United States Senate

WASHINGTON, DC 20510

September 16, 2026

Mr. Scott Kupor
Director
U.S. Office of Personnel Management
1900 E St NW
Washington, DC 20415

Dear Director Kupor,

We write to express serious concern regarding the System of Records Notice (SORN) published by the Office of Personnel Management (OPM) on June 23, 2026, following OPM's December 2025 proposal to obtain detailed health claims information from millions of federal employees, retirees, and their family members[1]. On April 20, 2026, we urged you to immediately reverse course on OPM's potentially illegal and dangerous decision to seek unprecedented access to personal medical records. The modified SORN does not resolve the fundamental privacy, legal, and constitutional concerns raised in our initial letter regarding a federal personnel agency maintaining a longitudinal repository of highly sensitive health information on more than eight million people[2].

The June SORN describes OPM's intent to use identifiable data of federal employees, retirees, and their family members to create person-level longitudinal records that include persistent unique identifiers. Furthermore, OPM would enable authorized personnel to retrieve records using member identifiers for approved linkage, validation, and data-quality activities. Most concerningly, the SORN states that OPM retains the right to re-identify pseudonymized records[3]. In combination, these features create an extraordinarily detailed longitudinal health history that remains linkable to a specific person.

While the SORN claims that pseudonymization will reduce some routine internal exposure, this change alone is not equivalent to eliminating identifiability. The National Institute of Standards and Technology (NIST) cautions that not all techniques that merely mask personal information provide sufficient de-identification and recommends that agencies evaluate re-identification risk, adopt measurable de-identification standards, and conduct governance and risk assessment

---

[1] U.S. Office of Personnel Management, Federal Register, 91 Fed. Reg. 37439. *Privacy Act of 1974; System of Records - OPM/Central-15, Health Benefits Claims and Cost Records*. June 23, 2026. https://www.federalregister.gov/documents/2026/06/23/2026-12596/privacy-act-of-1974-system-of-records

[2] Office of U.S. Senator Adam Schiff. *NEWS: Sens. Schiff, Warner, Schumer Lead 16 Senators in Urging Trump Admin to Reverse Course on Illegal Efforts to Seek Medical Records of Federal Workers*. April 20, 2026. https://www.schiff.senate.gov/news/press-releases/news-sens-schiff-warner-schumer-lead-16-senators-in-urging-trump-admin-to-reverse-course-on-illegal-efforts-to-seek-medical-records-of-federal-workers/

[3] KFF Health News (Amanda Seitz, Maia Rosenfeld, and Darius Tahir). *Trump's Personnel Agency Says It Will Remove Some Identifying Info as It Sweeps Up Medical Records*. July 22, 2026. https://kffhealthnews.org/insurance/trump-opm-federal-workers-medical-records-data-privacy-pseudonymize/

around data releases and access[4]. In the case of OPM's recent SORN, a stable identifier permits repeated encounters to be linked over time, utilizing ZIP code, birth year, provider, service dates, diagnoses, procedures, and drug information to reveal highly specific patterns of care. OPM itself maintains the mechanism needed to reconnect the pseudonymized history to the individual, negating any intended anonymization of data.

The Privacy Act requires federal agencies to only maintain information about an individual that is relevant and necessary to accomplish a purpose required by statute or Executive Order[5]. OPM has failed to provide any justification for the collection of person-level data, instead relying on broad references to program integrity, fraud prevention, or cost evaluation. Additionally, the SORN concerningly permits disclosure of personal data to federal, state, local, territorial, tribal, or foreign law-enforcement authorities whenever OPM believes a record indicates a potential violation of criminal, civil, or regulatory law. It also permits disclosures to other federal agencies to address suspected fraud, waste, and abuse in programs under those agencies' purview. These overly broad allowances to share sensitive health information are extremely concerning, given this administration's clearly stated goals of targeting vulnerable populations[6].

In our April 20, 2026, letter, we specifically expressed concern that sensitive health information could be used in employment actions, including hiring, suitability determinations, appeals, reductions in force, disability accommodation requests, labor-management relations, and performance reviews. We have yet to receive a response to that letter. Furthermore, the June SORN fails to confirm that collected data will not be used for these purposes or related personnel actions. We urge OPM to make these prohibitions explicit and enforceable, extending those protections to matching claims information against personnel systems or other OPM databases.

The SORN also incorporates a National Archives and Records Administration Records Schedule directing OPM to retain Health Claims Records for 30 years, materially increasing the consequences of breach or misuse of highly sensitive health data[7]. OPM has failed to explain why identifiable or re-identifiable longitudinal health claims must persist for decades. At a minimum, OPM should adopt a substantially shorter retention period for identifiable and pseudonymized person-level records, with automatic destruction of linkage keys after the operational need has expired to protect individuals' data.

