete. *TransUnion LLC*, 594 U.S. at 425. Indeed, “various” intangible harms may provide the basis for a suit. *Id.* Such injuries include

“reputational harms, disclosure of private information, and intrusion upon seclusion.” *Id.* (citing *Spokeo v. Robbins*, 578 U.S. 330, 340-341 (2016)). Because HHS’s wrongful disclosure of Medicaid beneficiary data causes harms that bear a close relationship to traditional common law and other concrete harms, this court may exercise Article III jurisdiction over Plaintiffs’ claims. *Id.* at 423-24.

Defendants’ wrongful transfer of Medicaid beneficiaries’ sensitive health information works a harm closely analogous to the harm traditionally recognized by the common law tort of intrusion upon seclusion. Intrusion upon seclusion is an intentional tort of intrusion, “physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns . . . [which] would be highly offensive to a reasonable person.” Restatement (Second) of Torts § 652B (A.L.I. 1977). Intrusion upon seclusion may result from “investigation or examination into [one’s] private concerns, as by opening his private and personal mail, searching his safe or his wallet, examining his private bank account, or compelling him by a forged court order to permit an inspection of his personal documents.” *Id.* at cmt. b. Notably, “the intrusion itself” triggers liability, even if there is no “publication or other use of any kind” of the information discovered. *Id.*

Courts recognize wrongful access to medical, financial, and employment records is a “highly offensive” intrusion into “private affairs.” *Id.* at cmt. a; *see, e.g., In re Ambry Genetics Data Breach Litigation*, 567 F.Supp.3d 1130, 1140 (C.D. Cal. 2021) (“confidential medical information, medical diagnoses, billing information” and personally identifiable information); *Randolph v. ING Life Ins. & Annuity Co.*, 973 A.2d 702, 710 (D.C. 2009) (social security number “and other identifying information”). Violations analogous to intrusion upon seclusion may work “intangible” but “concrete” harm sufficient for standing. *TransUnion*, 594 U.S. at 425;

see also *Garey v. James S. Farrin, P.C.*, 35 F.4th 917, 921-22 (4th Cir. 2022) (access to personal information in violation of statute constituted injury “closely related to the invasion of privacy, which has long provided a basis for recovery at common law”); *Nayab v. Capital One Bank (USA), N.A.*, 942 F.3d 480, 487, 492 (9th Cir. 2019).

Another district court recently held—after an exhaustive examination of case law and history—that a wrongful interagency disclosure of sensitive personal information is “analogous to the tort of intrusion upon seclusion” and “if unauthorized, or without adequate need, is surely sufficiently offensive so as to constitute concrete harm.” *Am. Fed’n of State, Cnty. & Mun. Empls., AFL-CIO v. SSA*, No. 25-cv-596, 2025 WL 1206246, at *42 (D. Md. Apr. 17, 2025) (“*AFSCME*”); see also *AFL-CIO v. Dep’t of Labor*, No. 25-cv-339, 2025 WL 1129227, at *7 (D.D.C. April 16, 2025) (“As three judges facing nearly identical issues have explained, the harm that plaintiffs allege their members are suffering has a close relationship with the harm asserted in a suit for the tort of intrusion upon seclusion.”); accord *Am. Fed’n of State, Cnty. & Mun. Empls., AFL-CIO v. SSA*, 771 F.Supp.3d 717, 766 (D. Md. 2025); *All. For Ret. Ams. v. Bessent*, 770 F.Supp.3d 79, 101–02 (D.D.C. 2025); *Am. Fed’n of Gov’t Empls., AFL-CIO v. Off. of Personnel Mgmt.*, No. 1:25-cv-1237, 2025 WL 996542, at *5 (S.D.N.Y. Apr. 3, 2025).

