epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

Department of Health and Human Services

on

Notice of Proposed Rulemaking:
HIPAA Privacy Rule to Support Reproductive Health Care Privacy

88 Fed. Reg. 23,506

June 16, 2023

---

The Electronic Privacy Information Center (EPIC) submits these comments in response to the Department of Health and Human Services (HHS)'s April 17, 2023 request for comment on its notice of proposed rulemaking to modify disclosure standards for protected health information under the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and the Health Information Technology for Economic and Clinical Health Act (HITECH Act).[1] The proposed modifications would limit uses and disclosures of Protected Health Information (PHI) where the information relates to lawfully obtained reproductive health care.[2] EPIC commends HHS for taking meaningful steps to protect the privacy of people's reproductive health information, but we recommend that the agency further strengthen the rule to ensure that these protections are not easily sidestepped, to raise the baseline level of protection for all health data to the constitutional standard, and to specifically overrule state mandatory reporting laws that would otherwise undermine the proposed rule.

[1] HIPAA Privacy Rule to Support Reproductive Health Care Privacy, 88 Fed. Reg. 23,506 (Apr. 17, 2023) [hereinafter NPRM].
[2] *Id*.

EPIC is a public interest research center in Washington, D.C. established in 1994 to focus public attention on emerging civil liberties issues and to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation. EPIC routinely files comments in response to proposed rulemakings concerning the protection of personal information. EPIC has advocated for reproductive privacy and health privacy protections, including through our statement opposing the Supreme Court's rollback of the constitutional right to abortion,[3] our analysis of reproductive privacy after the overturn of *Roe v. Wade*,[4] and our amicus brief to the Colorado Supreme Court explaining how new technologies like reverse keyword warrants can undermine access to abortion and reproductive health care.[5] EPIC has also urged that businesses and other entities be required restrict their collection, use, disclosure, and retention of sensitive personal data, such as protected health information, to that which is strictly necessary.[6]

To protect patient privacy, EPIC makes the following recommendations: (1) the Privacy Rule should remove "lawful" from the proposed language and require a sworn statement rather than a simple attestation; (2) the Privacy Rule should establish a warrant standard for law enforcement access to PHI for a permissible purpose; and (3) the Privacy Rule should Prohibit PHI disclosures in

[3] EPIC, *The Supreme Court Must Not Undermine the Constitutional Right to Privacy* (May 3, 2022), https://epic.org/the-supreme-court-must-not-undermine-the-constitutional-right-to-privacy/.
[4] Sara Geoghegan & Dana Khabbaz, *Reproductive Privacy in the Age of Surveillance Capitalism*, EPIC (July 7, 2022), https://epic.org/reproductive-privacy-in-the-age-of-surveillance-capitalism/.
[5] Brief of EPIC as Amicus Curiae Supporting Petitioner and Reversal at 5, *People v. Seymour*, No. 2023SA12 (Colo. Jan. 11, 2023), https://epic.org/wp-content/uploads/2023/01/Seymour-v.-Colorado-CO-Supreme-Court.pdf ("Reverse keyword warrants . . . threaten that right by exposing significant amounts of sensitive personal data to law enforcement scrutiny without a valid basis.").
[6] *See* Letter from EPIC et al. to Google on Location Data and Abortion Access (June 1, 2022), https://epic.org/wp-content/uploads/2022/06/Letter-to-Google-on-Location-Data-and-Abortion-Access-06-01-2022.pdf; EPIC, *Disrupting Data Abuse: Protecting Consumers from Commercial Surveillance in the Online Ecosystem* (Nov. 2022), https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf; EPIC & Consumer Reports, *How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking* (Jan. 26, 2022), https://epic.org/wp-content/uploads/2022/01/CR_Epic_FTCDataMinimization_012522_VF_.pdf.

mandatory reporting regimes where that information may be used to identify a person who has obtained or assisted someone in obtaining an abortion.

