epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

Comments of

THE ELECTRONIC PRIVACY INFORMATION CENTER

to

THE DEPARTMENT OF HEALTH AND HUMAN SERVICES

[Docket ID: SAMHSA-4162-20]

Confidentiality of Substance Use Disorder Patient Records

April 11, 2016

By notice published on February 9, 2016, the Substance Abuse and Mental Health Services Administration ("SAMHSA") of the Department of Health and Human Services ("HHS") proposes to amend certain provisions of the Confidentiality of Alcohol and Drug Abuse Patient Records regulations, including patient consent requirements and data linkage for research purposes.[1] Pursuant to this notice, the Electronic Privacy Information Center ("EPIC") submits these comments to: (1) urge HHS to strengthen the proposed consent requirements, and (2) oppose the proposed expansion of data linkages.

[1] Notice of Proposed Rulemaking, 81 Fed. Reg. 6987 (Feb. 9, 2016) [hereinafter "SAMHSA NPRM"].

EPIC's Interest

EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and related human rights issues, and to protect privacy, freedom of expression, and democratic values.[2] EPIC's Advisory Board includes leading experts in law, technology, and public policy.[3] Several members of EPIC's Advisory Board are leaders in the medical privacy field.[4] EPIC continually advocates for health information privacy rights and de-identified patient data.

EPIC has previously advocated for strong privacy protections for medical records. EPIC submitted comments regarding proposed changes to the Common Rule in 2011 and again in 2016, urging robust safeguards for the privacy of human research subjects.[5] In *IMS Health v. Sorrell* (2011), EPIC filed an amicus brief on behalf of 27 technical experts and legal scholars, as well as nine consumer and privacy groups, arguing that the privacy interest in safeguarding medical records is substantial and that the "de-identification" techniques adopted by data-mining

[2] EPIC, *About EPIC*, https://epic.org/epic/about.html.
[3] EPIC, *EPIC Advisory Board*, https://epic.org/epic/advisory_board.html.
[4] *See, .e.g*, Anita L. Allen, *Privacy and Medicine*, THE STANFORD ENCYC. OF MED. (Edward N. Zalta ed., 2015); Latanya A. Sweeney, *Only You, Your Doctor, and Many Others May Know*, TECH. SCI. (Sep. 29, 2015), http://techscience.org/a/2015092903/; Deborah C. Peel, Patient Privacy Rights, *The Case for Informed Consent: Why It Is Critical to Honor What Patients Expect – For Health Care, Health IT, and Privacy* (Aug. 2010), https://patientprivacyrights.org/wp-content/uploads/2010/08/The-Case-for-Informed-Consent.pdf; Frank Pasquale, *Redescribing Health Privacy: The Importance of Information Policy*, 14 Hous. J. Health L. & Pol'y 95, 96 (2014).
[5] *See* Latanya Sweeney, et al., *Comments on Common Rule Advanced Notice of Proposed Rulemaking*, Docket No. HHS–OPHS–2011–0005 (Oct. 26, 2011), https://epic.org/apa/comments/EPIC-et-al-Common-Rule-Cmts.pdf; EPIC, *Comments on Common Rule Notice of Proposed Rulemaking*, Docket No. HHS-OPHS-2015-0008 (Jan. 6, 2016) https://epic.org/apa/comments/EPIC-Common-Rule-Comments-2016.pdf. *See generally* EPIC, *Privacy and the Common Rule*, https://epic.org/privacy/privacy_and_the_common_rule.html.

firms do not protect patient privacy.[6] EPIC also submitted comments to HHS on the privacy implications of proposed amendments to the Health Insurance Pportability and Accountability Act ("HIPAA") Privacy Rule related to gun control and mental health records.[7] In *FAA v. Cooper*, a case involving government disclosure of an individual's HIV status, EPIC filed an amicus brief asserting that the government should not be allowed to avoid liability by asserting that it caused only mental and emotional harm when it intentionally and willfully violated the Privacy Act.[8]

EPIC has also submitted comments to the Presidential Commission for the Study of Bioethical Issues concerning issues of privacy with regard to human genome sequence data.[9] EPIC commended the Commission for recognizing the privacy implications associated with human genome sequence data, but also set out specific recommendations to safeguard the genetic information of individuals.

