How New Procedural Controls Using the Privacy Act of 1974 Can Improve the Protections of Reproductive Health Information Held by Federal Agencies

September 2022

By Robert Gellman and Pam Dixon

Executive Summary

This report suggests specific procedural and substantive ways that the Executive Branch can revise implementation of the Privacy Act of 1974 to restrict and more carefully administer some disclosures of reproductive health information by federal agencies to federal, state, and local law enforcement agencies. The focus is on disclosures that could place an individual at jeopardy for undertaking activities that support the ability of any woman to obtain reproductive health care for which the woman sought treatment.

New procedures can be established under the Privacy Act to better control the disclosure of reproductive health information so that individual employee at an agency could not disclose the information without appropriate supervision. At the same time, standard disclosures for health care or oversight can continue without significant disruption and without new threats to data subjects.

The report suggests three different ways that the Executive Branch could use existing Privacy Act of 1974 methods to create new disclosure controls without the need for statutory change.

The first is an Executive Order directing federal agencies to change their Privacy Act of 1974 implementation to control disclosure of reproductive health information.

The second is a directive from the Office of Management and Budget under its existing Privacy Act of 1974 authority to assist federal agencies in implementing the Act.

The third is action that each agency could undertake under existing authority without direction from the President or OMB.

With each option, agencies could implement the Act's routine use provision to include new substantive and procedural restrictions on disclosures of reproductive health information to law enforcement agencies.

The possibility of health-related disclosures in the post-*Dobbs* environment are of greater general concern today. Addressing the full spectrum of new risks to health privacy requires a wide array of tools and controls. The controls described in this report address one privacy-protective response that does not require new legislation.

I. Introduction

The privacy protections currently in place for identifiable health information – and in particular for reproductive health information or RHI – contain numerous gaps in coverage. For example, many cell phone and other health apps are beyond the scope of any existing privacy legislation. The shortcomings of U.S. privacy law are well-researched, documented, and understood at this point. The Supreme Court's decision overturning *Roe v. Wade* effectively raised the stakes for disclosures of RHI in ways that are consequential enough to chill the willingness of women to seek and receive reproductive health care – including care not specifically related to abortion – for fear that health information may be used in a law enforcement investigation or prosecution. Changes to federal health privacy rules[1] may occur, but they will take time and will not cover all records held by federal agencies that are subject to the Privacy Act of 1974.

There are more immediate steps that the federal government can take to limit risks from disclosure of RHI in federal agency records. This is not a small trove of information. Federal agencies maintain millions of health and health insurance records at agencies like the Department of Defense, Veterans Administration, Public Health Service, Centers for Medicare and Medicaid Services, and the Indian Health Service. In addition, like other employers, federal agencies maintain health and health insurance records about its employees. Addressing the privacy of these records is only one aspect of the problems presented by the overturning of *Roe v. Wade*. Importantly, changes to implementation of the Privacy Act of 1974 are something that can be accomplished administratively and without the need for new legislation or extensive rulemaking.

Recent media stories document that health information – especially reproductive health information or RHI – is susceptible to collection, retention, and possible sharing with law enforcement agencies. This includes RHI from routine health records and mobile phone data[2] as well as from third-party menstrual apps, location trackers, license plate readers, retail purchases, social media, search engines, and more.[3] Privacy experts warned for years that the widespread processing of personal information made everyone vulnerable in many ways. These warnings were often seen as largely theoretical. However, the overturning of *Roe v. Wade* has made the stakes of privacy harms more visible to everyone, and more consequential for potentially tens of millions of women, as well as their friends, family members, care providers, and others.

The possibility that federal privacy legislation could provide meaningful protection for RHI does not appear to be a realistic hope, at least not in the near term. The current legislative landscape suggests that no legislation addressing access to reproductive health and related privacy issues is likely pass Congress in the current environment or even in the foreseeable future.

Despite widespread and current debates about the possibilities of federal privacy legislation, the Privacy Act of 1974 is almost never mentioned. The Act has rarely been amended over the years, and it is in need of significant updating, but the law still remains relevant and useful.

Under the Privacy Act of 1974, there are steps that the Executive Branch can take that would provide some new protections against permissive disclosure of RHI to law enforcement agencies. The Act, one of our oldest

---

1 The federal health privacy rules, called after the Health Insurance Portability and Accountability Act or HIPAA, are available at https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/combined-regulation-text/index.html. See also World Privacy Forum, *A Patient's Guide to HIPAA* (2019), https://www.worldprivacyforum.org/2019/03/hipaa/.