## I. The Updated Privacy Rule Should Not be Limited to Only 'Lawful' Reproductive Health Care Services and Should Require Sworn Statements

The Department should further strengthen the HIPAA Privacy Rule in order to protect patient privacy. The Privacy Rule dictates that a covered entity may only use or disclose PHI as permitted or required by the Rule.[7] The Department's proposed amendments to the Privacy Rule would "prohibit a regulated entity from using or disclosing PHI where the PHI would be used for a criminal, civil, or administrative investigation into or proceeding against any person in connection with seeking, obtaining, providing, or facilitating lawful reproductive health care, or identifying any person for the purpose of initiating such an investigation or proceeding[.]"[8]

While this amendment would impose significant new limits on the disclosure of reproductive health information to law enforcement, we are concerned that there would remain gaps in coverage that could expose individuals to improper law enforcement inquiries. Specifically, the rule would condition its heightened protections for reproductive health data on the "lawful[ness]" of the underlying reproductive care—a distinction that is unnecessarily restrictive, wrongly differentiates federal privacy protections according to state law, and risks deterring patients who are poorly situated to evaluate the legality of particular reproductive health services from seeking essential care.

EPIC therefore urges the Department to eliminate the term "lawful" from Section IV.B.2 of the proposed rule to prohibit a regulated entity from using or disclosing PHI for use in a criminal, civil, or administrative investigation into or proceeding against *any* person in connection with seeking, obtaining, providing, or facilitating reproductive health care. The Department should not

[7] NPRM IV(B)(1).
[8] NPRM IV(B)(2).

limit the prohibition against disclosure of PHI to law enforcement only to PHI pertaining to lawful reproductive health services.

Disclosing PHI to law enforcement in connection with an investigation into reproductive health care is a secondary use of personal information directly at odds with the purpose for which that data was collected: the rendering of health care services.[9] When a patient seeks health care services and accordingly shares their sensitive information with a provider, the patient expects that their information will be used within this context. The patient may expect that some of their information may be used for billing or insurance purposes, or to verify the patient's identity. But the patient would not expect that their sensitive personal information would be used in a law enforcement investigation—particularly not if the patient reasonably believed that the reproductive health services they sought were legal (only to discover later that a state considers them illegal). To ensure that reproductive PHI is safeguarded in a manner consistent with the context and purpose of its collection—and to avoid legal uncertainty that may deter patients from seeking essential health care—the Department should remove the limiting "lawful" terminology from the proposed Privacy Rule.

As an additional step, the amended Privacy Rule should prohibit covered entities from using or disclosing reproductive PHI without receipt of a sworn statement that the use or disclosure is not being sought for a prohibited purpose. Absent such a statement made under penalty of perjury, a law enforcement agency or other entity may more readily conceal improper intent for obtaining PHI and subsequently use it for prohibited purposes. Although we separately advocate in Part II for an across-the-board warrant requirement for law enforcement access to PHI, requiring a sworn statement is an

[9] NPRM IV(B)(2) ("[T]he Department issued its prior iterations of the Privacy Rule at a time when individuals, as a practical matter, generally would not have expected their highly sensitive health care information to be used or disclosed for criminal, civil, or administrative investigations into or proceedings about that health care. The current regulatory and legal environment is in tension with that expectation and threatens to erode the trust that is essential to access to and quality of health care.").

important mechanism for ensuring that the Privacy Rule's safeguards against law enforcement misuse of reproductive PHI are effective.

Finally, in addition to the above measures, we note that the Department can and should use its authority to protect the health privacy of vulnerable populations in other ways. Other types of health information—in particular, PHI relating to gender-affirming care—is similarly sensitive to reproductive health care information (and may in some cases even qualify as reproductive PHI). The Department should explicitly extend the protections in the proposed Privacy Rule to data pertaining to other types of at-risk health care, including gender-affirming care and hormone treatments. Alternatively, the Department should update the Privacy Rule again in the future to protect these types of data.

## II. The Department Should Establish a Warrant Requirement for Law Enforcement Access to PHI

The HIPAA Privacy Rule should establish that police must get a warrant supported by probable cause before obtaining a patient's medical records unless a patient provides informed consent or an exigent circumstance requires warrantless access. Patients' medical information is widely understood to be one of the most private and confidential categories of information. For this reason, many courts rightfully consider patients to have a reasonable expectation of privacy in that information, meaning police must obtain a warrant supported by probable cause to access the information absent consent or exigent circumstances. The current Privacy Rule defies the constitutional standard by allowing law enforcement to obtain medical information without a warrant. Amending the Privacy Rule to bring it in line with the Fourth Amendment standard would help normalize privacy protections nationwide and provide clarity to covered entities' legal departments.