EPIC offers these comments to the Department of Health and Human Services to protect the privacy and autonomy of the countless Americans seeking treatment for substance abuse and mental health issues.

I. Medical Privacy is Critically Important and Widely Recognized

Privacy rights in medical records are critically important. "There can be no question that ...medical records, which may contain intimate facts of a personal nature, are well within the

[6] Amicus Curiae Brief of EPIC, *Sorrell v. IMS Health Inc.*, No. 10-779 (S.Ct. Mar. 1, 2011), https://epic.org/amicus/sorrell/EPIC_amicus_Sorrell_final.pdf
[7] EPIC, *Comments on HIPAA Privacy Rule and the National Instant Criminal Background Check System*, (June 7, 2013), https://epic.org/apa/comments/EPIC-HHS-HIPAA-Privacy-Rule.pdf.
[8] EPIC, *FAA v. Cooper*, https://epic.org/amicus/cooper/.
[9] EPIC, *Comments on Issues of Privacy Access With Regard to Human Genome Sequence Data*, (May 25, 2012), https://epic.org/privacy/genetic/EPIC-Human-Gene-Seq-Data-Comments.pdf.

ambit of materials entitled to privacy protection."[10] In addition to physical health information, medical records "may include information about family relationships, sexual behavior, substance abuse, and even the private thoughts and feelings that come with psychotherapy."[11] These records can have profound impact on a person's life, including his or her credit, admission to educational institutions, and employment.[12] More importantly, disclosure of these private details about one's life may result in a loss of dignity and autonomy.[13]

Privacy rights in medical records are also widely recognized. In a previous Comment submitted to the HHS, EPIC stressed patients' critical interest in preserving the privacy of their medical information.[14] "A majority of adults express discomfort (42 percent) or uncertainty (25 percent) with their health information being shared with other organizations— even if . . . [their] name, address, [date of birth, and social security number] were not included."[15] One out of every seven adults "would hide something from their doctor if they knew their information would be shared," even with guarantees that their names, addresses, dates of birth, and social security numbers stay secret.[16] Another third "would consider hiding information."[17] According to recent poll results, "[a]cross the board, Americans resoundingly say 'no'" to the question "[s]hould anyone other than you control your personal health information in electronic health

[10] *United States v. Westinghouse Elec. Corp.*, 638 F.2d 570, 577 (3d Cir.1980)
[11] EPIC, *Medical Records and Privacy*, https://epic.org/privacy/consumer/med_record.html
[12] *Id.*
[13] *Id.*
[14] EPIC, *Comments on the Common Rule NPRM,* (Jan 6, 2016), https://epic.org/apa/comments/EPIC-Common-Rule-Comments-2016.pdf
[15] California Healthcare Foundation, *Consumers and Health Information Technology: A National Survey*, 26 (2010), *available at:* http://www.chcf.org/publications/2010/04/consumers-and-health-informationtechnology-a-national-survey.
[16] *Id.*
[17] *Id.*

systems."[18] More than nine out of ten Americans want to control who can see and use their electronic health information.[19] A separate study confirms this result, finding that patients frequently prefer to restrict provider access to their electronic health records.[20]

II. Substance Abuse Records are Highly Sensitive and Demand Strict Confidentiality Protections

Health records related to drug and alcohol abuse are particularly sensitive. Confidentiality is necessary to ensure successful treatment, because many individuals with substance abuse problems are reluctant to seek treatment or fully participate in treatment programs if they know that this information will be disclosed to others.[21] In recognition of the stigma related to substance abuse and the fear of criminal prosecution, Congress passed the Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment, and Rehabilitation Act[22] in the early 1970s. This legislation included rules mandating the confidentiality of alcohol abuse patient records.[23] Soon after, Congress passed the Drug Abuse Prevention, Treatment, and Rehabilitation Act,[24] a law with identical confidentiality provisions applicable to drug abuse patient records.[25] These important public health laws are predicated on the understanding that stigma and fear of prosecution discourages individuals battling substance abuse issues from

