CITIZENS' COUNCIL FOR Health Freedom

SECURING HEALTH FREEDOM FOR ALL

May 23, 2019

The Honorable Alex Azar
Secretary
U.S. Department of Health and Human Services
200 Independence Avenue S.W.
Washington, D.C. 20201

Dear Secretary Azar,

Thank you for this opportunity to comment on the proposed rule for "Interoperability, Information Blocking, and the ONC Health IT Certification Program." **Our comments will focus mostly on the heart of the issue rather than the myriad details of this proposal.**

Citizens' Council for Health Freedom is a national patient-centered organization located in St. Paul, Minnesota. We have a free-market focus. Our mission is to protect health care choices, individualized patient care and the right to medical and genetic privacy.

Unfortunately, the EHR mandate, combined with the permissive HIPAA data-sharing rule, has eliminated patient privacy rights for most Americans, allowing their data to be shared broadly nationwide, perhaps globally, without their consent. Only patients who pay cash and know that cash payment gives them the right to ask for privacy protections—as well as patients in a few states with real privacy laws (e.g. Minnesota)—continue to have some medical privacy rights.

Notably, the proposed rule mentions privacy 329 times by our count, but doesn't actually protect it, at least not at the federal level which is under HIPAA with some exceptions (e.g. 42 CFR part 2). For example, on page 7527, the proposed rule states:

> We designed these exceptions to . . . ensure that the information blocking provision does not require the use or disclosure of EHI in a way that would not be permitted under the HIPAA Privacy Rule. Our intent is that the information blocking provision does not conflict with the HIPAA Privacy Rule.

But, as HHS surely understands, HIPAA permits unprecedented disclosure and use of private patient information *without* patient consent:

> "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." - **David Brailer**, former National Coordinator, ONC, on HIPAA (*Healthcare IT News*, May 1, 2015)

And where the proposal says "consent for use of restricted data," relatively little data is restricted for disclosure or use under HIPAA. Or as Niall Brennan, former CDO of CMS tweeted: **"HIPAA is actually quite permissive…"**(May 22, 2019). Thus HIPAA "privacy" protections are mostly security protections. In short, HIPAA requires confidential data be kept secure during continued use and disclosures (without patient consent) to prevent access by anyone who is not allowed by HIPAA to disclose and use the data.

Furthermore, there's no requirement to honor a patient's request for privacy. In 171.202, regarding exceptions to the prohibition against "information blocking":

> (e) *Respecting an individual's request not to share information.* In circumstances where not required or prohibited by law, an actor may **choose** not to provide access, exchange, or use of an individual's electronic health information if— (1) The individual requests that the actor not provide such access, exchange, or use; (2) Such request is initiated by the individual without any improper encouragement or inducement by the actor; (3) The actor or its agent documents the request within a reasonable time period; and (4) The actor's practice is implemented in a consistent and nondiscriminatory manner. (Emphasis added.)

Therefore, we find little about this interoperability proposal that protects patient privacy, while striving to share it more broadly. That said, federal law still allows states to pass real privacy laws, as Minnesota did three decades ago—an example every other state should follow. As this proposed regulation acknowledges (pp. 7509 and 7528):

> With regard to the statute's exclusion of practices that are ''required by law'' from the definition of information blocking, we emphasize that ''required by law'' refers specifically to **interferences with access, exchange, or use of EHI that are explicitly required by state or federal law**. By carving out practices that are ''required by law,'' the statute acknowledged that there are state and federal laws that advance important policy interests and objectives by restricting access, exchange, and use of their EHI, and that practices that follow such laws should not be considered information blocking.
>
> **Certain federal and state laws require that a person provide consent before his or her EHI can be accessed, exchanged, or used for specific purposes**. Although the HIPAA Privacy Rule does not have consent requirements for an individual (as that term is defined in the HIPAA Privacy Rule) when a covered entity or business associate is using or disclosing ePHI for treatment, payment or health care operations, some state laws and federal laws and regulations do require that a person's consent be obtained by the disclosing party/entity before disclosing certain health information. . . . It would not be considered information blocking to refuse to provide access, exchange, or use of EHI if the actor has not received the person's consent…." (Emphasis added.)

We also note with appreciation the following language about inducements:

> "…to the extent that the precondition at issue was the provision of a consent or authorization by an individual, the actor must not have improperly encouraged or induced the individual to not provide the consent or authorization. This does not mean that the hospital cannot inform an individual about the advantages and disadvantages of exchanging EHI and any associated risks, so long as the information communicated is accurate and legitimate."

However, we believe this important requirement must also be *in reverse*. There must be no improper inducements for patients *to sign* these consent forms.

For example, many, perhaps most, patient consent forms in Minnesota—where a state law requires patient consent prior to sharing or using patient data in most situations—are coercive. The single-signature forms **include consent for treatment plus consent for data sharing** for treatment, payment, health care operations, research as well as acknowledgement of the Notice of Privacy Practices—forcing many patients to agree to the disclosure and use of their data as a prerequisite to receiving medical treatment. Some patients have been told they must sign the form or they cannot be seen. And indeed, some have left the clinic, canceling their appointment and foregoing care, rather than sign the form. We have heard and received these stories direct from patients.