2 See, for example, Jack Gillam, *Post-Dobbs America is a digital nightmare* (Bloomberg) (August 4, 2022), https://www.bloomberg.com/news/articles/2022-08-04/period-tracking-apps-among-common-post-dobbs-privacy-risks. See also Tatum Hunter and Geoffrey A. Fowler, *For people seeking abortions, digital privacy is suddenly critical* (Washington Post) (June 24, 2022), https://www.washingtonpost.com/technology/2022/05/04/abortion-digital-privacy/.

3 See FTC v. Kochava, where the Commission filed a lawsuit against data broker Kochava for selling geolocation data from hundreds of millions of mobile devices that can be used to trace the movements of individuals to and from sensitive locations. The data can reveal people's visits to reproductive health clinics, places of worship, homeless and domestic violence shelters, and addiction recovery facilities. https://www.ftc.gov/legal-library/browse/cases-proceedings/ftc-v-kochava-inc.

privacy laws,[4] is a law that applies mostly to federal agencies.[5] Many federal agencies maintain identifiable health information, including RHI. The Privacy Act of 1974 offers a heretofore unnoticed opportunity to offer additional protections.

The World Privacy Forum was the administrative sponsor of an effort by Robert Gellman to develop a comprehensive replacement for the Privacy Act of 1974. The May 2021 proposal sought to build on the successful parts of the Act and to make other parts more reflective of modern record keeping and privacy practices. See *From the Filing Cabinet to the Cloud: Updating the Privacy Act of 1974*.[6] The revision did not address specific RHI issues.

This current report begins with a general description of how the Privacy Act of 1974 works. This basic understanding of the Act will make clear to all readers how the administrative changes discussed in this report will better protect RHI.

II. Background on How the Privacy Act of 1974 Controls Disclosures

The Privacy Act of 1974 regulates identifiable and retrievable records about individuals held by federal agencies. The focus of that regulation is a *system of records*.[7]

The Act defines a *system of records* as a group of records about individuals under the control of an agency from which the agency retrieves records by name, identifying number, or other identifying particular assigned to an individual. Many issues and questions arise from this old-fashioned "retrievability" definition, a definition that predates modern information technology by multiple generations.[8]

Each agency must publish a description of each system of records in the Federal Register to ensure transparency of such systems.[9] One bedrock principle is that there are no secret systems of records. A *System of Records Notice* or SORN is the important acronym in the Privacy Act of 1974 that stands for these notices. The Office of the Federal Register maintains a website with all published SORNs.[10] Each notice includes all *routine uses* for a system, or SORN. No agency is exempt from the publication obligation. In current parlance, the term *SORN* means both a system of records and the notice for that system of records. Small agencies may have a handful of SORNs. Large agencies have hundreds of SORNs.

Not all personal information held by agencies is maintained in a SORN.[11] However, as a practical matter, the vast majority of personally identifiable health information held by federal agencies is indeed covered by a SORN.

The Privacy Act of 1974 allows for two different categories of disclosures for personal information subject to

---

4 For a comprehensive background on the history of the Privacy Act, see World Privacy Forum, *From the Filing Cabinet to the Cloud: Updating the Privacy Act of 1974* (2021), https://www.worldprivacyforum.org/2021/05/from-the-filing-cabinet-to-the-cloud-updating-the-privacy-act-of-1974/.

5 https://www.law.cornell.edu/uscode/text/5/552a.

6 https://www.worldprivacyforum.org/2021/05/from-the-filing-cabinet-to-the-cloud-updating-the-privacy-act-of-1974/.

7 5 U.S.C. § 552a(a)(5).

8 See World Privacy Forum, *From the Filing Cabinet to the Cloud: Updating the Privacy Act of 1974* (2021), https://www.worldprivacyforum.org/2021/05/from-the-filing-cabinet-to-the-cloud-updating-the-privacy-act-of-1974/.

9 5 U.S.C. § 552a(e)(4).

10 https://www.govinfo.gov/app/collection/PAI/.