---

[18] Patient Privacy Rights, Zogby International Poll (Nov. 23, 2010), https://patientprivacyrights.org/2010/11/new-patient-privacy-poll/.
[19] *Id.*
[20] Tierney WM et al., *Provider Responses to Patients controlling Access to their Electronic Health Records: A Prospective Cohort Study in Primary Care,* 30 J. GEN. INTERNAL MED. Supplement 1, 31 (2014), http://www.ncbi.nlm.nih.gov/pmc/articles/PMC4265224/
[21] *Whyte v. Connecticut Mutual Life Ins. Co.*, 818 F.2d 1005, 1010 (1st Cir.1987),
[22] Pub. L. No. 93-282, 88 Stat. 125 (codified at 42 U.S.C. §§ 4541, et seq. (2013)).
[23] 42 U.S.C. § 4582, as amended and transferred to the Public Health Service Act § 523, codified at 42 U.S.C. § 290dd-2 (2013).
[24] Pub. L. No. 94-237, 90 Stat. 241 (codified at 21 U.S.C. §§ 1101, et seq. (2013)).
[25] 21 U.S.C. § 1175, as amended and transferred to the Public Health Service Act § 527, codified at 42 U.S.C. § 290ee-3 (2013).

seeking help. The express purpose of these laws is to encourage patients to seek treatment for substance abuse without fearing that their privacy will be compromised.[26]

The Congressional committee responsible for finalizing these patient confidentiality protections recognized the important public health implications of patient privacy:

> The conferees wish to stress their conviction that the strictest adherence to . . . [confidentiality] is absolutely essential to the success of all drug abuse prevention programs. Every patient and former patient must be assured that his right to privacy will be protected. Without that assurance, fear of public disclosure of drug abuse or of records that will attach for life will discourage thousands from seeking the treatment they must have if this tragic national problem is to be overcome.[27]

These Acts authorized the Secretary of HHS to promulgate rules regulating the disclosure and use of substance abuse patient records. The agency's implementing regulations, commonly referred to as "Part 2," describe the circumstances in which information about a substance abuse patient's treatment may be disclosed and used with and without patient consent. [28] Disclosure of substance abuse patient records is permissible without patient consent only in cases of medical emergency,[29] certain qualified research activities,[30] and to entities performing audit and evaluation activities of the program.[31] These rules were last substantively updated in 1987.[32]

[26] *See* H.R. Rep. No. 92-920, at 33 (1972) (Conf. Rep.), *reprinted in* 1972 U.S.C.C.A.N. 2062, 2072.
[27] *Id.*
[28] 42 C.F.R. §§ 2.1 – 2.67.
[29] 42 CFR § 2.51.
[30] 42 CFR § 2.52.
[31] 42 CFR § 2.53.
[32] 42 C.F.R. § 2.1.

Courts have long recognized that the privacy of substance abuse records is vital for the delivery of medical services, and should not be "lightly abrogated."[33] In *United States v. Cresta*, the United States Court of Appeals for the First Circuit explained:

> Both the statute invoked by [defendant] and the governing regulations carry a strong presumption against disclosing records of this kind. The express purpose of this provision is to encourage patients to seek treatment for substance abuse without fear that by so doing, their privacy will be compromised.[34]

SAMHSA recognized that "[f]or the almost three decades since the Federal confidentiality regulations (42 CFR Part 2 or Part 2) were issued, confidentiality has been a cornerstone practice for substance abuse treatment programs across the country."[35] In addition to the privacy rights of individual patients, public health is also at stake. Confidentiality is critical to continued effectiveness and viability of substance treatment programs.[36] According to a recent SAMHSA survey on drug use and health, one in 10 Americans aged 12 or older had used an illicit drug within 30 days of the survey.[37] With such a large population impacted by drug use, any change to the confidentiality policies of substance abuse treatment records will have profound social and public health impacts.

