CITIZENS' COUNCIL FOR
Health Freedom
SECURING HEALTH FREEDOM FOR ALL

March 30, 2015

CCHF Public Comments on ONC Interoperability Roadmap to Impose Nationwide Data Sharing and End Medical Privacy

Citizens' Council for Health Freedom is a national health care policy organization with a vision of "Health Freedom for All." Our mission is to protect health care choices, individualized patient care and medical and genetic privacy rights.

Here are our organization's public comments on the **"Connecting Health and Care for the Nation: A Shared Nationwide interoperability Roadmap, Draft Version 1.0**" – a 166-page document, which most of the public do not know about and will never read, although it is intended to end their medical privacy rights forever.

We are opposed to the creation of national electronic medical records and patient and doctor tracking system— and the proposed ONC Roadmap to impose that system. We therefore, call for ONC to start over with privacy rights as a priority.

In particular, we note that the federal HIPAA "no privacy" rule authorizes this kind of broad sharing without the patient's consent. Americans, deceived by the term "privacy rule" believe that their data cannot be shared without their consent. The Roadmap briefly mentions that there should be some effort to let patients know how broadly their data can be shared, but the real answer to preserve the integrity of the health care system and the confidential patient-doctor relationship necessary for patients to trust and timely use the system – the sole purpose of the health care system – is to restore patient consent requirements over all sharing of patient data.

The following list, although not inclusive of all our concerns, provide specific reasons for our opposition:

- **Plan to undo right of state legislatures to actually protect the medical privacy rights of their constituents.** The Roadmap proposes to undo the "state preemption" part of HIPAA and conform all laws to the HIPAA "no privacy" rule: "The U.S. legal, regulatory and policy landscape for sharing health information is complex. When the laws are designed to protect health information and individual rights, they also must enable appropriate information sharing to support health and health care…. (p. 66 – 67)

  "[I]t has become clear that the complexity of the rules environment will continue to hinder the development and adoption of a consistent nationwide technical framework…for electronically managing individuals' basic and granular choices until the complexity is resolve. Reducing variation in the current legal, regulatory and organizational policy environment related to privacy that is additive to HIPAA [state privacy laws] will help facilitate the development of technical standards and technology that can adjudicate and honor basic and granular choices nationwide in all care settings while ensuring that special protections that apply as a results of deliberative legislative processes remain conceptually in place… Through the course of harmonization, however, individual privacy rights as specified in state and federal laws must not be substantively eroded." (p. 67) [Emphasis added.]

In fact, the Roadmap instead calls for "state government [to] standardize existing laws pertaining to 'sensitive' health information…so that those laws mean the same things in all U.S. jurisdictions" and calls for "All of state governments and stewards of health information…[to] revise regulations and policies to align with the consensus on non-sensitive information that is permissible to exchange – or access, use and disclose – for TPO [Treatment, Payment and Health Care Operations] without an individual's written consent establishing consensus background rules for the nation." [Emphasis added.]

Thus, the administration's plan is not only to erode, but also to eliminate any individual privacy rights enacted by state legislatures. That's the point of federal harmonization and we strongly oppose it. The only protection patients have from ONC's all-points sharing interoperability plan is: 1) state privacy laws; 2) the practitioner's right to opt-out of the EHR mandate; 3) practitioner fear of lawsuits for violating their patient's privacy; and 4) the lack of nationwide interoperability because EHR vendors do not want to become public utilities (arms of the state government). The HIPAA "no privacy" rule allows state legislatures to enact laws that are stronger than HIPAA and provide patients with real privacy rights not found in HIPAA.

- **The false presumption that patient medical information is a public good for use by multiple entities, including government, rather than the privately owned and very personal property of the patient:** "Data holders and entities facilitating exchange of electronic health information should ensure standards are prioritized, developed and implemented to support the public interest, national priorities and the rights of individuals." (p. 33) [Emphasis added.] *However, the only person whose interests need protection and prioritization is the patient. Until HIPAA was made effective in 2003, permitting broad sharing and exchange of data (and EHRs and HIE), practitioners understood they could be sued if they shared the patient's data without the patient's consent. Thankfully, some of that fear remains today.*

- **Hacking of patient data is likely and acknowledged in Roadmap, but no plans to interrupt the administration's EHR interoperability agenda:** "As health IT systems have become increasingly connected to each other, cyber threats have concurrently increased at a significant rate. In an interoperable, interconnected health system, an intrusion in one system could allow intrusions in multiple other systems. Additionally, there is high variability in the capabilities and resources healthcare organizations have at their disposal to prevent cyber-attacks. Large organizations have the resources and expertise to have a dedicated information security team to address cyber security; however, small and mid-sized health care organizations, like other small businesses, may not have these resources an may not be able to afford them. … Many in the industry do not realize the significant risk to their systems and do not understand the importance and urgency of implementing security best practices to prevent cyber attacks. Despite being identified as critical infrastructure for the nation, the healthcare system could do more to prepare for a cyber-security attack." (p. 55-56) Other than requiring contracts and post-attack responses, the Roadmap says, "All data stored in any database connected to the network (whether through a companion system, interface engine, or gateway) is fully encrypted." (p. 57)