11 In order for a group of records to be subject to the major parts of the Privacy Act of 1974, information must be retrieved from that group by individual name or other identifying particular assigned to the individual. 5 U.S.C. § 552a(a)(5). Retrievability calls for a factual determination reflecting how an agency actually uses the records.

the Act. The first category covers disclosures expressly allowed in the Act itself that the Congress deemed to be appropriate for all agency SORNs.[12] Examples include disclosures within an agency, required under the Freedom of Information Act, to the National Archives, in compelling circumstances affecting health or safety of an individual, to the Congress, to the Government Accountability Office, or pursuant to a court order.

The second category covers disclosures that an agency can define for each SORN through a process similar to, but not as rigorous, as a rulemaking. The Act calls these disclosures routine uses. A routine use is the use of a record "for a purpose which is compatible with the purpose for which it was collected."[13]

Confusingly, a routine use is a disclosure. As privacy terminology evolved in the decades since the Privacy Act of 1974, a "use" came to mean the *use of a record within the agency or organization that collected or maintains the record*. A disclosure is the *sharing of a record with someone outside the agency that collected or maintains the record*. The Act's terminology grew out-of-date, but remained unchanged. In summary, a routine use is a disclosure outside the agency.

For each SORN, an agency may define what disclosures are appropriate to allow the agency to carry out the purpose of the SORN. Thus, for an agency payroll system, a typical routine use allows disclosure of payroll information to the Department of the Treasury to issue payments to employees. Another typical routine use allows disclosures to agency contractors and consultants. A more recently adopted class of routine uses covers disclosures in the event of a data breach.[14]

Some SORNs have many routine uses. Some have only a few. A system covering agency parking permits is an example of a system of records that typically requires only a few routine uses. On the other hand, a health record system will have dozens of routine uses. Much depends on the scope of the agency activity that the SORN supports. In addition to routine uses for each SORN, some agencies apply "general" routine uses to all agency SORNs.

It is important to keep in mind that disclosures allowed by the Privacy Act of 1974 are discretionary and not mandatory. Both the statutorily allowed disclosures and the routine use disclosures give each agency authority to disclose records, but the Act itself does not require the agency to actually disclose records pursuant to either authority. Another law or court order might mandate that an agency disclose a record, but the Privacy Act of 1974 itself does not mandate any disclosure (other than to the data subject of a record,[15] and there are some exceptions to data subject disclosures).

This description of the Privacy Act of 1974 is at a high-level of generality. There are many details, specific issues, and controversies about how the Act works and what the terminology means that are not addressed here. Nevertheless, the description offered is sufficient so that the goals of this proposal are understandable.

III. Law Enforcement Disclosures Under the Privacy Act of 1974

Generally speaking, the Privacy Act of 1974 allows for two types of law enforcement disclosures. A statutory provision allows disclosures from all SORNs for law enforcement.

---

12 5 U.S.C. § 552a(b).

13 5 U.S.C. § 552a(a)(7).

14 See Office of Management and Budget, *Preparing for and Responding to a Breach of Personally Identifiable Information (Jan. 2017) (OMB Memorandum M-17-12),* https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2017/m-17-12_0.pdf.

15 5 U.S.C. § 552a(f)(1) - (f)(3).

> (b) Conditions of Disclosure. – No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be –
> ***
> (7) to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought.[16]

This authority is less likely to be used because it requires a formal request from the head of a law enforcement agency. It does not reflect how disclosures to law enforcement work in the real world. For example, if one agency uncovers personal information in a SORN that indicates the possibility of a crime, the statutory provision will not support a disclosure because the head of the agency that would investigate the crime does not know to ask for the record. Another example is the absence of a provision allowing for disclosure to foreign law enforcement authorities.

Agencies commonly use routine uses to give themselves authority to make law enforcement disclosures in a manner that reflects real world conditions. This is often accomplished through a routine use applicable to all agency SORNs. Here's an example of a common routine use for law enforcement from the Department of Health and Human Services:

> In the event that a system of records maintained by this agency or carry out its functions indicates a violation or potential violation of law, whether civil, criminal or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the appropriate agency, whether federal, or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation or order issued pursuant thereto.[17]

HHS has a second, nearly identical, agency-wide routine use covering disclosure to state and local law enforcement agencies:

> In the event that a system of records maintained by this agency to carry out its function indicates a violation or potential violation of law, whether civil, criminal or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the appropriate agency, whether state or local charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation or order issued pursuant thereto.[18]

Significant features of these two routine uses are:

(a) The breadth of allowable disclosures. Disclosures are allowed for civil, criminal or regulatory violations or potential violations of law.