Under the Fourth Amendment, police must generally obtain a warrant when a search or seizure would violate a person's reasonable expectation of privacy. In *Smith v. Maryland*, the Supreme Court explained that when a person subjectively expects something to remain private, and this expectation is something that society is prepared to recognize as reasonable, then police must obtain a warrant before conducting a search.[10] Certain limited and pre-defined exceptions may excuse police from obtaining a warrant, such as when exigent circumstances make the warrant process untenable.[11]

People have an expectation that their sensitive medical records are private documents, and society readily recognizes this expectation as reasonable. Medical records can include some of the most intimate details about a person's life: the way a patient's body and mind works, whether a patient has been subjected to violence or has done harm to him or herself, embarrassing details about a patient's bodily functions, and more. Nearly 75 percent of patients are concerned about protecting the privacy of their health data.[12] For this reason, medical records have long been treated as highly confidential. The Hippocratic Oath has bound health care providers to confidentiality for millennia.[13] Several signers of the Declaration of Independence were physicians who had sworn an oath of confidentiality in treating patients.[14] Every state has some form of statute restricting the use and disclosure of medical information.[15]

Many courts have recognized that people are entitled to privacy protections for their medical records. The Supreme Court, for example, ruled that patients have a reasonable expectation of

[10] *Smith v. Maryland*, 442 U.S. 735, 743 (1979) (citing *Katz v. United States*, 389 U.S. 347, 361 (1967)).
[11] *Kentucky v. King*, 563 U.S. 452, 460 (2011).
[12] American Medical Association, *Patient Perspectives Around Data Privacy* (2022), https://www.ama-assn.org/system/files/ama-patient-data-privacy-survey-results.pdf.
[13] *See Oregon Prescription Drug Monitoring Program v. U.S. Drug Enf't Admin.*, 998 F. Supp. 2d 957, 964 (D. Or. 2014), *rev'd on other grounds*, 860 F.3d 1228 (9th Cir. 2017).
[14] *Id.*
[15] Jacob M. Appel, *Trends in Confidentiality and Disclosure*, 17 Focus 360 (2019), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7011305/?report=reader.

privacy in their medical records and that police must get a warrant before searching them, noting that the "reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent."[16] Many other courts have ruled that medical records require privacy protections, such as federal courts of appeals in the Third Circuit,[17] Fourth Circuit,[18] and Ninth Circuit,[19] and the highest courts in Louisiana,[20] Montana,[21] Massachusetts,[22] Georgia,[23] Pennsylvania,[24] Vermont,[25] and New York.[26] The number and diversity of courts to have recognized a need for medical record privacy protection demonstrates that society's expectation of privacy in these records is reasonable.

Some courts have recognized that patients' privacy interest in their medical records is so strong that full Fourth Amendment protections such as the warrant requirement apply. The Supreme Court ruled that a hospital could not share pregnant patients' drug testing results with law

---

[16] *Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001).
[17] *United States v. Westinghouse Elec. Corp.*, 638 F.2d 570, 577 (3d Cir. 1980) ("There can be no question that an employee's medical records, which may contain intimate facts of a personal nature, are well within the ambit of materials entitled to privacy protection.")
[18] *Doe v. Broderick*, 225 F.3d 440, 450 (4th Cir. 2000) (finding a Fourth Amendment reasonable expectation of privacy).
[19] *Tucson Woman's Clinic v. Eden*, 379 F.3d 531 (9th Cir. 2004), *abrogated on other grounds by Dobbs v. Jackson Women's Health Org.*, 213 L. Ed. 2d 545, 142 S. Ct. 2228 (2022) (warrantless search of abortion clinic violated the Fourth Amendment).
[20] *State v. Skinner*, 2008-2522 (La. 5/5/09), 10 So. 3d 1212, 1218 (finding a Fourth Amendment reasonable expectation of privacy).
[21] *State v. Nelson*, 941 P.2d 441, 449 (Mont. 1997) (finding the state must show probable cause to issue an investigative subpoena for the discovery of medical records).
[22] *Alberts v. Devine*, 479 N.E.2d 113, 118 (Mass. 1985) ("We continue to recognize a patient's valid interest in preserving the confidentiality of medical facts communicated to a physician or discovered by the physician through examination.").
[23] *King v. State*, 535 S.E.2d 492, 495 (Ga. 2000) ("[A] patient's medical information, as reflected in the records maintained by his or her medical providers, is certainly a matter which a reasonable person would consider to be private.").
[24] *Commonwealth v. Riedel*, 651 A.2d 135, 139-40 (Pa. 1994) (noting that a person has "a reasonable expectation of privacy in his medical records" and requiring probable cause for access to medical records, though in this case exigent circumstances applied).
[25] *State v. Welch*, 624 A.2d 1105 (Vt. 1992) (finding a reasonable expectation of privacy in medical records).
[26] *In re Grand Jury Investigation in New York Cnty.*, 98 N.Y.2d 525 (2002) (finding that a hospital could cite New York's patient confidentiality statute to refuse a grand jury subpoena seeking patients' medical records).