Despite already spending upwards of **$30 billion** to get every practitioner to put their patient's data "on the grid" where it is vulnerable to hackers, ONC only offers to "work with payers to explore the availability of private sector financial incentives to increase the rate of encrypting…" (p. 57) [Emphasis added]

*Encryption didn't help Blue Cross Premera, **a payer**, whose 11 million encrypted records were hacked. Earlier this year, Blue Cross Anthem, **a payer**, had 80 million records hacked. As House E&C Committee Chairman Fred Upton (R-Mich.) said it is now "not a matter of if [businesses] will be infiltrated, but when." -- article in* The Hill.

- **The call for nationwide harmonization and policy alignment.** The Roadmap calls on governance entities and data holders (EHR vendors) to "align their policies with the nationwide governance framework" for implementation of a national health data system and the end of patient privacy and physician autonomy. (p. 35)

- **The desire for "seamless flow of electronic clinical health information."** The Roadmap considers using payment controls and federal regulation to force today's "complex web of electronic health information sharing arrangements that create some degree of interoperability within specific geographic, organization and vendor boundaries" to "produce seamless nationwide interoperability to support a learning health system." (p. 29) *Many patients will not want such seamless flow or outside access, and no practitioner should be forced to violate the trust and confidentiality of their patients.*

- **The shift from using a patient's data for their treatment to the use of data for ongoing research purposes without patient consent:** "The goal of this shift is to a nationwide learning health system—an environment that links the care delivery system with communities and societal supports in 'closed loops' of electronic health information flow, at many different levels, to enable continuous learning and improved health." (p. 8) [Emphasis added.]

- **Broad sharing of data without specific, voluntary, and informed patient consent:** "The Roadmap focuses on actions that will enable a majority of individuals and providers across the care continuum to send, receive, find and use a common set of electronic clinical information at the nationwide level of the end of 2017. Although this near-term target focuses on individual and care providers, interoperability of this core set of electronic heath information will also be useful to community-based services, social services public health and the research community." (p. 10)

- **A vision of interoperability that many patients would not accept:** "An interoperable health IT ecosystem should support critical public health functions, such as real-time case reporting, disease surveillance and disaster response, as well as data aggregation for research and value-based payment that rewards higher quality care, rather than a higher quantity of care." (p. 17) *These purpose portend planned government intrusions, research that may be objectionable, use of patient data to develop rationing protocols, and using the patient's data to financially penalize the patient's doctor for providing necessary care.*

- **The elements necessary for the provision of medical care – data quality, usability and workflow – which are problematic in today's EHR is relegated to a later discussion**: "There are also many aspects of health IT beyond interoperability that are important and will be critical to a learning health system, including technology adoption, data quality, usability and workflow." As the Roadmap notes, the deserve "separate, dedicated attention." *But they actually deserve to get ALL the attention until such time as those problems are solved because the focus of medical professionals should be taking care of the patient, not trudging through difficult systems to implement an intrusive national medical records system.*

- **The euphemistic Newspeak claims on privacy:** HHS will consider clarifying the so-called HIPAA privacy rule "to effectively support individual privacy in a learning health system" [allowing research without consent] and "clarify privacy and security requirements that enable interoperability." [allowing broad sharing of patient data for non-treatment purposes]. The Roadmap claims, "The HIPAA Privacy Rule was designed to ensure that individuals' health information is protected while allowing the flow of health information needed to provide high quality health care." Additionally, "all organization regulated by HIPAA must understand in the same way that HIPAA, through its permitted uses and its privacy protections, actually enables interoperability." *None of this is actually privacy, and as listed earlier, the Roadmap proposes to undo stronger state laws that actually protect privacy. Here are two more examples on Orwell-like Newspeak from page 68:*

  - "ONC will brief key stakeholders, possibly including NCSL, NGA, privacy advocates and Congress on findings regarding the complexity of the rules environment, especially the diversity among more restrictive state laws that seek to regulate the same concept impedes computational privacy"

  - "ONC, in collaboration with states, national and local associations, and other federal agencies will convene a Policy Academy on Interoperability with a particular focus on privacy as an enabler of interoperability."