---

16 5 U.S.C. § 552a(b)(7).

17 45 C.F.R. Part 5b, Appendix B at (1), (Routine Uses Applicable to More Than One System of Records Maintained by HHS), https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-A/part-5b.

18 Id. at (5).

(b) The absence of any internal procedural prerequisites. While there may be other applicable agency rules or practices, the routine use in theory allows any agency employee to disclose any record from any agency SORN to any of the nation's law enforcement agencies and to any foreign law enforcement agencies because the employee thinks there may be a potential violation of law.

(c) The absence of any standard (e.g., a documented reason to believe) that must be met before a record may be disclosed other than a suspicion about a violation or potential violation of law.

(d) The absence of any requirement for a written or oral request for the record from a law enforcement agency for a record.

(e) The absence of a limit on the content of a disclosure. Nothing in the routine uses tells an agency employee how much of a particular record may be disclosed.

For a variety of practical reasons, it may be both necessary and appropriate for a federal agency to retain broad authority to make law enforcement disclosures. If exercised with discretion, restraint, and appropriate internal procedures, the result in any given circumstance may be reasonably consistent with public policy objectives and with the potentially conflicting goals of protecting individual privacy and enforcing the law.

There is no available evidence documenting abuse of the authority in routine uses for law enforcement. Nor is there any known review of the use of the authority to disclose to law enforcement. Just what constitutes appropriate discretion, restraint, and procedure, however, may be debatable and may change over time and over different Administrations. The flexibility of routine uses might be viewed as both a shortcoming and a strength at the same time.

IV. Examples of Limits on Law Enforcement Disclosures of RHI from Other Laws

A. HIPAA

To the extent that the federal health privacy rules under HIPAA provide stronger protections against law enforcement (or other) disclosures, the HIPAA rules override any less stringent language found in the Privacy Act of 1974 or in routine uses issued by agencies under the Privacy Act of 1974. This helps somewhat to protect RHI as well as other health information from being turned over to law enforcement. However, the protections in HIPAA are far from ideal.

First, the HIPAA protections against disclosure to law enforcement are limited and may not address concerns arising today for RHI. This issue is explored in more detail in an FAQ on HIPAA and Reproductive Health maintained on the World Privacy Forum website.[19]

Second, not all federal agency information that may reveal that RHI is subject to HIPAA. As a general rule, HIPAA only applies to health information held by health care providers or health insurers (and their business associates). For example, an agency personnel system may include information on the reasons for an employee's absence from work that includes RHI. That information is not likely to be covered by HIPAA. In another example, HHS chose not to apply HIPAA privacy rules to information maintained by the National Institutes of Health for research and treatment activities.[20] In addition, there will be other circumstances in which

---

19 World Privacy Forum, *HIPAA and Reproductive Health: A companion FAQ to the Patient's Guide to HIPAA, World Privacy Forum (2022),* https://www.worldprivacyforum.org/2022/07/hipaa-and-reproductive-health-a-companion-faq-to-the-patients-guide-to-hipaa/.

20 See National Institutes of Health, *PRIVACY, Frequently Asked Questions at 21 (Who can I contact if a person or organization covered by the Privacy Rule violates my health information privacy rights?),* https://oma.od.nih.gov/DMS/Documents/Privacy/

information pertaining to RHI comes into the possession of a federal agency that is not subject to HIPAA limits. For example, a law enforcement agency investigating health care fraud may obtain patient records with RHI.

B. Substance Abuse Regulations

The Secretary of Health and Human Services has authority to issue rules to protect patient records created by federally assisted programs for the treatment of substance use disorders.[21] The Substance Abuse and Mental Health Services Administration (SAMHSA) maintains the rules, often referred to simply as Part 2.[22] These rules prohibit law enforcement's use of substance abuse patient records in criminal prosecutions against patients, absent a court order. Part 2 restricts the disclosure of substance abuse treatment records without patient consent, subject to several exceptions. The rules are complex and have one feature absent from most U.S. privacy laws. That is, the confidentiality rules can follow the records so that the confidentiality limits apply to those who receive substance abuse records from a program covered by Part 2. By contrast, HIPAA rules only apply to health care providers and insurers. In contrast, when health information regulated by HIPAA is disclosed to third parties who are not providers or insurers, the HIPAA privacy rules do not apply to the information in the hands of those third parties. The HIPAA protections apply for the most part only when to records held by health care providers or other entities regulated directly by HIPAA.

