

Congress of the United States

Washington, DC 20515

December 12, 2023

The Honorable Xavier Becerra
Secretary
Department of Health & Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201

Dear Secretary Becerra,

We are writing to share concerning findings from a recent oversight inquiry into the privacy practices of pharmacies related to law enforcement demands for patient records. Through briefings with the major pharmacies, we learned that each year law enforcement agencies secretly obtain the prescription records of thousands of Americans without a warrant.¹ In many cases, pharmacies are handing over sensitive medical records without review by a legal professional. Although pharmacies are legally permitted to tell their customers about government demands for their data, most don't. As a result, many Americans' prescription records have few meaningful privacy protections, and those protections vary widely depending on which pharmacy they use.

As you are aware, this July we and 44 other Members of Congress wrote to you, urging the Department of Health and Human Services (HHS) to revise its regulations under the Health Insurance Portability and Accountability Act (HIPAA) to protect Americans' medical records from warrantless law enforcement agencies' demands.² Since then, we have been conducting oversight into the practices of major pharmacy chains related to their routine disclosure of patients' medical information to law enforcement agencies. Today we write as a follow up to our July letter and to provide you with the findings.

In June 2023, in response to the outpouring of concern from Americans about health privacy and surveillance in post-*Dobbs* America, we sought briefings from major pharmacy chains about their policies related to law enforcement demands for patient prescription records. We contacted the nation's seven largest pharmacy chains, CVS Health, Walgreens Boots Alliance, Cigna, Optum Rx, Walmart Stores, Inc., The Kroger Company, and Rite Aid Corporation, as well as Amazon Pharmacy. These briefings made clear that these companies' privacy practices vary widely, in ways that seriously impact patient privacy.

Americans' prescription records are among the most private information the government can obtain about a person. They can reveal extremely personal and sensitive details about a person's life, including prescriptions for birth control, depression or anxiety medications, or other private medical conditions.

Five of the eight pharmacy companies surveyed — Amazon, Cigna, Optum Rx, Walmart and Walgreens Boots Alliance — attested that they require law enforcement demands for pharmacy records to be reviewed by legal professionals prior to responding to those requests. The three remaining pharmacy chains — CVS Health, The Kroger Company, and Rite Aid Corporation — indicated that their pharmacy staff face extreme pressure to immediately respond to law enforcement demands and, as such, the companies instruct their staff to process

¹ This estimate is based on conversations with all eight companies. Some pharmacies were unable to disaggregate legal demands by the type of requester (for example: law enforcement vs. civil litigant), because they do not keep sufficiently granular data. Collectively, the pharmacies reported receiving tens of thousands of legal demands annually for their patients' pharmacy records. The companies indicated that the vast majority of these requests are in connection with civil litigation.

² https://www.wyden.senate.gov/imo/media/doc/wyden-led_hhs_surveillance_letter_71823.pdf.

those requests in the store. CVS Health and the Kroger Company both defended this practice, arguing that their pharmacy staff — who are not lawyers or paralegals — are trained to respond to such requests and can contact the legal department if they have questions.

All of the pharmacies surveyed stated that they do not require a warrant prior to sharing pharmacy records with law enforcement agents, unless there is a state law that dictates otherwise.³ Those pharmacies will turn medical records over in response to a mere subpoena, which often do not have to be reviewed or signed by a judge prior to being issued. To justify this low standard of protection, several pharmacies cited language in HHS regulations that allow healthcare providers to disclose such records if it is required by law, pursuant to legal process, or pursuant to an administrative request.⁴ HIPAA gives discretion to HHS via regulation to determine the standard of legal process that will govern disclosure of medical records,⁵ which means HHS can revisit and strengthen the minimum bar set in the current regulations to require a warrant.

We urge HHS to consider further strengthening its HIPAA regulations to more closely align them with Americans' reasonable expectations of privacy and Constitutional principles. Pharmacies can and should insist on a warrant, and invite law enforcement agencies that insist on demanding patient medical records with solely a subpoena to go to court to enforce that demand. The requirement for a warrant is exactly the approach taken by tech companies to protect customer privacy. In 2010, after just one Federal Court of Appeals held that Americans have a reasonable expectation of privacy in their emails and that the 1986 Congressionally enacted law permitting disclosures of email pursuant to a subpoena was unconstitutional,⁶ all of the major free email providers — Google, Yahoo, and Microsoft — started insisting on a warrant before disclosing such data.⁷

At the outset of this inquiry, CVS Health was the only company that had publicly committed to publishing annual transparency reports on law enforcement demands.⁸ Over the course of this inquiry, however, Walgreens Boots Alliance and The Kroger Co. committed to adopting this practice. Annual transparency reporting is a standard practice in the technology and telecommunications sectors. Companies like Amazon, Meta, Google, and Apple already publish transparency reports. These reports are of significant utility to journalists, academics, and policymakers as they provide a window into the state of government legal requests for sensitive information. Their widespread adoption across the pharmacy sector would be similarly instructive.