Furthermore, some consent forms include language that says the form "cannot be altered" without first contacting the health care corporation to seek permission, thus prohibiting patients from crossing out objectionable sharing and use of their data.

Therefore, related to your question on page 7531, a "meaningful opportunity to provide consent" should also include a "meaningful opportunity to choose whether or not to provide consent." There should be no coercion, and no coercive consent forms that mandate consent for data-sharing before the patient is allowed to receive care.

Non-Regulated Entities

Regarding your question on page 7529, we do not believe federal law allows HHS to impose HIPAA-like conditions using this rule or any other rule on providers or others that are not regulated by the HIPAA law or the HIPAA rule.

General Opposition

Notwithstanding the acknowledged exceptions for state privacy law, we oppose this rule because it seeks to effectuate HIPAA-permitted, broad use and disclosure of confidential patient data nationwide, without patient consent. In short, it makes HIPAA worse. It mandates the conditions that HHS believes will improve the sharing and use of confidential patient data without patient consent. In fact, lack of interoperability is one of the few things that protects American FROM the vast array of permissive disclosures and uses of confidential patient information that are allowed by HIPAA today.

In addition, we see nothing in this rule to undo the dangers patients face from the electronic health records (EHRs) Congress imposed on medical practices and at hospital bedsides. Instead the rule proposes **continued government certification of the EHR** (1,465 mentions of "certification") and proposes to use these faulty technology systems to advance seamless unconsented disclosure and use of confidential patient data. Notably, a recent survey showed that 54% are very or somewhat concerned about privacy, 45% are concerned about medical information errors in the EHR, and 21% of patients found errors in their EHR records, incorrect data that interoperability, if achieved, will distribute more profusely making it even more difficult to correct the record. https://www.healthcaredive.com/news/patients-mostly-accept-ehrs-but-privacy-worries-remain/550774/

The Dangers of Today's EHRs

Other dangers include making patients vulnerable to hackers and system shutdowns, diverting the doctor's time and attention away from patients, impeding critical thinking and proper diagnoses, facilitating surveillance, and forcing the EHR, not the patient, to be the focus of the exam room visit—a violation of medical ethics.

The EHR is also coercive. It forces physicians and nurses to report on their patients, violating confidences and the patient-doctor relationship. It forces physicians and clinic staff to ask questions that have nothing to do with that visit. It forces physicians to follow treatment protocols determined by executives and officials far from the bedside or exam room, diverting the doctor's critical thinking skills, eyes and listening ears from patient faces, vocal inflections, and physical examinations as they click box after box after box in the EHR.

Consider the recent 27-page report called **"Death by a Thousand Clicks: Where Electronic Health Records Went Wrong,"** an extensive investigation of EHRs by *Fortune* and Kaiser Health News. Death and injury are known—from the EHR. Even the FDA has testified to these dangers.

Critical orders have not been transmitted. Diagnoses have been missed. Finding data among the various screens and drop-down menus is difficult. There are glitches galore, including records from one patient inserted into records from another patient, inaccurate medication lists, and critical information hidden in extensive (and meaningless) copy and paste notes.

This disaster for patient care is not surprising given that the mandate was premised on the promises of those who would most likely benefit from the $36 billion in federal grants and the five-year buy-it-or-be-penalized deadline imposed on medical practices and hospitals.

As a result of the rush to design and purchase, today's EHRs don't work for those forced to use them—EHR programming to follow the workflow of patient care was not part of

the mandate. Furthermore, patient-centric programming is inherently difficult because it can't be standardized and patients aren't widgets. Thus, EHRs hurt the most vulnerable of all, the patients and their families forced to deal with the resulting deaths, delays, medical errors, and injuries.

We call the mandated EHR a "government EHR." The government EHR is certified to do what the government wants it to do, such as tracking, data-sharing, and "population health," not what the patient and doctor need it to do. Unfortunately, earlier EHRs that once worked well for doctors and their patients have been jettisoned to avoid the federal penalties imposed for failing to buy and use the government EHR.

The government EHR, combined with the permissive HIPAA rule, has opened the exam room door, letting an untold number of third parties into confidential conversations and private lives—virtually, through public and private health information networks that share patient data nationwide as permitted by HIPAA, and physically, through the uninvited "scribes" now in exam rooms recording everything patients say to doctors.

This 690-page regulation does not remedy the intrusions and dangers patients now face. It may indeed worsen it. More money and staff diverted from patient care to follow the "no information blocking" rule, more opportunities to be penalized, more fear and less trust in the exam room, mandates to more completely violate patient confidentiality, more reasons for doctors and nurses to pay attention to the rules, not their patients, and more reasons for independent physicians to exit the practice of medicine and leave behind the patients who depend on them.