What is particularly noteworthy about the Part 2 rules is they implement express statutory provisions that provide strong privacy protections for patients whose activities are known to involve overt violations of state or federal law (e.g., use of illegal drugs). The Part 2 rules allow patients to seek medical treatment from drug abuse treatment providers without fear that their treatment records will be available for law enforcement to use in investigations or prosecutions.

V. Proposal to Limit Disclosure of RHI to Law Enforcement

The first issue is how to define RHI. It is not an easy term to define, especially with the possibilities for Internet activities, mobile phone usage, travel, and the purchase of routine goods and services to generate RHI. We offer this definition as a starting point:

> Reproductive health information includes all information relating to the reproductive system and its processes, including (a) information from health records originated by health care providers; and (b) information from other sources that pertains to seeking or providing information or services about (1) reproductive health or sexual activities and choices; (2) over-the-counter products pertaining to reproductive health or sexual activities; (3) transportation or location at or near facilities that provide reproductive health advice or services; and (4) payment for products and services used in connection with reproductive health or sexual activities.

A second issue is the difficulty of distinguishing appropriate from inappropriate disclosures. While many agencies and many SORNs will not maintain any RHI or other health information, some agencies and some SORNs will have RHI and other health information in abundance. These agencies include the Centers for Medicare and Medicaid Services, Veterans Administration, the Indian Health Service, and Department of Defense. Federal employee records may also have RHI as part of health and health insurance records routinely maintained. In total, these records hold health information on millions of individuals, and the health records they maintain include RHI just as the records of any other health provider, insurer, or employer.

Privacy%20FAQs%202021%20June%20Final.pdf.

21 42 U.S. Code § 290dd–2. https://www.law.cornell.edu/uscode/text/42/290dd-2.

22 42 C.F.R. Part 2, https://www.ecfr.gov/current/title-42/chapter-I/subchapter-A/part-2?toc=1.

In some instances, the disclosure of RHI to law enforcement will be routine. Examples include activities involving child abuse, sexual assault, health care fraud, and more. When seeking to limit disclosures of RHI to law enforcement, it is vital not to interfere with the unobjectionable reporting of any health information for a legitimate governmental purpose that does not place individuals at risk for receiving or providing health treatment.

It is likely not possible to write a single, clear substantive standard that distinguishes all appropriate from all inappropriate disclosures of RHI to law enforcement. In the absence of a substantive yardstick, the best alternative is to impose a process that allows for review of disclosures so that the broad unregulated discretion in the Privacy Act of 1974's provisions for disclosure does not allow unsupervised individuals to make inappropriate disclosures. This can be accomplished by requiring the approval of an agency head, general counsel, privacy officer, or other designated senior agency official before any disclosure of RHI may be made to a law enforcement agency.

For cases where disclosures of RHI are routine and unobjectionable, an agency can be authorized to establish classes of allowable disclosures to minimize or avoid procedural requirements when disclosures as a class are unobjectionable. For example, an agency may allow routine sharing of health records with RHI to health researchers who have a certificate of confidentiality.[23] Overall, the purpose is that each agency makes disclosures of RHI in a manner consistent with agency goals.

A third issue is whether agencies can or should impose limits on the disclosure of records to law enforcement. For example, if an agency shares a large number of health records with state health care fraud investigators as part of a joint investigation or otherwise, the agency might seek to limit use of those records in law enforcement investigations unrelated to health care fraud. During the Clinton administration, there was concern about the possibility that health records shared for oversight investigations might be used against individual patients not directly involved in the activities being investigated. This led to the issuance of Executive Order 13181 providing:

> It is, therefore, the policy of the Government of the United States that law enforcement may not use protected health information concerning an individual, discovered during the course of health oversight activities for unrelated civil, administrative, or criminal investigations, against that individual except when the balance of relevant factors weighs clearly in favor of its use. That is, protected health information may not be so used unless the public interest and the need for disclosure clearly outweigh the potential for injury to the patient, to the physician-patient relationship, and to the treatment services.[24]

It is not clear how or if this policy applies when federal agencies share health records with state agencies. The policy might prevent some activities involving use or disclosure of RHI by federal agencies themselves.