---

[33] *Mosier v. American Home Patient, Inc.*, 170 F. Supp. 2d 1211, 1213 (N.D. Fla. 2001) (citing *Fannon v. Johnston,* 88 F.Supp.2d 753, 758 (E.D.Mich.2000))
[34] 825 F.2d 538, 551–552 (1st Cir.1987), *cert. denied,* 486 U.S. 1042, (1988) (internal citations omitted).
[35] U.S. Dep't of Health and Human Serv., *The Confidentiality of Alcohol and Drug Abuse Patient Records Regulation and the HIPAA Privacy Rule: Implications for Alcohol and Substance Abuse Programs* (June 2004), http://www.samhsa.gov/sites/default/files/part2-hipaa-comparison2004.pdf.
[36] *U.S. ex rel. Chandler v. Cook County*, Ill., 277 F.3d 969, 981 (7th Cir.), *aff'd,* 538 U.S. 119 (2003).
[37] Substance Abuse and Mental Health Serv. Admin, U.S. Dep't of Health and Human Serv., *Behavioral Health Trends in the United States: Results from the 2014 National Survey on Drug Use and Health* (2014), http://www.samhsa.gov/data/sites/default/files/NSDUH-FRR1-2014/NSDUH-FRR1-2014.pdf.

Confidentiality is especially vital for adolescents because adolescents are more willing to communicate with and seek health care from physicians who assure confidentiality.[38] According to one study, assurances of confidentiality increased the number of adolescents willing to disclose sensitive information about sexuality, substance use, and mental health from 39% to 47% and increased the number willing to seek future health care from 53% to 67%.[39] Maintaining the confidentiality of substance abuse records at its highest level is imperative not only to respect the dignity and privacy of thousands of Americans seeking treatment, but also to promote the public health across the country.

EPIC recommends that SAMHSA provide meaningful privacy protections for substance abuse and mental health records by strengthening the requirements for patient consent to disclosure of these records, and by removing the proposed linkage of these records with other federal and non-federal databases.

III. Patient Privacy and Public Health Interests Require SAMHSA to Strengthen Proposed Consent Requirements

In most circumstances, substance use treatment programs must obtain express consent prior to disclosing patient records.[40] The current Part 2 confidentiality regulations require that

[38] Carol A. Ford et al., *Influence of Physician Confidentiality Assurances on Adolescents' Willingness to Disclose Information and Seek Future Health Care: A Randomized Controlled Trial*, 278 (12) J. OF AM. MED. ASSOC. 1029 (1997). *See also* Lehrer, J.A. et al., *Forgone Health Care Among U.S. Adolescents: Associations Between Risk Characteristics and Confidentiality concern*. 40(3) J. OF ADOLESCENT HEALTH, 218 (2007); Ford, C. et al., *Confidential Health Care for Adolescents: Position Paper of the Society for Adolescent Medicine*. 35(2) J. OF ADOLESCENT HEALTH, 160 (2004).
[39] Carol A. Ford et al., *Influence of Physician Confidentiality Assurances on Adolescents' Willingness to Disclose Information and Seek Future Health Care: A Randomized Controlled Trial*, 278 (12) Journal of Am. Med. Assoc. 1029 (1997).
[40] 42 U.S.C. § 290dd-2.

written consent forms must include the "name or title of the individual or the name of the organization to which disclosure is to be made."[41]

SAMHSA proposes to permit "[i]n the case of an entity that has a treating provider relationship with the patient whose information is being disclosed, . . . the designation of the name of the entity without requiring any further designations . . . ."[42] In addition, SAMHSA proposes to permit a "general designation to those individuals or entities with a treating provider relationship."[43] This would permit programs to request vague patient consent for disclosures to, for example, "my current and future treating providers."[44]

While SAMHSA is correct to include information about the entities to which patient data is made available, the current proposed "general designation" fails to provide sufficient detail and fails to facilitate informed patient decisions. Notably, SAMHA is not requiring that individuals be listed in the "To Whom" form when disclosures are made to an organization or entity.[45] Nor can a patient require that the identity of specific individuals be disclosed on request.[46] Thus, the proposal does not provide patients with information necessary to determine who actually has access to the patients' sensitive and confidential substance abuse treatment records.