Of the companies reviewed, Amazon Pharmacy was the only one that affirmed that it has a policy of notifying customers about law enforcement demands for pharmacy records, as long as there is no legal prohibition to doing so. Such notification policies are already the norm among technology companies, and carefully balance law enforcement interests and patient privacy by enabling the government to delay notice for a finite amount of time, if notice would disrupt an investigation or put lives at risk. Patients already have an established right to

³ Several pharmacies cited state-law exception(s) to their general practice of disclosing records in response to a subpoena. Louisiana, Montana, and Pennsylvania all have special protections in connection with medical data disclosure. However, federal law enforcement is not subject to these state laws.

⁴ Law enforcement agencies are not HIPAA covered-entities. Still, HIPAA governs how covered-entities, like pharmacies, can disclose health information. There is a specific portion of the statute that centers on disclosures to law enforcement. The types of legal process that suffice are court-orders, subpoenas, and grand jury subpoenas, but there is also a separate administrative route.

⁵ Section 264, codified at 42 U.S. Code § 1320d–2.

⁶ *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010).

⁷ David Kravets, “Yahoo, Like Google, Demands Warrants for User E-Mail,” *Wired*, January 25, 2013. <https://www.wired.com/2013/01/yahoo-demands-warrants/>.

⁸ Raghav Mahobe, “US pharmacy chain CVS to bolster customer privacy protection after shareholder push,” *Reuters*, March 28, 2023. <https://www.reuters.com/business/healthcare-pharmaceuticals/us-pharmacy-chain-cvs-bolster-customer-privacy-protection-after-shareholder-push-2023-03-28/>.

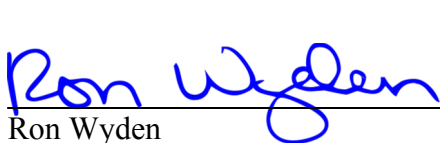
know who is accessing their health information through HIPAA's "Accounting of Disclosure" mechanism. However, the HHS regulations put the burden on Americans to request medical record disclosure data, rather than requiring health care providers to notify their patients. Consequently, few people ever request such information, even though many would obviously be concerned to learn about disclosures of their private medical records to law enforcement agencies. Last year, CVS Health, the largest pharmacy in the nation by total prescription revenue, only received a single-digit number of such consumer requests. HHS can, and should, do much more to protect patient data and push for far more transparency when pharmacy records are disclosed. But pharmacies share some blame, as they are fully within their legal rights to notify customers, and have, thus far, mostly chosen not to do so. Proactively notifying customers about any patient record disclosures to law enforcement that impact their medical records, except where prohibited by a non-disclosure or "gag" order issued by a judge, would be a major step forward for patient transparency.

These findings underscore that not only are there real differences in how pharmacies approach patient privacy at the pharmacy counter, but these differences are not visible to the American people. This information is not posted publicly or included in companies' privacy policies, so the average American is likely unaware that this is even a problem. Further, even if someone were independently motivated to seek out this information, there is no requirement for companies to provide it to them. This opacity inhibits patients from voting with their wallets on the merits of a pharmacy's privacy practices, while also excusing pharmacies from having to compete on this important metric.

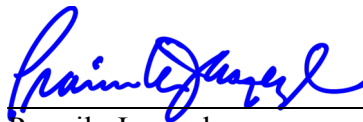
Americans deserve to have their private medical information protected at the pharmacy counter and a full picture of pharmacies' privacy practices, so they can make informed choices about where to get their prescriptions filled. Our oversight has uncovered significant differences between the practices of major pharmacy chains under current HIPAA regulation and this initial inquiry resulted in immediate policy changes at some of these companies. If the landscape were made clearer, patients will finally be able to hold pharmacies with neglectful practices accountable by taking their business elsewhere.

Moving forward, HHS should address the shortcomings in pharmacy privacy practices identified in our inquiry by revising the HIPAA standard for legal process for disclosure as it finalizes the upcoming regulation, conducting regular pharmacy privacy policy surveys and publishing the findings in an easily understandable format. Americans' health records deserve the greatest degree of protection available in law.

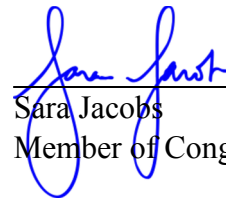
Sincerely,



Ron Wyden
United States Senator
Chairman, Committee on Finance



Pramila Jayapal
Member of Congress



Sara Jacobs
Member of Congress