The government EHR is a travesty—mandated by Congress and funded by taxpayers, who have now been put in harm's way.

Furthermore, the government EHR has not cut costs or been the wonder-technology advertised pre-mandate by HIMSS, Rand Corporation, the Center for Information Technology Leadership (CITL) and others. Instead, direct and indirect costs have skyrocketed. These include purchasing, installing, training, maintaining, updating, securing, onboarding, new staff, and leasing, to name just a few.

Question:
Why was the initial comment period just 30 days? Only after protests was it extended another 30 days. Many comment periods are 90 days. How could HHS think the two most important people in the exam room would have time to respond: the patients and doctors whose lives, practices, ethics, treatment options, and trust may be impacted?

But even so, **what patient** is going to comb through 690 pages of regulatory text to try to figure out what to say to HHS to convince federal regulators to protect them when they are most vulnerable (sick and injured) and cannot protect themselves. And **how many physicians**, especially those in independent practice, already burdened by the

costs and time-consuming clicking of the government EHR, have time or energy to read this lengthy document to figure out how federal officials are planning to further impinge on their autonomy and infringe on the patient-doctor relationship, and then develop a cogent response to the threat?

Interoperability is not what the doctor ordered.

The government EHR, and each complex regulation issued to embed this intrusive command-and-control technology system deeper into the all-important practice of medicine will encourage fewer physicians to stay in practice and discourage many critically-thinking, highly-motivated candidates for medical school to choose another profession. This will leave fewer well-trained, highly-motivated physicians available to a population in which Medicare enrollment is growing at 10,000 American senior citizens every day. The impending physician shortage will not be helped, and could be hastened, by hunting for the "unicorn" called interoperability.
(https://www.forbes.com/sites/theapothecary/2014/09/03/health-data-interoperability-a-30-billion-unicorn-hunt/#2d3fd4415a9b)

The Right Solution Awaits
Why not look at the real problem, instead of layering more regulations onto the problem in hopes of fixing this faulty technology? The proposed fixes do not aim to fix the fundamental problems of the EHR, or the troubling use of them to violate patient rights and medical ethics. The real problem is the ubiquitous existence of poorly-planned, hastily-imposed government EHRs that were never built for patient care. This regulation prohibiting "information blocking," which not everyone agrees even exists, will not solve that problem.

The solution to today's technological disaster, which was foisted untried on doctors and their patients, is clear: **End the EHR mandate. Stop this costly and dangerous experiment on patients.**

HHS has a responsibility to do the right thing. HHS must tell Congress the truth. Congress may still think the EHR is technological wizardry, but we believe HHS knows EHRs are hurting patients and that the dreams of a safe, perfectly operating and flawlessly interoperable nationwide EHR system are not coming true anytime soon. We also believe HHS knows that HIPAA does not protect the privacy and consent rights of patients and that interoperability requirements will only facilitate even greater violations.

Some say the only solution to the mess created by the EHR mandate is to start all over again: ***"I used to think we could improve the electronic health record from within, but now I realize the only way to truly improve electronic health records is to start over,"*** said Andrew Hines, an engineer at Canvas Medical to Shawn Martin, AAFP senior vice president of advocacy, practice advancement and policy (AAFP Blog, May 2018). This is true.

What HHS Should Do

HHS should focus its efforts on restoring patient safety, confidentiality, trust, and the patient-centered practice of medicine. The sole purpose of the practice of medicine must continue to be the patient, who cannot heal, cure, or save him or herself. HHS should not continue to engage in these policies, protocols, and mandates that harm patients and demoralize doctors.

HHS should publicly acknowledge the dangerous failure of this poorly-planned EHR mandate and use its regulatory authority to restore privacy and consent rights rather than advance the further demise of the confidential patient-doctor relationship.

HHS should tell Congress the truth—publicly. Patients lives are at stake.

HHS should tell Congress the EHR mandate is hurting patients. HHS should advise Congress to end the mandate, eliminate the penalties, reverse HIPAA to protect patient consent rights, and let the free-market work to create computerized medical records that follow the flow of patient care, work for the doctors and nurses who depend on them to care for patients, prohibit outside control of private medical decisions, and improve the safety of patients in the hospital, not jeopardize their lives.

Yes, it will take courage. But how many American lives are HHS and Congress willing to lose before they admit that today's electronic health record (EHR) is a known safety hazard in every exam room and at the bedside of each hospitalized patient?

Therefore, we call on you, Secretary Azar, to withdraw this rule and inform Congress that the U.S. Department of Health and Human Services is not willing to advance a technology system that violates medical ethics, conducts exam room surveillance, destroys medical excellence, has already led to patient deaths, and is putting every patient in harm's way.

Please do not hesitate to contact our office if you have questions.

Sincerely,

Twila Brase, RN, PHN
President and Cofounder,
Author, award-winning book, *Big Brother in the Exam Room: The Dangerous Truth About Electronic Health Records*