It is, however, crucial that patients are aware of the specific recipients of this sensitive health data, not simply an organization or entity. Individual health care employees are frequently

[41] 42 C.F.R. § 2.31(a)(2).
[42] *Id*. at 7000.
[43] *Id*. at 7001.
[44] *Id*.
[45] *Id*. at 7001.
[46] *Id*. at 6998.

the cause of confidential patient data breaches.[47] While the discussion of data breaches largely focuses on remote hackers and cybersecurity failures, individual employees in fact play a substantial role in many of these incidents. Data breaches involving inadequate physical safeguards plague the medical field.[48] Several such examples illustrate this point, from the hospital employee who disclosed details about an 11-year-old child's attempted suicide to others at his school, to the patient care technician who publicly announced an old classmate's HPV diagnosis.[49] Mere months ago, a former employee of an East Texas children's medical clinic improperly accessed up to 16,000 patient health records, and then proceeded to disclose those records to a third party. The breach compromised patient names, birth dates, diagnostic information, and treatment information.[50] In Little Rock, Arkansas, a nephrology lab staff member inadvertently transmitted protected health information to a vendor in an unsecured email, compromising the data of as many as 1,260 patients.[51]

[47] Nicole Hong, *Employee Error Leading Cause of Data Breaches, New Survey Says*, WALL ST. J. (Dec. 9, 2015), http://blogs.wsj.com/law/2015/12/09/employee-error-leading-cause-of-data-breaches-new-survey-says/?mg=id-wsj.
[48] *Small Violations Of Medical Privacy Can Hurt Patients And Erode Trust*, NPR, http://www.npr.org/sections/health-shots/2015/12/10/459091273/small-violations-of-medical-privacy-can-hurt-patients-and-corrode-trust) (last visited Apr 5, 2016).
[49] *Id*.
[50] Sara Heath, *Employee Theft Results in PHI Data Breach for 16K Children*, HEALTHITSECURITY (Nov. 11, 2015), http://healthitsecurity.com/news/employee-theft-results-in-phi-data-breach-for-16k-children.
[51] Max Green, *Employee Email Error Compromises 1,260 Patient Records at Arkansas Nephrology Lab*, BECKER'S HEALTH IT & CIO REVIEW (Oct. 27, 2015), http://www.beckershospitalreview.com/healthcare-information-technology/employee-errors-compromises-1-260-patient-records-at.html.

These cases represent a small fraction of the incidents in which an individual working in a healthcare facility was directly responsible for patient data breaches.[52] The current proposal to reduce patient consent disclosure would ultimately reduce individual accountability to patients. Disclosure to patients of the specific recipients of their substance abuse records is crucial to maintain effective oversight and accountability for employees that cause data breaches. Although HIPAA covered entities are required to annually report "small data breaches" – those affecting fewer than 500 individuals –to the HHS Office of Civil Rights ("OCR") once a year, OCR does not post breaches online.[53] In September of 2015, the HHS Inspector General criticized OCR for mishandling small breaches by failing to investigate the breaches or log them into its tracking system altogether.[54] Given the failure at multiple levels for oversight and accountability in the cases of small data breaches, the listing of individuals who have access to the data is one of the few means available to individuals to address potential compromises of their health records. Such transparency not only allows the individual to make a fully informed decision with regards to disclosure of his or her sensitive medical data, but also holds the individual and overarching entity accountable for the breach.

[52] Akanksha Jayanthi, *11 Latest Healthcare Data Breaches*, BECKER'S HEALTH IT & CIO REVIEW (Nov. 24, 2015), http://www.beckershospitalreview.com/healthcare-information-technology/11-latest-healthcare-data-breaches-11-24-15.html.
[53] *See* 45 C.F.R. § 164.408.
[54] Office of Inspector Gen., Dep't of Health and Human Serv., *OCR Should Strengthen Its Followup of Breaches of Patient Health Information Reported by Covered Entities* (Sep. 2015), http://oig.hhs.gov/oei/reports/oei-09-10-00511.asp.

