RAND PAUL
KENTUCKY

United States Senate

WASHINGTON, DC 20510

23 September 2021

The Honorable Patrick Leahy
Chairman
U.S. Senate Committee on Appropriations
Room S-128, The Capitol
Washington, D.C. 20510

The Honorable Richard Shelby
Ranking Member
U.S. Senate Committee on Appropriations
Room S-128, The Capitol
Washington, D.C. 20510

Dear Chairman Leahy, Ranking Member Shelby, and Members of the Committee:

I write to alert you of a potential threat to medical privacy that must be addressed in the FY2022 Labor-HHS appropriation, or any continuing resolution to fund the government.

As you may know, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) established the statutory authority to create a unique health identifier for every individual, employer, health plan, and health care provider in America. However, in each Labor-HHS appropriations bill since the passage of HIPAA, Congress has explicitly restricted the use of federal funds for the development of this sort of national health ID by including Section 510, which reads as follows:

> None of the funds made available in this Act may be used to promulgate or adopt any final standard under section 1173(b) of the Social Security Act providing for, or providing for the assignment of, a unique health identifier for an individual (except in an individual's capacity as an employer or a health care provider), until legislation is enacted specifically approving the standard.

Maintaining this provision is crucial because, as the American Civil Liberties Union (ACLU) has pointed out in the past,

> Absent strong privacy protections, use of unique health identifiers could empower HHS and potentially other federal agencies (including law enforcement) to gain unprecedented access to sensitive medical information. For this reason, it is critical that any use of unique health identifiers be subject to strict privacy and

security protections, which are approved by Congress and subject to public debate."[1]

To your credit, you reinstated the protection of Section 510 to the Senate versions of the FY2020 and FY2021 Labor-HHS appropriations bills, even though the House of Representatives removed it earlier in those appropriations cycles. Unfortunately, this summer the House struck the provision for the third year in a row.

If enacted in its current form, the House bill would open the floodgates for the government to develop a cradle-to-grave tracking system for the private medical history of every man, woman, and child in America. As one of the few physicians in the Senate, I understand the convenience a national patient ID would bring to a health care system that has become increasingly dependent on electronic medical records (EHRs) in recent decades. But I have weighed that convenience against the dangers posed by hackers and cyber-terrorists, and the choice is clear. Recent history shows us that the federal government cannot be trusted to keep such information secure.

For example, in 2006, computer equipment, including a hard drive, was stolen from a data analyst at the Department of Veterans Affairs. That hard drive stored *unencrypted* names, dates of birth, and Social Security numbers of more than 26 million veterans and active-duty servicemembers.[2] After a class action lawsuit was filed, the federal government had to pay out $20 million for needlessly subjecting our veterans to the risk of identity theft.[3]

Apparently, the government didn't learn its lesson after that settlement, because three years later a similar incident occurred, again affecting our military, at the National Archive and Records Administration (NARA). When a hard drive at NARA malfunctioned, the government sent it to an IT contractor for repairs—without wiping it first. That drive held the personally identifiable information (PII) of some 76 million servicemembers.[4]

---

[1] Ronald Newman and Neema Singh Guliani, "ACLU Vote Recommendation on Foster-Kelly Amendment #20 to Minibus Appropriations Bill (Unique Health Identifier)," 12 June 2019: https://www.aclu.org/letter/aclu-vote-recommendation-foster-kelly-amendment-20-minibus-appropriations-bill-unique-health

[2] Christopher Lee, the Washington *Post*, "Worker Often Took Data Home," 26 May 2006: https://www.washingtonpost.com/wp-dyn/content/article/2006/05/25/AR2006052501843.html

[3] Martha Neil, *ABA Journal*, "VA to Pay $20M to Settle Case Over Stolen—and Recovered—Laptop," 10 Feb. 2009: https://www.abajournal.com/news/article/va_to_pay_20m_to_settle_case_over_stolen--and_recovered--laptop

[4] Andy Greenberg, *Forbes*, "The Year of the Mega Data Breach," 24 Nov. 2009: https://www.forbes.com/2009/11/24/security-hackers-data-technology-cio-network-breaches.html#3ca114f1d038

Then in 2014, the government suffered two massive cyberattacks that exposed the PII of another 22 million people. Most of the data involved was stolen from a cache of security clearance files at the Office of Personnel Management (OPM). Every single OPM security clearance application dating back to the year 2000 is believed to have been affected, including financial and health records, user names and passwords, and perhaps most troubling of all, *over a million sets of fingerprints*.[5]

A standardized tracking system would certainly add some convenience to electronic medical filing, but the privacy of the American people must come first. We must seriously consider the risk of hackers or cyber-terrorists using sensitive health information to blackmail or intimidate those with rare diseases, psychiatric conditions, or other medical histories they do not want the world to know about.

As you consider FY2022 appropriations and related measures for any continuing resolution, I urge you to follow your committee's precedent and again reinstate the text of Section 510. The American people deserve no less.

Sincerely,

Rand Paul

Rand Paul, M.D.
United States Senator

[5] Ellen Nakashima, Washington *Post*, "Hacks of OPM databases compromised 22.1 million people, federal authorities say," 9 July 2015: https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/