---

[4] National Institute of Standards and Technology. *NIST Special Publication 800-188: De-Identifying Government Datasets: Techniques and Governance*. September 2023. https://csrc.nist.gov/pubs/sp/800/188/final

[5] U.S. House of Representatives, Office of the Law Revision Counsel. *5 U.S.C. § 552a - Records maintained on individuals*. current preliminary edition. See especially §§ 552a(a)(7), (b), and (e)(1). https://uscode.house.gov/view.xhtml?req=%28title%3A5+section%3A552a+edition%3Aprelim%29

[6] The Trump administration is making an unprecedented reach for data held by states. June 24, 2025. https://www.opb.org/article/2025/06/24/the-trump-administration-is-taking-state-data-for-immigration-push/

[7] National Archives and Records Administration. *Records Schedule DAA-0478-2017-0006: Health Claims Data Warehouse Program (HCDW)*. approved July 20, 2017; PDF created October 18, 2022. Health Claims Records: destroy 30 years after fiscal-year cutoff. https://www.archives.gov/records-mgmt/rcs/schedules/independent-agencies/rg-0478/daa-0478-2017-0006_sf115.pdf

OPM's proposal covers not only federal employees but also annuitants, spouses, former spouses, family members, Postal Service employees and their families, certain tribal employees, separated employees, and former family members. Many of these individuals are not federal employees and have no employment relationship with OPM. Young-adult dependents may receive reproductive, sexual-health, mental-health, substance-use, or other sensitive services that should not be accessible to the federal government, regardless of their family member's Federal Employee Health Benefits (FEHB) coverage. OPM should preserve strict separation among family members' records and prohibit use of one individual's claims information to infer or investigate another family member's conduct.

Lastly, reports indicate that OPM intends to use claims data to identify potential anomalies and that records deemed suspicious by analysts may be referred to OPM's Office of Inspector General for investigation[8]. However, claims data are not complete clinical narratives and may reflect rare diseases, complex pregnancy, disability, chronic illness, fragmented care, referral patterns, or coding practices rather than fraud. We are deeply concerned that adverse referral or action based solely on automated scoring or anomaly detection, without documented human review, will result in wrongful targeting of individuals with complex health needs and subject them to unwarranted administrative or law enforcement scrutiny.

Requested actions

Before OPM proceeds further with expanded collection and use of federal employee health data, we urge OPM to take the following actions:

1. Suspend implementation of any expanded person-level collection under the modified SORN.
2. Publish a field-by-field necessity analysis identifying the statutory purpose served by each data element and explaining why de-identified, aggregated, limited, or sampled data would be insufficient.
3. Use genuinely de-identified or aggregated data by default and permit re-identification only after a documented, individualized showing of necessity, with dual authorization, immutable audit logging, and periodic independent review.
4. Adopt an enforceable firewall prohibiting use, disclosure, matching, or linkage of claims data for any employment or personnel decisions.
5. Prohibit use or disclosure of OPM records to other federal agencies or any law-enforcement entities, including – but not limited to – records related to an individual's for seeking, obtaining, providing, or assisting with lawful health care.
6. Prohibit the use or referral of any health information for unrelated civil, criminal, or regulatory enforcement, particularly when based merely on a potential violation of law

[8] KFF Health News (Amanda Seitz, Maia Rosenfeld, and Darius Tahir). *Trump's Personnel Agency Says It Will Remove Some Identifying Info as It Sweeps Up Medical Records*. July 22, 2026. https://kffhealthnews.org/insurance/trump-opm-federal-workers-medical-records-data-privacy-pseudonymize/

and require senior-level legal and privacy review before any external law-enforcement disclosure.

7. Reevaluate the 30-year retention schedule for health claims records and adopt much shorter retention periods for identifiable and pseudonymized person-level data, including time-limited retention of re-identification keys.
8. Establish independent oversight and public transparency, including annual reporting on the number and categories of re-identifications, external disclosures, law-enforcement referrals, access-control violations, security incidents, and disciplinary actions for misuse.
9. Provide specific protections for dependents and family members, including strict separation of family members' claims and a prohibition on using one family member's health data to infer or investigate another family member.
10. Describe the validation, human-review, error-correction, and anti-bias safeguards that will govern any automated or algorithmic fraud or anomaly detection before a person or provider is referred for investigation.

We support responsible efforts to protect the integrity of federal health-benefit programs. However, OPM's proposals create an unnecessarily broad, decades-long, re-identifiable medical history of millions of workers, retirees, spouses, children, and other family members. We strongly urge OPM to suspend further implementation while these concerns are addressed and to work with Congress, federal employees and retirees, health plans, privacy and civil-rights experts, reproductive-health advocates, and other affected stakeholders to establish safeguards commensurate with the sensitivity of the information at issue.

We request a written response and briefing by OPM on the office's efforts related to the above requested actions no later than September 25, 2026.

Sincerely,

Adam B. Schiff
United States Senator

Mark R. Warner
United States Senator

Tim Kaine
United States Senator

Richard Blumenthal
United States Senator

Chris Van Hollen
United States Senator

Angela D. Alsobrooks
United States Senator