The broader issue here is whether and how federal agencies might impose a similar restriction on health records shared with state or local law enforcement. Nothing in the Privacy Act of 1974 seems directly relevant here. The ability of agencies to share information with state and local law enforcement under conditions that restrict use of that information is left here as an open question. Agencies may authority have specific laws or regulations, or they may have inherent authority to share information under restrictions. This issue is not pursued here other than to raise it as a possibility. Each agency could find its own response or the President might cover the subject in an Executive Order.

---

23 See National Institutes of Health, What is a Certificate of Confidentiality?, https://grants.nih.gov/policy/humansubjects/coc/what-is.htm.

24 Executive Order 13181, To Protect the Privacy of Protected Health Information in Oversight Investigations (Dec. 20, 2000), https://www.federalregister.gov/documents/2000/12/26/00-33004/to-protect-the-privacy-of-protected-health-information-in-oversight-investigations.

Given a standard for identifying RHI and a process for overseeing approval of disclosures, the next issue is to find an administrative (non-statutory) way to direct agencies to follow that process. There are three precedents.

Executive Order

Irrespective of its goals, a model for the process of changing agency implementation of the Privacy Act of 1974 comes from an Executive Order issued in the Trump Administration, E.O. 13768 (Enhancing Public Safety in the Interior of the United States). This order directed agencies regarding implementation of the Privacy Act of 1974:

> Sec. 14. Privacy Act. Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information.[25]

The Executive Order did not provide any specifics about implementation or any directions to specific agency officials. The order left it to agencies to determine how to implement the directions.

The same model could work for an Executive Order that directs agencies to add limits on disclosure of RHI. Specifically, an Executive Order from the President could direct agencies to avoid disclosures of RHI to law enforcement if a disclosure could have the result of placing any individual at jeopardy for undertaking activities that support the ability of any woman to obtain reproductive health care for which the woman sought treatment. A broadly stated order of this type could leave it to agencies to determine how to implement the order. A downside of directing agencies in this fashion is that a subsequent President could revoke the order at will.

The Biden administration issued two Executive Orders on reproductive healthcare, however, neither addressed issues relating directly to the Privacy Act of 1974.[26]

A new Executive Order addressing restrictions on Privacy Act of 1974 disclosures might also address restrictions on the subsequent use of health or other records containing RHI by state and local law enforcement agencies.

Office of Management and Budget

The second model for process-based limits comes from a 2017 Office of Management and Budget memorandum that sought to establish a uniform policy on data breaches.[27]

The directions here were quite specific, ordering each agency to adopt routine uses that allowed for appropriate responses in the event of a data breach at the agency. OMB provided the specific language for agencies to use.

A. Privacy Act Routine Uses Required to Respond to a Data Breach

> The SAOP [Senior Agency Official for Privacy] has agency-wide responsibility and accountability for the agency's privacy program and is responsible for overseeing, coordinating, and

---

25 Executive Order 13768, *Enhancing Public Safety in the Interior of the United States (Jan. 25, 2017),* https://www.federalregister.gov/documents/2017/01/30/2017-02102/enhancing-public-safety-in-the-interior-of-the-united-states.

26 Executive Order 14076, *Protecting Access to Reproductive Health Care Services (July 8, 2022),* https://www.federalregister.gov-/d/2022-15138; Executive Order 14079, Securing Access to Reproductive and Other Healthcare Services (August 3, 2022), https://www.federalregister.gov/d/2022-17420.

27 Office of Management and Budget, *Preparing for and Responding to a Breach of Personally Identifiable Information, (Jan. 3, 2017) (M-17-12),* https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf.

facilitating the agency's privacy compliance efforts, including those related to the Privacy Act of 1974.

> The SAOP shall ensure that all agency Privacy Act system of records notices (SORNs) include routine uses for the disclosure of information necessary to respond to a breach either of the agency's PII or, as appropriate, to assist another agency in its response to a breach. The SAOP should include the following routine use in each of the agency's SORNs to facilitate the agency's response to a breach of its own records:
>
> To appropriate agencies, entities, and persons when (1) [the agency] suspects or has confirmed that there has been a breach of the system of records, (2) [the agency] has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, [the agency] (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with [the agency's] efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.[28]

This data breach memorandum went on to require a second routine use that would support assisting another agency with its data breach response. That second routine use is not included here. The example above is sufficient to illustrate the level of specificity that could be included in an OMB memorandum regarding RHI disclosures to law enforcement.