So too here: HHS invaded the privacy of Medicaid recipients when it wrongfully disclosed sensitive health and health-related information to DHS. The data transferred by HHS includes immigration and demographic information, unique identifiers, addresses, race, health claims and encounters, diagnosis and treatment details, and more.¹ The unlawful disclosure of such information is closely analogous to the type of offensive “investigation or examination

¹ See Comp. at 103-105; CMS, *T-MSIS Data Guide (Ver. 3.38.0)*, <https://www.medicaid.gov/tmsis/dataguide/v3/> (last visited July 17, 2025).

into” a person’s private matters that constitutes intrusion upon seclusion. Restatement § 652B, cmt. b. To divulge protected health information is equivalent to “opening [one’s] private and personal mail, searching his safe or wallet, examining his private bank account,” or fraudulently compelling someone to allow an inspection of their personal documents. *Id.* Moreover, such a disclosure is highly offensive to a reasonable person. As the court in *AFSCME* put it, “in our society PII [personally identifiable information], such as SSNs, medical and mental health information, and certain financial records, are regarded as private, sensitive, and confidential information.” *AFSCME*, 2025 WL 1206246, at *40. Indeed, Congress “created a new sphere” with laws like the Privacy Act where Americans “not only *expect* privacy, but have a right to it.” *AFL-CIO v. DOL*, 2025 WL 1129227, at *8.

The harms suffered by Medicaid beneficiaries subject to HHS’s wrongful data disclosure are also closely analogous to the common law tort of breach of confidence, which establishes Article III standing in this case on independent grounds. *See AFL-CIO v. DOL*, 2025 WL 1129227, at *9. As Judge Bates recently explained in *AFL-CIO*, breach of confidence:

“lies where a person offers private information to a third party in confidence and the third party reveals that information to another.” Nothing beyond the “plaintiff’s trust in the breaching party [being] violated” must occur for the harm to be actionable. The trusted party’s disclosure to a third party is sufficient.

Id. (internal citations omitted) (quoting *Jeffries v. Volume Servs. Am.*, 928 F.3d 1059, 1064–65 (D.C. Cir. 2019)). Here, as in *AFL-CIO*, Medicaid beneficiaries provided or generated much of the personal information at the heart of this case on the assurance and reasonable assumption that it would be protected under the Social Security Act, Privacy Act, HIPAA, Federal Information Security Modernization Act (FISMA), 35 U.S.C. § 3501 *et seq.*, and CMS’s own policies. These safeguards were breached when HHS made “unconsented, unprivileged disclosure[s] to a third party”—namely, DHS. *Jeffries*, 928 F.3d at 1065 (citation omitted). Medicaid beneficiaries’

harms thus bear a sufficiently close relationship to those recognized at common law to support Article III standing. Indeed, “[t]his common-law analogue is more like a common-law twin.” *AFL-CIO v. DOL*, 2025 WL 1129227, at *9.

The injuries inflicted on Medicaid beneficiaries do not end, either, with analogy to traditional common law harms. In exposing sensitive health information, HHS has also curtailed the autonomy of and exceeded the consent provided by beneficiaries. Autonomy is diminished when an agency thwarts individuals’ reasonable expectations concerning the use of their personal information or deprives them of rightful control over their data. Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U.L. Rev. 793, 831 (2021). When applying for or accepting Medicaid benefits, individuals give their consent to specific, limited uses of their personal information—an understanding effectuated by laws like the Privacy Act and HIPAA. Importantly, these uses do not include unrestricted transfers of data for immigration enforcement. HHS did not inform beneficiaries that it would share their health information for such purposes, nor would beneficiaries have reasonably expected HHS to do so.

Though intangible, the privacy harms suffered here by Medicaid beneficiaries are nevertheless concrete injuries in fact sufficient for Article III standing. Congress’s judgment is “instructive and important” for “identifying and elevating” redressable intangible harms. *Spokeo*, 578 U.S. at 341. Because it is “well positioned to identify intangible harms that meet minimum Article III requirements,” Congress has the authority to “elevat[e] to the status of legally cognizable injuries concrete, *de facto* injuries that were previously inadequate in law.” *Id.* at 341 (quoting *Lujan*, 504 U.S. at 578). This is precisely what Congress has done through the privacy and confidentiality provisions of the Privacy Act, Social Security Act, and HIPAA. As the Ninth Circuit has confirmed, the unlawful disclosure of legally protected information is precisely the

kind of intangible injury that Congress may elevate. *See Eichenberger v. ESPN, Inc.*, 876 F.3d 979 (9th Cir. 2017) (citing *Perry v. Cable News Network, Inc.*, 854 F.3d 1336, 1341 (11th Cir. 2017)); *see also In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262, 274 (3d Cir. 2016).