enforcement without a warrant supported by probable cause when the aim of the drug testing was aiding criminal law enforcement.[27] The Fourth Circuit ruled that the Fourth Amendment requires police to obtain a warrant before searching through medical records for a criminal investigation.[28] And many state courts of last resort have ruled similarly for the Fourth Amendment or their state constitutional analogs.[29]

Unfortunately, patients' privacy rights have not been consistently protected, and the state of the law is confusing due in part to the current version of the HIPAA Privacy Rule. The Privacy Rule conflicts with the aforementioned judicial rulings by permitting covered entities to share patients' medical records with law enforcement based only on the presence of a subpoena, which is insufficient for Fourth Amendment purposes.[30] Subpoenas do not include the Fourth Amendment protections of judicial oversight, probable cause, and particularity. They have often been subject to abuse—for example, government officials having been exposed as having served subpoenas they claim are from grand juries when those grand juries in fact do not exist.[31]

The Department should amend the HIPAA Privacy Rule to meet the constitutional standard by requiring law enforcement to obtain a warrant for medical records unless a patient provides informed consent or a warrant exception applies. This would help avoid confusion and distress for patients and would provide uniformity and clarity to hospitals' legal departments. It could also ensure that courts adopt the warrant requirement more uniformly in more circumstances, since courts

[27] *Ferguson*, 532 U.S. at 78.
[28] *Broderick*, 225 F.3d at 450–52.
[29] *E.g.*, *Skinner*, 10 So. 3d at 1218 (Louisiana); *Riedel*, 651 A.3d at 190–40 (Pennsylvania); *Welch*, 624 A.2d at 1109 (Vermont).
[30] 45 C.F.R. § 164.512(f)(1)(i)–(ii).
[31] *E.g.*, *People v. O'Dette*, 2017 IL App (2d) 150884 ¶¶ 5–6, 21, https://www.illinoiscourts.gov/Resources/982b9725-1187-4edd-a3d6-1891eced43b6/2150884.pdf; Petition for Writ of Certiorari at 23–24, *Huse v. Texas* (No. 16-535), https://www.scotusblog.com/wp-content/uploads/2016/10/16-535-cert-petition.pdf.

sometimes look to statutes and regulations when determining whether society regards a person's expectation of privacy as reasonable.[32]

EPIC proposes that the Department amend the Privacy Rule consistent with the redlines in Attachment A.

## III. The Privacy Rule Should Prohibit Mandatory Reporting Requirements that Could be Used to Identify a Person Who Has Obtained or Aided Someone to Obtain an Abortion

While the Department's proposal to strengthen the HIPAA Privacy Rule rightly focuses on limiting law enforcement access to reproductive health records, the rule as proposed would not address a major vehicle through which that data is currently exposed: state mandatory reporting laws. For the proposed to rule to be most effective, it must also address mandatory reporting regimes because that data collection becomes a source to propel or initiate criminal intervention. For that reason, HHS should prohibit disclosure of identifying reproductive health information in response to mandatory reporting laws.

Health information can be viewed as a "valuable commodity that society needs in order to identify criminal suspects, investigate epidemics, calculate budgets, monitor the quality of care, develop social policy, and conduct biomedical and behavioral research."[33] However, a person's reproductive health information is also intensely personal. The mandatory collection and potential disclosure of reproductive health information is harmful in myriad ways, spanning from the invasion of privacy to the threat of criminalization, social consequences, and chilling access to health care. Considering the growing risk and volatility surrounding reproductive health information and health care criminalization after *Dobbs*, HHS should reevaluate the balance between the public health

[32] *See, e.g.*, *Doe v. Broderick*, 225 F.3d 440, 450 (4th Cir. 2000) (evaluating a privacy statute as part of the determination of whether society would consider a defendant's expectation of privacy reasonable); *Florida v. Riley*, 488 U.S. 445, 451–52 (1989) (considering Federal Aviation Administration regulations when deciding whether a police practice violated a reasonable expectation of privacy).
[33] Wendy K. Mariner, *Reconsidering Constitutional Protection for Health Information Privacy*, 18 U. Pa. J. Const. L. 975, 981-82 (2016).

surveillance benefits and the harms caused by the collection, threat of disclosure, and actual disclosure of reproductive health information fueled by mandatory reporting laws.