It might be more difficult to order that each agency adopt the same exact routine use on law enforcement because of the variability of existing routine uses on law enforcement across agencies. This question is not further explored here. However, it would be possible to order agencies to amend existing law enforcement routine uses for all SORNs containing any type of RHI by adding text similar to this:

> In the event that a disclosure under this routine use involves the disclosure of RHI to a law enforcement agency, the disclosure must first be reviewed and approved by [an appropriate senior agency official] unless the disclosure is allowed without additional review under a protocol adopted by the Senior Agency Official for Privacy.

Allowing some RHI disclosures under a protocol adopted by each agency would avoid the need for reviewing disclosures that are not likely to place any patient, health care provider, other service provider, or other person at risk of prosecution with respect an activity related to the obtaining of health care for which a woman sought treatment. The OMB memorandum could provide appropriate examples and sample language for the protocols.

It would take agencies several months at best to find and amend all relevant routine uses. Once adopted, it would take agencies some time to change the routine uses in the event that a future OMB directive sought a change in the policy.

An OMB memorandum on the subject might also direct agencies to address limiting the use by state and local law enforcement officials of shared health information against individuals identified in the shared records. Limits on subsequent use by recipients of federal information as a condition of receiving the information might be enforceable by data subjects through an exclusionary rule in subsequent proceedings that sought to use the information in a manner inconsistent with the agency-imposed limits. For example, if a routine use allows the disclosure of identifiable health information to a state public health agency for public health functions, a condition of the disclosure might prohibit the use of any RHI information in any investigation or prosecution of an individual not directly related to a public health function. An alternative formulation might

---

28 Id. (footnotes omitted). The World Privacy Forum questioned the breadth of OMB's proposed data breach routine use, but that issue is not relevant here. The point is that OMB can direct agencies to adopt routine uses.

prohibit the use of any personally identifiable information disclosed for a public health function without further permission from the agency that made the disclosure.

Each of the two methods has advantages and disadvantages. A President can issue an Executive Order quickly, and the order can take effect almost immediately. An OMB directive would take longer to prepare, and agencies would have to find and change multiple SORNs. It would likely take six months at best before all the work could be completed. On the other hand, an Executive Order can be rescinded quickly by a new President whereas action by OMB and compliance by agencies would be more durable, as it would take months to undo a previous OMB memorandum. In either case, however, action by agencies to undo changes would take more time.

Agency Action

In the absence of Presidential action or a directive from OMB, each agency could take steps on its own to restrict the disclosure of RHI to law enforcement. An agency can establish its own internal rules under the Privacy Act of 1974 or under other authority to control the ability of any employee to make a disclosure. An agency rule can also adopt a procedure of requiring the approval of a suitable agency official before any employee (or contractor) can disclose RHI to a law enforcement agency. An agency may also issue an internal rule without changing any existing routine use.

An agency could also adopt a routine use as suggested above for any agency SORN that includes RHI and that allows for disclosure of that RHI to a law enforcement agency. Given that amending a routine use takes months to accomplish, an agency might proceed down both tracks, starting immediately with an internal procedure and an updated routine use later.

Finally, each agency could also explore the possibilities raised by its own legislation or rules of limiting use of RHI information shared with state and local law enforcement agencies against individuals identified in the shared records.

VI. Conclusion

Making changes in the way that federal agencies implement the Privacy Act of 1974 is not a panacea for solving all consequential health privacy issues raised by the *Dobbs* decision. However, a vast amount of identifiable health information held by federal agencies is routinely shared with state or local law enforcement and other agencies.

This report offers several different approaches to imposing new protections for RHI. Adding new procedural protections – and especially protections that do not require either legislation or formal rulemaking – can be accomplished in relatively short order through an Executive Order, through OMB action, and through action by the Federal agencies, as appropriate. These protections could help both for considerations regarding post-*Dobbs* disclosures, and for disclosures of other health information in other circumstances.

These protections have heightened importance given the potential legal consequences for individuals who seek health care and for those who interact with them, including family members, friends, roommates, healthcare providers, health insurers, and others.

Publication date: September 2022
Author: Robert Gellman, Pam Dixon
Permalink: https://www.worldprivacyforum.org/2022/09/privacy-act-procedural-changes-reproductive-health/