- **The push to get citizens to report their daily activities, thoughts and behaviors for outsider access and analysis:** "Health information such as personally maintained dietary logs, medical device data such as blood glucose readings and many other bits of information that inform health-related decision-making (both inside and outside the care delivery system) must also be connected in reusable ways in a dynamic ecosystem supported by health IT. Across this ecosystem, electronic health information in its broadest sense is and increasingly needs to be the stuff of everyday decision-making by everyday people." (p. 17)

- **The expansion of health IT into the personal non-clinical lives of citizens:** "The health IT community must expand its focus beyond institutional care delivery and health care providers, to a broad view of person-centered health….Most determinants of health status are social and are influenced by actions and encounters that occur outside traditional institutional health care delivery settings, such as in employment, retail, education and other settings." This expansive role is also seen here: "Providers, government, payers and health IT developers have a role in supporting and empowering individuals to becomes effective managers of their health and wellness where they live, work and play, using information and technology." (p. 46)

- **The change from a "learning healthcare system" to a "learning health system" which portends broad intrusions in the daily lives of individuals:** "A learning health system is characterized by continuous learning cycles at many levels of scales, and includes a broad array of stakeholders that include the care delivery system, but extend beyond care delivery to public health [government] and the research community." (p. 19)

- **The focus on "population health" and the de-emphasis on the rights of individual patients and their right to be informed about and offered the best**

medical advice and options for treatment. The stated rationale for a national medical records system – a "learning health system" – violates the rights of patients to a confidential patient-doctor relationship, the right to not be a research subject, the right to patient autonomy and the right to have a physician with autonomy.

The term "contributions" is false because the data is being forcibly shared without the patient's consent. Furthermore public health is the government, and a patient has a Fourth Amendment right against search and seizure of their persons, homes, papers and effects, including their personal health information. Additionally, terms in the following paragraph, such as "collaboratively," "efficiently," "equitably," and "public good" leave the patient out in the cold in decision-making about their data and their health care choices and call on the doctor to serve the State's interests, not the patients:

> "A learning health system [w]ill improve the health of individuals and population. This learning health system will accomplish this be generating information and knowledge from data captured and updated over time – as an ongoing and natural by-product of contributions by individual, care delivery systems, public health programs and clinical research – and sharing and disseminating what is learned in timely and actionable forms that directly enable individuals, clinicians and public health entities to separately and collaboratively make informed health decisions…The proximal goal of a learning health system is to efficiently and equitably serve the learning needs of all participants, as well as the overall public good" (p. 18)

- **Matching and linking patient and provider data without patient consent:** "As a learning health system evolves, more than individual/patient-specific information from health records will be matched and linked, including provider identities, system identities, and device identities and others to support public health and clinical research." (p. 24)

- **Forcing EHR companies to become public utilities forced to share data for the implementation and imposition of a national medical records system:** "Data holders and entities facilitating interoperability of electronic health information should not establish policies or practices in excess of law that limit the availability of electronic health information by another entity that is in compliance with applicable laws and these governance principles." (pp. 32-33)

- **Enforcement of practitioner compliance through financial penalties:** "It is important that there be a set of 'rules for the road,' a multi-stakeholder process to address operational issues to support the rules of the road and a mechanism for demonstrating and identifying compliance with the rules, as well as addressing noncompliance." (p. 30). The Roadmap further states, "A supportive business and regulatory environment that encourages interoperability: Rules that govern how health and care is paid for must create a context in which interoperability is not just philanthropic, but is a good business decision." (p. 23)

Additionally, the Roadmap calls for "requirements/penalties that raise the costs of not moving to interoperable systems." (p. 39) As the document notes, "In order to bill for [chronic care management, according to the 2015 Physician Fee Schedule] physicians will be required to utilize certified health IT to furnish certain services to beneficiaries." In addition, under federal value-based payment programs "programs may transition to [adoption of health IT] measures more directly focused on interoperability." [Emphasis added.]

- **Real-time, bedside and clinic exam research on patients without asking patients for their consent:** "The Roadmap shifts the nation's focus from meaningfully using specific technologies with specific features to working together as a nation to achieve the outcomes desired from interoperability and a learning health system. Providers should have the tools they need to support a cultural shift in the way they practice medicine and use technology that supports the critical role of information sharing." (p. 50). [Emphasis added]

  This includes "the availability of holistic longitudinal information on each individual in a computable format," meaning a patient has nowhere to go to keep a secret. It includes outsider-generated "clinical decision support (CDS) tools" on their computer screens that tell doctors how to practice medicine and track their compliance with the CDS protocols ("calculation of electronically specified clinical quality measures" for "guiding the transformation of the delivery system to a learning health system." (p. 50) [Emphasis added.]

  This national transformation, shift in practice of medicine, use of outsider-derived treatment protocols is a research project being done to the patient without the patient's knowledge or consent.

Sincerely

Twila Brase, RN, PHN
President and Co-founder