***a. Mandatory Reporting Laws Amass Reproductive Health Care Information***

There are various types of mandatory reporting laws that require the collection of reproductive health information. Mandatory reporting requirements produce troves of information that can be shared with third parties or disclosed in a way that may enable re-identification. Most states in the U.S. have mandatory reporting laws that require providers to submit abortion data. Typically, abortion providers are required to disclose many of the following categories of information: physician and facility where the abortion was performed, demographic information about the patient (e.g., age, race, marital status, ethnicity, other birth history), gestational age, and type of abortion procedure.[34] Most states also require abortion providers to report abortion procedures, abortion complications, abortion records for minors, and abortion information relating medical emergencies and informed consent.[35] Many states submit abortion data to the Center for Disease Control and Prevention (CDC), further expanding the breadth of disclosure.[36] "Although patients' names are removed [in accordance with confidentiality requirements], many potentially identifying characteristics remain. This information, too, is useful for law enforcement and may be subject to FOIA requests."[37] The demographic information required by mandatory reporting forms is sometimes so extensive that people can be re-identified.[38] "Thus, pregnant persons may unwittingly

[34] Guttmacher Institute, *Abortion Reporting Requirements* (Mar. 1, 2023), https://www.guttmacher.org/state-policy/explore/abortion-reporting-requirements.
[35] Temple Law Center for Public Health Law Research, *Abortion Reporting Requirements* (Sept. 30, 2020), https://phlr.org/product/abortion-reporting-requirements.
[36] Guttmacher Institute, *supra* note 34.
[37] Katye Spector-Bagdady & Michelle M. Mello, *Protecting the Privacy of Reproductive Health Information After the Fall of Roe v Wade*, JAMA Health Forum (June 30, 2022), https://jamanetwork.com/journals/jama-health-forum/fullarticle/2794032 [hereinafter *JAMA Health Forum*].
[38] Electronic Frontier Foundation, *Abortion Reporting*, https://www.eff.org/issues/abortion-reporting (last visited June 13, 2023).

create incriminating documentation that has scant legal protection and is useful for enforcing abortion restrictions."[39]

State mandatory reporting laws relating to childhood abuse can also be interpreted to cover abortions or related health care.[40] This is particularly evident where state laws define life as beginning at fertilization or if they have redefined "personhood" to include the unborn.[41] Currently there are laws in "38 states [that] authorize homicide charges to be brought for causing the loss of pregnancy."[42] In this way, criminal action can be taken on behalf of a fetus, and in some states even a zygote or an embryo. Mandatory reporting could also implicate fetal homicide laws that "authorize charges for abortion, assisted reproductive technology, or contraception[.]"[43]

Mandatory reporting for drug use of pregnant people can also lead to criminalization and other harmful outcomes. Hospitals are required to screen for drug use in labor and delivery units to "comply with federal and state regulations for safe care for infants affected by substance abuse during pregnancy."[44] A recent study found that hospitals in Pennsylvania were racially biased because providers were more likely to give drug tests to Black women, exposing them to various harms from criminalization.[45] Another report focused on the harsh effects of mandated reporting for prenatal use of medication to treat opioid use disorder.[46] This includes when clinicians prescribe

[39] JAMA Health Forum, *supra* note 3737.
[40] *Id*.
[41] *See Id*.
[42] Pregnancy Justice, *Who Do Fetal Homicide Laws Protect? An Analysis for A Post-Roe America* (Aug. 17, 2022), https://www.pregnancyjusticeus.org/wp-content/uploads/2022/12/fetal-homicide-brief-with-appendix-UPDATED.pdf.
[43] *Id*.
[44] Roni Caryn Rabin, *Black Pregnant Women Are Tested More Frequently For Drug Use, Study Suggests*, N.Y. Times (Apr. 14, 2023), https://www.nytimes.com/2023/04/14/health/black-mothers-pregnancy-drug-testing.html.
[45] *Id*.
[46] Erin C. Work et al., *Prescribed and Penalized: The Detrimental Impact of Mandated Reporting for Prenatal Utilization of Medication for Opioid Use Disorder*, Maternal Health J. (2023), https://doi.org/10.1007/s10995-023-03672-x.