II. Courts may set aside unlawful transfers of personal information between federal entities, even in the absence of public disclosure.

By establishing strict privacy and security protections under laws like the Privacy Act, Social Security Act, and HIPAA, Congress has manifested its judgment that the wrongful disclosure of personal data *between federal agencies*—not merely public disclosure—adversely affects the individuals to whom such data pertains. *See* 5 U.S.C. § 552a(b) (“No agency shall disclose any record . . . to another agency,” subject to limited exceptions, under Privacy Act); *AFSCME*, 2025 WL 1206246, at *41. A violation of the Privacy Act, Social Security Act, or HIPAA, like the tort of intrusion upon seclusion itself, “does not depend upon any publicity given to the person whose interest is invaded or to his affairs.” *AFSCME*, 2025 WL 1141737, at *38 (quoting Restatement § 652B, cmt. a). Rather, it is enough that an agency has disclosed an individual’s personal information in excess of its authority or to a party not legally entitled to access it, even if that recipient is another federal agency or officer. To hold otherwise would upend Congress’s decision to prohibit and make actionable wrongful intra-governmental disclosures of personal information.

The legislative history of the Privacy Act makes particularly clear Congress’s intent to establish *within* government the same types of privacy safeguards that have long existed *outside* of government. As the 93rd Congress understood, “[t]he privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by federal agencies[.]” Privacy Act of 1974, Pub. L. No. 93-579, § 2(a)(1), 88 Stat. 1896 (Dec. 31, 1974). “[T]o provide certain safeguards for an individual against an invasion of personal

privacy,” Congress found it necessary “to regulate the collection, maintenance, use, and dissemination of information by such agencies.” *Id.* §§ 2(a)(1), (5). Congress viewed these internal protections (“No agency shall disclose . . . to another agency”) as an extension of the common law—or in the words of Rep. Robert Drinan, “another important step in protecting the ‘sacred precincts of private and domestic life.’” S. Comm. on Gov’t Operations & H. Comm. on Gov’t Operations, 94th Cong., 2d Sess., *Legislative History of the Privacy Act of 1974*, at 776 (Comm. Print. 1976)² (statement of Rep. Robert Drinan) (quoting Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 195 (1890)); *see also id.* at 776 (statement of Sen. Charles Percy) (“[W]e have computers, the type of devices Brandeis probably never even conceived of. I hope that we are prepared to take that next step by passing legislation to safeguard privacy.”); *id.* at 803 (statement of Sen. Barry Goldwater) (“By privacy, . . . I mean the right ‘to be let alone’—from intrusions by Big Brother in all his guises. We must act now while there is still privacy to cherish.”).

Moreover, the unlawful transfer of personal information to another agency—such as a disclosure of records in violation of the Privacy Act—may be set aside as “final agency action” under the APA. 5 U.S.C. § 704. An agency action is final if it “mark[s] the consummation of the agency’s decisionmaking process” and is an action “by which rights or obligations have been determined, or from which legal consequences will flow.” *Bennett v. Spear*, 520 U.S. 154, 156, 177–78 (1997) (quotation marks and citations omitted). This test describes HHS’s disclosure of Medicaid data precisely: HHS reached the decision to transfer Medicaid data to DHS in bulk; effected the transfer in violation of the statutory rights of affected individuals and the agency’s own data protection obligations; caused DHS to incur new statutory obligations with respect to

² Available at https://www.justice.gov/d9/privacy_source_book.pdf.

the data it received; and radically increased the risk of subsequent legal consequences for affected individuals, including possible deportation at the hands of DHS and its subcomponents. Indeed, an agency's mere *decision* to provide interagency access to personal data (in violation of the Privacy Act) has been held to constitute final agency action. *See AFSCME*, 2025 WL 1206246, at *52 (“In sum, the Agency's decision to allow the DOGE Team access to the PII of millions of Americans, is a sea change that falls within the ambit of a final agency action.”). Accordingly, this Court is fully empowered to set aside HHS's interagency transfer of Medicaid data to DHS.

