For Immediate Release  
October 8, 2018

CONTACT:  
Deborah Hamilton, Hamilton Strategies, Media@HamiltonStrategies.com, 610.584.1096, ext. 102, or Patrick Benner, ext. 104

Creating National Biometric System for Patient Matching Will Threaten Privacy and Security

Citizens’ Council for Health Freedom Responds to New Pew Study on ‘Patient Matching’—Just Another Name for ‘National Patient ID’

ST. PAUL, Minn.—The Pew Research Center last week released a new public opinion report on “patient matching,” a term which is simply a less-offensive moniker for “national patient ID,” says Citizens’ Council for Health Freedom (CCHF).

Pew led off the study with this dubious claim about developing a national system of patient identification: “Enhanced Patient Matching Is Critical to Achieving Full Promise of Digital Health Records.” However, problems abound with both the idea of pushing a national patient ID strategy to link patient data and the proposed use of a national infrastructure to collect and store the biometrics of Americans, such as their DNA, fingerprints or iris scans.

At an event with the study’s authors, Pew claimed “many of the participants agreed that getting organizations to settle on one unified national strategy for records matching is more crucial than agreeing on one technology,” Politico’s “Morning eHealth” newsletter reported.

However, CCHF president and co-founder Twila Brase doubts the methodology and questions the extremely small size of the survey group—just 95 respondents in 11 focus groups in five cities—especially for a topic so significant and having so much impact on patient privacy and consent rights.

“Why such a large claim from the opinions of such a small group of Americans?” Brase asked. “Studies show Americans want privacy and are concerned they have none. As reported in ‘Big Brother in the Exam Room,’ a Black Book survey of 12,090 consumers in late 2016 found 87 percent unwilling to comprehensively divulge all of their information to their doctors due to privacy concerns and 81 percent concerned that information on chronic conditions is being shared beyond their chosen doctor and payer. Their concerns are valid. Under the HIPAA disclosure rule, their consent is not required for most data-sharing, unless a stronger state law exists. The Black Book survey mimics the concerns found in the 2000 Gallup survey of 1,000 people. Imagine how much greater the intrusion, if every patient medical record from birth to death could be linked through a national identifier.

“The evidence for the Pew report is razor-thin and questionable,” Brase continued. “The questions asked and the raw data are not disclosed, and the size of the survey group was minimal. Plus, it’s not clear that the privacy concerns about national IDs and biometrics, or the authority under HIPAA to share data broadly
without patient consent, were explained to the 95 individuals who participated in the focus groups. For example, as the report notes, once biometrics are utilized, a door is opened that can never be closed. DNA, iris scans and fingerprints are unique and cannot be changed if a computerized single national infrastructure is hacked and the biometrics are stolen. Did Pew warn the 95 individuals about this possibility? Nothing in the report says they did. Did these 95 people understand that interoperability would involve all their medical records and not just the specific information that a patient wants to get from Dr. A to Dr. B.?”

CCHF also pointed to a few key findings in the Pew report:

- Sweeping claim without raw numbers or definitions of terms: “On the whole, participants expressed support for enhanced interoperability—fueled by better matching—to give patients and clinicians more timely access to data, though they expressed concerns about the prospects of information being stolen, privacy, and the sale of the data.”
- U.S. law currently prohibits HHS to fund the creation of a unique patient identifier without explicit approval from Congress. This is in place for good reason, Brase says. National patient IDs open the door to government surveillance and outsider controls on access to patient care (i.e. “No card, No care”).
- National ID systems are subject to error and fraud, such as the Social Security number.
- The cost to create government-issued numeric health identifiers for all patients would be exorbitant. The Centers for Medicare & Medicaid Services estimated in 2011 that transitioning from Social Security Numbers to a new Medicare identifier could cost more than $800 million. Congress provided $320 million for the effort in the Medicare Access and CHIP Reauthorization Act.
- Some states, like Minnesota and Nevada, passed state legislation in the 1990s to create their own health identifiers, with little progress being made in the past 20 years.

Brase is the author of the new book, “Big Brother in the Exam Room: The Dangerous Truth About Electronic Health Records,” which exposes how government EHRs negatively impact both patients and doctors. Already in its second printing, “Big Brother in the Exam Room,” published this summer by Beaver’s Pond Press and previously ranked at least three times as the No. 1 best-seller on Amazon (in the privacy and surveillance category and the Medical History and Records category), also details how EHRs affect privacy, personalized care, costs, patient safety and more, according to doctors and data from more than 125 studies.

“Big Brother in the Exam Room” is available online wherever books are sold and at www.BigBrotherInTheExamRoom.com.

For more information about CCHF, visit www.cchfreedom.org, its Facebook page or its Twitter feed @CCHFreedom. Also view the media page for CCHF here. For more about CCHF’s initiative The Wedge of Health Freedom, visit www.JointheWedge.com, The Wedge Facebook page or follow The Wedge on Twitter @wedgeoffreedom.

###

To interview Twila Brase of Citizens’ Council for Health Freedom, contact Deborah Hamilton, Media@HamiltonStrategies.com or 610.584.1096, ext. 102, or Patrick Benner, ext. 104.