NEWS RELEASE

For Immediate Release
March 24, 2015

CONTACT:
Deborah Hamilton, Hamilton Strategies, 215.815.7716, 610.584.1096, DHamilton@HamiltonStrategies.com

Dangerous Interoperability Bill would Connect Electronic Health Records across the Country

Citizens' Council for Health Freedom Says Americans' Private Health Data is Already at Risk and Forced Interoperability Will Make Gaining Access Even Easier

ST. PAUL, Minn.—One lawmaker is pushing for a bill that will require all Electronic Health Records (EHRs) in the country to work together and be able to communicate from system to system.

That plan might sound efficient and technologically sound, but ***Citizens' Council for Health Freedom (CCHF, www.cchfreedom.org),*** a Minnesota-based national organization dedicated to preserving patient-centered health care and protecting patient and privacy rights, says the bill would be dangerous for patients and would compromise the privacy of their personal medical information, which is already at risk.

Rep. Mike Burgess (R-Texas) is working on a bill that will require EHR interoperability by 2018 and created a congressionally appointed 12-member advisory committee to replace the current federal advisory committees. According to a report by iHealthBeat, the new board would develop a standard for interoperability that EHR systems must meet by 2018 to gain certification and avoid penalties. By next July, the bill would also call for recommended standards for measuring interoperability.

"Given that there are no patient consent requirements in the HIPAA 'privacy rule,'" Brase said, "the interoperability sought by proponents will ensure that the 2.2 million entities, plus government agencies, that are allowed access under HIPAA and HITECH without patient consent will get easy access to patient medical records via online portals. The current lack of interoperability is the only thing keeping the eHealth Exchange—a national medical records system—from becoming fully operational under the 'no consent required' of HIPAA and HITECH. As soon as there are hook-ups between all companies that are holding our medical data, there is a huge problem and a great risk.

"Under the HIPAA 'privacy rule' and HITECH," she continued, "all of our private records are susceptible to widespread sharing, use and analysis, down to our genetic test results, doctors notes, behaviors, diagnoses, personal comments and more. No patient consent is required. Essentially, our private data becomes owned by outsiders, and access decisions are taken out of our control. Given the absence of patient consent requirements for data sharing, the lack of

interoperability is all that protects Americans from a nationally imposed breach of their medical privacy."

Brase has been working against the EHR push, including in her home state of Minnesota, where doctors, clinicians and mental health professionals are fighting the state's EHR mandate, which unlike the federal EHR mandate, has no opt out options. She points out that private medical data is already much too accessible, too easily shared and unsecured. But an inoperability bill will guarantee even easier access to private data without patient consent.

In a recent interview with CNSNews.com, Brase also said that a national medical records system is the foundation for the national health care system, so, in essence, the Burgess bill would help prop up a floundering and doomed Obamacare health care system.

Brase also points to the recent health insurance hacks as evidence of the dangers of interoperable Electronic Health Records. Last week, Premera Blue Cross announced that a cyberhacker attack may have compromised the personal and/or health data of 11 million people. According to NBC News, the Premera hackers may have gained "unauthorized access" to its systems in a "sophisticated attack" that began in May 2014 and may have accessed data including name, date of birth, Social Security number, mailing address, email address, telephone number, member identification number, bank account information, and claims information, including clinical information.

Last month, in an even larger attack, the data of as many as 80 million people may have been accessed through a massive hack at the health insurer Anthem—including 8 to 18 million non-Anthem customers who are covered under other Blue Cross Blue Shield plans but used their insurance in the past decade in a state where Anthem operates.

"Medical identity theft is the most pressing cybercrime outside of national security," Brase said. "Interoperability would make medical identity theft even easier, as access to some data could easily translate into access to all data."

For more information about ***CCHF,*** visit its web site at www.cchfreedom.org, its Facebook page at www.facebook.com/cchfreedom or its Twitter feed, @CCHFreedom.

Citizens' Council for Health Freedom *is a patient-centered national health freedom organization based in St. Paul, Minn., that works to protect health care choices and patient privacy.* ***CCHF*** *sponsors the daily, 60-second radio feature, Health Freedom Minute, which airs on approximately 350 stations nationwide, including 200 on the American Family Radio Network and 100 on the Bott Radio Network. Listeners can learn more about the agenda behind health care initiatives and steps they can take to protect their health care choices, rights and privacy.*

###

For more information or to interview Twila Brase, president and co-founder of *Citizens' Council for Health Freedom*, contact Deborah Hamilton at 215-815-7716 or 610-584-1096, or Beth Harrison at 610-584-1096, Media@HamiltonStrategies.com.