III. Defendants have ignored the public's statutorily protected interests in data sharing transparency.

The states' first and third causes of action, which form the basis for their motion, implicate the general public's interest in the transparency of government decision- and rule-making around data collection and use. For decades, federal policymaking has walked a careful line in balancing the government's legitimate need to obtain and manage personal information against safeguarding the individual privacy rights of all Americans. The Privacy Act, 5 U.S.C. § 552a, and the APA's provision for notice and comment rulemaking, *id.* § 553(b), which Plaintiffs plead, epitomize this balance-striking alongside other foundational federal privacy laws including the Paperwork Reduction Act of 1980, 44 U.S.C. § 3501 *et seq.*, and the E-Government Act of 2002, 44 U.S.C. § 3601 *et seq.*³ These laws embody a common vision

³ Other examples of laws that illustrate the longstanding commitment to achieving a careful equilibrium between protecting individual privacy with the government's need to collect and share data include the Trade Secrets Act, 18 U.S.C. § 1905; the Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501; Social Security Number Fraud Prevention Act of 2018, P.L. 115-59; and the Health Insurance Portability and Accountability Act's (HIPAA) Congressionally mandated privacy rule, 45 C.F.R. Parts 160, 164.A, and 164.E.

whereby any significant federal sharing of sensitive personal data is subject to substantive limits; transparency requirements to proactively and publicly convey the government’s intention and purpose in such sharing; and an interactive dialogue where the government may adjust its data collection and dissemination of this data in light of legitimate concerns raised through public comment. *See, e.g.*, 5 U.S.C § 552a(e)(11) (Privacy Act); 44 U.S.C. §§ 3506(c)(2), 3507(a)(C), (a)(D)(VI) (Paperwork Reduction Act).

While the plaintiffs clearly articulate the interests of Medicaid participants and health care providers in the integrity of their data protections, amici write to emphasize the centrality of broad public participation to Congress’s aim to “restore trust in government” through the Privacy Act and related laws. *See generally* U.S. Department of Justice, *Overview of the Privacy Act of 1974 (2020 ed.)*, https://www.justice.gov/Overview_2020/dl?inline, at 1 (providing overview of the legislative history of the Privacy Act). *See also* 44 U.S.C. §§ 3501(2), 3501(8) (detailing Paperwork Reduction Act purposes: “ensur[ing] the greatest possible public benefit from” information collected and shared by the federal government while safeguarding the information’s “privacy,” “confidentiality,” and “security”).

Careful compliance with these transparency and public comment requirements set especially high stakes when the federal government is engaged in a far-reaching effort to combine sensitive individual data from a range of federal and state sources, as is the broader landscape today. During the same timeframe as this Medicaid data dispute, the “Department of Government Efficiency” (DOGE) has reportedly driven the technology company Palantir’s selection as chief vendor in a project to construct a database with personal information from the

Internal Revenue Service, Social Security Administration, and HHS.⁴ Nothing analogous has ever existed in the American experience, and the federal government’s intentions in amassing vast quantities of data on individuals from a variety of sources are opaque at best. *See* Executive Order 14243, 90 Fed. Reg. 13681 (Mar. 20, 2025) (ordering federal agencies to collect and aggregate data at unprecedented levels, including gaining “unfettered access to comprehensive data from all State programs that receive Federal funding”). Indeed, Congress has expressly warned the executive branch against “the establishment or maintenance by any agency of a national data bank that combines, merges, or links information on individuals maintained in systems of records by other Federal agencies[.]” 5 U.S.C. § 552a note.

The government has obeyed precisely zero of the required steps under federal law for use or sharing of state Medicaid records for a novel purpose. These steps are fundamental to ensuring the public not only understands how a federal agency is deploying data collected about them, but can weigh in on proposed new uses of this information. For example, HHS has not published a system of record notice (SORN) or other Privacy Act notice in the Federal Register to reflect the use of state data collected under the Medicaid program for immigration enforcement. The lack of this notice in turn has deprived the public of the “at least 30 days” the Privacy Act requires for “interested persons to submit written data, views, or arguments to the agency” upon the establishment or revision of a system of records. 5 U.S.C. § 552a(e)(11). Had it done so, HHS

⁴ Sheera Frenkel & Aaron Krolic, *Trump Taps Palantir to Compile Data on Americans*, N.Y. Times (May 30, 2025), <https://www.nytimes.com/2025/05/30/technology/trump-palantir-data-americans.html>; Priscilla Alvarez et al., *DOGE is building a master database for immigration enforcement, sources say*, CNN (April 25, 2025), <https://www.cnn.com/2025/04/25/politics/doge-building-master-database-immigration>.