medications to treat infants exposed to opioids in utero. These mandatory reporting policies "are ostensibly designed to identify infants at risk for abuse and neglect to prevent harm. However, [researchers] identified that reporting itself caused tangible harm due to the trauma cause by an investigation of parental fitness in the immediate postpartum period."[47] Mandatory reporting contributed to avoidance of prenatal and postpartum services and caused anxiety from the loss of privacy.[48]

***b. Mandatory Reporting Regimes Are Harmful to Patients***

Mandatory reporting of reproductive care in various contexts can cause serious physical and emotional harm, chill access to health care, cause reputational harm from disclosure, and lead to a loss of liberty and other consequences through criminalization. Mandatory reporting is often the inception of a criminal investigation related to abortion care. In a recent study evaluating the criminalization of self-managed abortion, most cases came to the attention of law enforcement through mandatory reporting, with 36% of the cases reported by health care providers and 6% reported by social workers.[49] Criminal action was not limited to the person seeking an abortion, as 26% of the adult sample involved the criminalization of people helping others self-manage an abortion.[50] Critically, these investigations and arrests were not limited to states with statutes that criminalize self-managed abortion: "prosecutors applied criminal laws meant to address mishandling of human remains, concealment of a birth, practicing medicine without a license, child abuse and assault, and murder and homicide allegations of self-managed abortion."[51] Once law enforcement accesses information, often through mandatory reporting, they have various means to criminalize

[47] *Id*.
[48] *Id*.
[49] Laura Huss et al., *Self-Care, Criminalized: August 2022 Preliminary Findings*, If/When/How (2022), https://www.ifwhenhow.org/resources/self-care-criminalized-preliminary-findings/.
[50] *Id*.
[51] *Id*.

people seeking abortion care.[52] The study also revealed a stark racial disparity: "a homicide consideration was two times more frequent in cases involving people of color compared to those involving non-Hispanic white individuals."[53]

Criminal intervention related to abortion care, and the fear of criminal investigation, can have harmful impacts beyond an arrest. People can lose custody of their children, face shame within their communities, or face immigration consequences. The looming threat of criminalization can impact the ability of people to seek reproductive health care. Criminalization has a chilling effect on women's health generally, decreasing access and "causing physicians to withhold information from patients for fear that their medical advice could violate their state's anti-abortion statutes."[54]

***c. The HIPAA Privacy Rule Must Address Mandatory Reporting Laws***

It is critical that the Department examine the effects of mandatory reporting laws on reproductive health care in the HIPAA Privacy Rule. HHS should develop language in the HIPAA Privacy Rule to prohibit mandatory disclosure identifying an individual that has obtained or has aided someone in obtaining an abortion. The process for developing this provision should balance the need to prohibit mandatory disclosures that are most likely to lead to criminalization of care with the benefits that certain mandatory reporting mechanisms have for public health purposes. The information gathered by mandatory reporting laws lead to circumstances that most frequently and

---

[52] *See* If/When/How, *Making Abortion A Crime (Again): How Extreme Prosecutors Attempt to Punish People for Abortions in the U.S.*, https://www.ifwhenhow.org/resources/making-abortion-a-crime-again/ (last visited June 13, 2023)("While a few states have explicit bans on self-administered abortion care, there are roughly 40 other types of laws that politically motivated prosecutors may wield against people who end their own pregnancies and those who help them.").

[53] Laura Huss et al., *supra* note 4949.

[54] Human Rights Watch, *Human Rights Crisis: Abortion in the United States After Dobbs* (April 18, 2023), https://www.hrw.org/news/2023/04/18/human-rights-crisis-abortion-united-states-after-dobbs. *See* American Psychological Association, *Frequently Asked Questions About Abortion Laws and Psychology Practice* (Sept. 1, 2022), https://www.apaservices.org/practice/business/hipaa/abortion-laws#report ("Until state laws on abortion reporting are more settled, and the enforcement of these laws has been tested, one strategy to consider is discussing with your patient the potential limits to your confidentiality and potential duty-to-report obligations in your state.").

immediately lead to criminal investigations of people seeking reproductive health care. The threat of criminalization chills access to care for people, further harming health outcomes even without criminal involvement. Addressing mandatory reporting in the HIPAA Privacy Rule is a necessary and impactful way to support reproductive health care privacy.

