CITIZENS' COUNCIL FOR Health Freedom
SECURING HEALTH FREEDOM FOR ALL

Unique Patient Identifier (UPI)

10 Reasons to Oppose a National Patient ID

The U.S. House 2020 HHS-Labor appropriations bill would end the longstanding 20-year prohibition against funding and development of a Unique Patient Identifier (UPI, aka "National Patient ID"). The ban began in 1998 when Congressman Ron Paul (R-TX) began to annually add this prohibition to the HHS-Labor appropriations bills. U.S. Senator Rand Paul has now introduced a bill to repeal the UPI from federal statute (S. 2538). The following are 10 reasons to oppose ending the ban on the UPI, or better yet, supporting the repeal of the Unique Patient Identifier:

1. **No card, no care** - This federal number would become a requirement for patient access to care. No American would be able to escape from the number, which would also be used to monitor patients. The number would track whatever facility they use, whomever they see, whatever medications they take, whatever diagnosis they have, procedures, and more.

2. **National medical records system** - The UPI is the keystone -- the one missing piece needed to create a national system of everyone's private medical records. The UPI will link all the medical records of a patient together, wherever they reside, without patient consent. This national database was first proposed in the Clinton Health Security Act (Section 5101) and became law under HIPAA 1996 (Section 262). The lack of a federally-issued patient ID number has prevented the national database from becoming a reality.

   But as Julie Dooling, a director at American Health Information Management Association (AHIMA), said in an audiotaped interview about the UPI: *"[T]hat allows that provider, that physician to collect all of the records from that patient…"* She later commented in the audio, *"I think that there's a lot of unknowns here. I think that we all have to work together so that the goal is accurate patient matching to enable seamless interoperability health records nationwide."* ("Making the Case for National Unique Patient ID: Julie Dooling of AHIMA Offers Arguments in Favor of an Identifier," Marianne Kolbasuk McGee, *Healthcare Info Security*, 10/11/19, transcribed by CCHF)

3. **Data sharing without consent** - HIPAA is not a privacy rule. It is a permissive data-sharing rule. According to a 2010 HHS rule, 2.2 million entities can have access to a person's medical records if those holding the data agree to share it. As David Brailer, the first National Coordinator of Health IT once said, *"You can't force a covered entity to give your data to someone you choose, and you can't stop them from giving it to someone they choose."* Thus, a federal patient ID number will facilitate this access by linking all patient data together and providing HIPAA-authorized access to all patient medical records. No consent required.

4. **Unconstitutional** - If permitted to be developed, the federal government would issue a unique ID number to every citizen, which would facilitate government surveillance, tracking, and analysis of patients, doctors, conversations, and confidential information discovered in the exam room and at the hospital bedside. This is a violation of the Fourth Amendment,

which prohibits unreasonable search and seizure of persons, homes, papers and effects without probable cause and a search warrant that *"describes the place to be searched, and the persons or things to be seized."*

5. **No fresh second opinions** - Physicians differ in treatment choices and some physicians can be biased against a patient or disagree with preferred outcomes. Patients have lived, or lived longer, because of a second opinion untainted by the first physician's findings and assessment. Patients need to be able to see a second physician who does not know what the previous physician diagnosed, or ordered, or wrote.

6. **Data security threat** - The 2009 HITECH Act's requirement that physicians and hospitals install and "meaningfully" use a government-certified version of an electronic health record (EHR) or face penalties has led to breaches, widespread hacking, ransomware attacks, physician burnout and system shutdowns. The nationwide computerized medical records system created by the UPI would become a rich target for hackers. As of March 31, 2018, the HHS Office for Civil Rights recorded 344,823 breaches affecting fewer than 500 patients, and 2,267 breaches affecting 500 or more patients—approximately 178 million individuals.

7. **Detailed dossiers** - EHRs are now including details unrelated to patient medical encounters, such as "social determinants of health" (SDOH), which are *"The conditions in which people are born, grow, live, work and age"* (World Health Organization). These can include behavioral choices, biological and genetic factors, income level, occupation, early childhood experiences, availability of transportation, gender inequity, educational opportunities, access to drinking water, leisure opportunities. Judith Faulker, CEO of Epic, the nation's largest EHR vendor, wants the EHR to become a CHR (Comprehensive Health Record) and claims: *"We have to look at who you are, what you eat, how much you sleep, and what your social conditions are like."* The UPI would help build this dossier on every American.

8. **Socialized Medicine** - Socialized medicine is facilitated by socialized health data systems. Once every American has a government-issued patient ID number, America will have a government-controlled health care system. HIPAA and four national health care IDs (EIN, HPID, NPI, UPI) were first proposed in the Clinton Health Security Act (national health care plan), but became law under HIPAA in 1996. However Congressman Ron Paul's annual prohibition on funding the UPI has stopped the UPI from being developed and issued.

9. **No escape; No consent** - Whatever history is recorded in the EHR—from womb to tomb—including every embarrassing condition, personal secret confided in confidence, biological vulnerability, genetic predisposition, diagnosis, or family history could potentially be seen, used, or shared by all, most, or some of the more than 702,000 covered entities and 1.5 million business associates, without patient consent—all accessible over the Internet.

10. **Won't work** - Julie Dooling at AHIMA, in the interview with Healthcare Info Security, supported the UPI but said this about the problems of duplicate names, fraud, dirty data, security, and accurately identifying individuals: *"[U]nique patient identifier is not a total solution. . . . The unique patient identifier is not going to solve this total solution."*