would have been required to consider whether its proposed disclosure of Medicaid records for non-Medicaid purposes was “compatible with the purpose for which [the record] was collected.” *Id.* § 552a(a)(7). It is unlikely HHS could have done so, because the Social Security Act and HIPAA contain their own meaningful privacy protections. *See Swenson v. U.S. Postal Serv.*, 890 F.2d 1075, 1078 (9th Cir. 1989) (explaining Privacy Act compatibility standard); *see generally* Compl. (Dkt. #1) at ¶¶ 56-66. In the complete absence of a SORN or other notice in the Federal Register, HHS has successfully evaded having to publicly justify using Medicaid records for immigration enforcement. In weighing the equities here, the Court should be mindful of the public’s strong statutory interest in having HHS explain itself under Privacy Act procedures.

The public interest favors interim relief here for at least two reasons. First, in violating the reasonable expectation of privacy of Medicaid recipients and sharing private data with DHS, eligible beneficiaries may fear detention by DHS if they appear at a medical facility. This could lead many to avoid seeking essential and/or emergency medical care, including publicly funded prenatal, labor and delivery, and other emergency health care. Further public health consequences could follow from any such deterrent effect, including increased public cost to care for children born after insufficient prenatal care, elevated communicable disease risk, and diminished public health capabilities.⁵ Second, organizations like amici and the broader public

⁵ *See* Arek Sarkissian, ‘There was a lot of anxiety’: Florida’s immigration crackdown is causing patients to skip care, Politico (Feb. 14, 2024), <https://www.politico.com/news/2024/02/14/florida-immigration-crackdown-healthcare-00141022> (Explaining that women skipped prenatal visits out fear of immigration enforcement at hospitals); Peter Sangeyup Yun, Lindsey Williams & Janice Blanchard, *Legislating Fear: How Immigration Status Mandates Threaten Public Health*, Western Journal of Emergency Medicine: Integrating Emergency Care with Population Health (Mar. 24, 2025),

have a statutory right to understand and express their point of view on how their personal data is used. The procedural rights to comment on significant data collections and disclosures by federal agencies can only be safeguarded if HHS goes through the necessary steps to provide transparency into its plans and engage in a responsible public process.

CONCLUSION

The public interest in federal privacy protections supports Plaintiffs' motion for a preliminary injunction.

<https://doi.org/10.5811/westjem.42065> (describing generally how immigration status chills people from seeking medical care).

Nicole Schneidman (SBN 319511)
PROTECT DEMOCRACY PROJECT
P.O. Box 341423
Los Angeles, CA 90034-9998
(202) 579-4582
nicole.schneidman@protectdemocracy.org
Attorney for Protect Democracy Project

Adam Schwartz (SBN 309491)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
adam@eff.org
Attorney for Electronic Frontier Foundation

Alan Butler (SBN 281291)
ELECTRONIC PRIVACY
INFORMATION CENTER
1519 New Hampshire Ave, N.W.
Washington, D.C. 20036
(202) 483-1140
butler@epic.org
*Attorney for Electronic Privacy
Information Center*

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

STATE OF CALIFORNIA, et al.,

Plaintiffs,

v.

U.S. DEPARTMENT OF HEALTH AND
HUMAN SERVICES, et al.,

Defendants.

3:25-cv-05536-VC

**[PROPOSED] ORDER GRANTING
UNOPPOSED MOTION FOR LEAVE
TO FILE AMICUS CURIAE BRIEF BY
ELECTRONIC FRONTIER
FOUNDATION, ELECTRONIC
PRIVACY INFORMATION CENTER,
AND PROTECT DEMOCRACY
PROJECT IN SUPPORT OF
PLAINTIFFS' MOTION FOR A
PRELIMINARY INJUNCTION**

The motion of Electronic Frontier Foundation, Electronic Privacy Information Center, and Protect Democracy Project to file an amicus curiae brief in support of Plaintiffs' Motion for a Preliminary Injunction is **GRANTED**.

SO ORDERED.

Hon. Vince Chabbria
U.S. District Court Judge