EPIC recommends that SAMHSA abandon the proposed revisions to patient consent and retain the current requirement to inform patients of the "name or title of the individual or the name of the organization to which disclosure is to be made."[55]

IV. SAMHSA Should Not Permit Linkage of Substance Abuse Records to Other Databases

The SAMSHA NPRM includes proposed revisions on the use of substance abuse data for research purposes. Specifically, SAMHSA proposes "to permit researchers to request to link data sets that include patient identifying information if: (1) The data linkage uses data from a federal data repository; and (2) the project, including a data protection plan, is reviewed and approved by an [Institutional Review Board] registered with [the Department of Health and Human Services, Office for Human Research Protections] in accordance with 45 CFR part 46.[56]

The agency's rational to permit substance abuse records to be linked and combined with data from other federal repositories is that federal agencies "have policies and procedures in place to protect the security and confidentiality of the patient identifying information that must be submitted by a researcher in order to link to data sets."[57] However, the recent surge in government data breaches makes clear that federal agencies are simply unable to adequately safeguard personal information. According to a recent report by the U.S. Government Accountability Office (GAO), "[c]yber-based intrusions and attacks on federal systems have become not only more numerous and diverse but also more damaging and disruptive."[58] This is

[55] 42 C.F.R. § 2.31(a)(2).
[56] SAMHSA NPRM at 7004.
[57] *Id*.
[58] U.S. Gov't Accountability Office, *DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System* (Jan. 2016), http://www.gao.gov/assets/680/674829.pdf.

illustrated by the 2015 data breach at OPM, which compromised the background investigation records of 21.5 million individuals.[59] Also in 2015, the Internal Revenue Service (IRS) reported that approximately 390,000 tax accounts were compromised, exposing Social Security Numbers, dates of birth, street addresses, and other sensitive information.[60] In 2014, a data breach at the U.S. Postal Service exposed personally identifiable information for more than 80,000 employees.[61]

The SAMHSA NPRM also seeks public comment on whether to expand the data linkages provision further and permit researchers to combine substance abuse records with data from state, local, and private data repositories.[62] Like federal databases, healthcare data repositories are also notoriously insecure. According to OCR, health care data breaches in 2015 compromised over 112 million records. Since 2009, more than 1,100 separate health care data breaches have compromised the personal records of over 120 million people in the U.S.[63] In the past two years, 91% of all health care organizations reported experiencing at least one data breach.[64]

SAMHSA's proposal to permit researchers to link data sets that include patient identifiable information with federal data repositories, and potentially even non-federal databases, would place these records at significant risk of compromise. In recognition of the need

[59] *Id.* at 8.
[60] *Id*. at 7-8.
[61] *Id*. at 8.
[62] SAMHSA NPRM at 7005.
[63] Andrea Peterson, *2015 is Already the Year of the Health-Care Hack – and it's Only Going to Get Worse*, WASH POST (Mar. 20, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/03/20/2015-is-already-the-year-of-the-health-care-hack-and-its-only-going-to-get-worse/.
[64] Experian Data Breach Resolution, *2016 Data Breach Industry Forecast*, http://www.experian.com/assets/data-breach/white-papers/2016-experian-data-breach-industry-forecast.pdf.

to maintain strong confidentiality protections for this sensitive information, EPIC recommends that SAMHSA remove the proposal to permit researches to links data sets that include patient identifiable information.

V. Conclusion

For the foregoing reasons, EPIC urges HHS and SAMHSA to strengthen patient consent requirements for the disclosure of substance abuse treatment records, and to withdraw the proposal to link such data to federal, state, local, and private data repositories.

Respectfully Submitted,

Marc Rotenberg
EPIC President and Executive Director

Khaliah Barnes
EPIC Associated Director and
Administrative Law Counsel

Claire Gartland
EPIC Consumer Protection Counsel

Jin Nie
EPIC Law Clerk

Ajay Sundar
EPIC Law Clerk