Respectfully Submitted,

/s/ *Sara Geoghegan*
Sara Geoghegan
EPIC Counsel

/s/ *Suzanne Bernstein*
Suzanne Bernstein
EPIC Law Fellow

/s/ *Tom McBrien*
Tom McBrien
EPIC Law Fellow

**ATTACHMENT A**

(f) ***Standard: Disclosures for law enforcement purposes.*** A covered entity may disclose protected health information for a law enforcement purpose to a law enforcement official if the conditions in paragraphs (f)(1) through (f)(~~6~~ 4) of this section are met, as applicable.

(1) ***Permitted disclosures: Pursuant to process and as otherwise required by law.*** A covered entity may disclose protected health information:

~~(i) As required by law including laws that require the reporting of certain types of wounds or other physical injuries, except for laws subject to paragraph (b)(1)(ii) or (c)(1)(i) of this section; or~~

~~(ii)~~ (i) In compliance with and as limited by the relevant requirements of:

(A) A ~~court order or~~ court-ordered warrant supported by probable cause~~, or a subpoena or summons issued by a judicial officer~~;

~~(B) A grand jury subpoena; or~~

~~(C)~~ (B) An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that:

(*1*) The information sought is relevant and material to a legitimate law enforcement inquiry;

(*2*) The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; ~~and~~

(*3*) De-identified information could not reasonably be used; and

(*4*) The law enforcement officer avers in writing, under penalty of perjury, that the record will not be used in a criminal investigation or prosecution regarding the patient to whom the record relates.

(2) ***Permitted disclosures: Limited information for identification and location purposes.*** Except for disclosures required by law as permitted by paragraph (f)(1) of this section, a covered entity may disclose protected health information in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, provided that:

(i) The covered entity may disclose only the following information:

(A) Name and address;

(B) Date and place of birth;

(C) Social security number;

(D) ABO blood type and rh factor;

(E) Type of injury;

(F) Date and time of treatment;

(G) Date and time of death, if applicable; and

(H) A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

(ii) Except as permitted by paragraph (f)(2)(i) of this section, the covered entity may not disclose for the purposes of identification or location under paragraph (f)(2) of this section any protected health information related to the individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue.

(3) ***Permitted disclosure: Victims of a crime.*** ~~Except for disclosures required by law as permitted by paragraph (f)(1) of this section, a~~ A covered entity may disclose protected health information in response to a law enforcement official's request for such information about an individual who is or is suspected to be a victim of a crime, other than disclosures that are subject to paragraph (b) or (c) of this section, if:

(i) The individual agrees to the disclosure; or

(ii) The covered entity is unable to obtain the individual's agreement because of incapacity or other emergency circumstance, provided that:

(A) The law enforcement official represents in writing that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim;

(B) The law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and

(C) The disclosure is in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.

(4) ***Permitted disclosure: Decedents.*** A covered entity may disclose protected health information about an individual who has died to a law enforcement official for the purpose of alerting law enforcement of the death of the individual if the covered entity has a suspicion that such death may have resulted from criminal conduct.

(5) ***Permitted disclosure: Crime on premises.*** A covered entity may disclose to a law enforcement official protected health information that the covered entity believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the covered entity.

(6) ***Permitted disclosure: Reporting crime in emergencies.***

(i) A covered health care provider providing emergency health care in response to a medical emergency, other than such emergency on the premises of the covered health care provider, may disclose protected health information to a law enforcement official if such disclosure appears necessary to alert law enforcement to:

(A) The commission and nature of a crime;

(B) The location of such crime or of the victim(s) of such crime; and

(C) The identity, description, and location of the perpetrator of such crime.

(ii) If a covered health care provider believes that the medical emergency described in paragraph (f)(6)(i) of this section is the result of abuse, neglect, or domestic violence of the individual in need of emergency health care, paragraph (f)(6)(i) of this section does not apply and any disclosure to a law enforcement official for law enforcement purposes is subject to paragraph (c) of this section.