June 16, 2025

RE: **Public Comment on CMS-0042-NC: Request for Information; Health Technology Ecosystem**

FROM: Twila Brase, RN, PHN, Co-founder and President

TO: Centers for Medicare & Medicaid Services, U.S. Dept. of Health and Human Services

Citizens' Council for Health Freedom appreciates this opportunity to respond to the RFI on the Information Health Technology Ecosystem. CCHF is a national non-profit organization with a mission to protect patient and doctor freedom, which includes protecting health care choices, individualized patient care, and the right to medical and genetic privacy.
We are patient-centered, privacy-focused, and free-market-driven.

Summary:
We will provide information regarding digital health products for Medicare beneficiaries, data interoperability, health technology infrastructure, certified EHR technology (CEHRT), and value-based care. We urge this administration (and the agencies involved) to prioritize patient privacy as well as patient consent for sharing, use, and storage of protected health information.

Digital Health Products for Senior Citizens:
Proponents of digital health products and applications on smartphones argue the potential to revolutionize access to personal wellness tools but rarely discuss the far graver potential to expand third-party data collection and use without patient knowledge or consent. Digital products increase the risk of data breaches, unauthorized access, and identity theft. These apps also often collect deeply sensitive information—such as a person's medical history, reproductive health data, mental health status, biometric data, or daily habits—and store it or share it with third parties, without the user's fully informed consent. Many health apps operate outside the protections of federal health privacy laws like HIPAA, meaning that once a user inputs their data, it can be sold, analyzed, or used for purposes far beyond health care, including targeted advertising, corporate profiling, or even law enforcement surveillance. **NOTE:** despite the statement above about HIPAA, as we describe elsewhere in this RFI, HIPAA is actually not protective of patient information because it is considered a permissive data sharing rule that allows for sharing of PHI without patient consent for a plethora of non-clinical purposes. HIPAA did not establish privacy rights, as alluded in the RFI.

We are concerned about the lack of informed consent. Many users agree to lengthy and complex terms of service just to use a phone application, without fully understanding what data is collected, how it's used, or with whom it is shared. Data may be shared with insurance companies, third-party analytics firms, advertisers, or other business associates without users realizing it. This undermines individual autonomy and the foundational right to control one's own protected health information.

The role of HHS and CMS in this landscape is critical. While innovation in digital health is not intrinsically bad, it must not come at the cost of privacy and patient rights. Lawmakers and regulators must modernize privacy laws to match today's technology, ensuring that digital health data, along with clinical health data, is protected by laws and regulations that actually affirm a patient's right to privacy. This includes requiring explicit and informed consent, restricting data sharing and secondary uses, and holding app developers, data clearinghouses, and data brokers accountable for violations.

Ultimately, protecting health data privacy is not just a technical issue—it's a civil/human rights issue. If more health decisions and records move to mobile platforms, governments must safeguard the constitutional and longstanding ethical right to patient privacy and ensure that individuals—not corporations or government entities—remain in control of personal health data.

> **REQUEST: – Prohibit collection, storage, and use of digital health data without the informed, written and specific consent of the individual.** Furthermore, protect the individual's/patient's right to privacy by prohibiting the conditioning of access to a digital health application based upon their consent and privacy choices.

Data Interoperability:
HIPAA permits unprecedented disclosure and use of private patient information *without* patient consent. Ironically, a lack of interoperability is perhaps the greatest protector of privacy rights in the current system. The permissive sharing of data is best described by one who really knows:

> "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)

Relatively little data is restricted for disclosure or use under HIPAA. According to a 2010 HHS HIPAA rule, 2.2 million entities are permitted to access patient data without patient consent if the holders of the data agree to share it. Or as Niall Brennan, former Chief Data Officer 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 ongoing use, analysis, and disclosure (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. For example, in 45 CFR 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.)

We find little about interoperability that protects patient privacy since by definition it seeks to share PHI more readily and broadly. While federal law still allows states to pass real privacy laws, as Minnesota did three decades ago—an example every other state should follow—most states and state legislators falsely believe HIPAA protects medical privacy.

> **TWO RELATED REQUESTS: – To end the deception that HIPAA protects privacy, require the Notice of Privacy Practices form to be renamed: "Notice of Disclosure Practices." Furthermore, require health care practitioners and facilities to clearly state in writing and orally that the patient is not required to sign the form.**
>
> Too many patients who choose not to sign the form as by law they are allowed to do, are DENIED access to care or forced to pay cash for care.

Health Technology Infrastructure:
Health technology infrastructure must have patient privacy and informed consent at its core. Informed consent means a process by which an individual receives information about what information may be collected, retention policies, use policies, and what decisions the individual can make about these policies. Most importantly, informed consent must include the option to refuse consent without repercussions such as being denied access to care or coverage.

A major component of health technology infrastructure, the **Unique Patient Identifier (UPI)** has the potential to decimate patient privacy. If implemented, this national patient ID will become a national tracking number used to link patient medical records together for outsider access without patient consent. This ID card would also be required for patient access to medical care (i.e. "no card, no care"). The UPI was first proposed in the 1993 Clinton Health Security Plan as part of a "Health Security Card" for the national health care system he proposed.

Although the Clinton legislation did not become law, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) mandated the creation of a UPI for all Americans and authorized broad sharing of patient information without patient consent. In 1998, Congressman Ron Paul stopped the development of the UPI by placing the following prohibition in the 1999 Appropriations bill:

> *None of the funds made available in this Act may be used to promulgate or adopt any final standard under section 1173(b) of the Social Security Act (42 U.S.C. 1320d–2(b)) providing for, or providing for the assignment of, a unique health identifier for an individual (except in an individual's capacity as an employer or a health care provider), until legislation is enacted specifically approving the standard.*

This prohibition was added annually to the Labor-HHS appropriations bill. However, once Congressman Paul left office in 2013, proponents began to push Congress to allow the UPI to be developed. For example, in 2017, although the prohibition remained, the Appropriations Act of 2017 bill authorized HHS to examine "the issues around patient matching" and encouraged the National Coordinator for Health Information Technology and CMS *"to provide technical assistance to private-sector led initiatives to develop a coordinated national strategy that will promote patient safety by accurately identifying patients to their health information."*

A UPI would create a national patient identification number for every man, woman, and child in America. This unconstitutional federal number would be used to track patients, create a lifelong, fully linked, cradle-to-grave medical record, conduct research using patient data without consent (as permitted by the permissive HIPAA data-sharing rule and the Federal Common Rule), and become the only way to access medical care in America.
A national patient ID will pave the way to socialized medicine and a fully linked national medical records system. It will lead to government coercion, control, and interference in private medical decisions.

> **REQUEST: End federal attempts to create a UPI / National Patient Identifier.**
> Additionally, we urge you to cease any work with private partners or contractors who are attempting to create a backdoor UPI or engaged in patient matching without the informed consent of the patient. This includes any attempt to use the controversial and unconstitutional REAL ID – Federal ID – as a UPI.

Certified Electronic Health Record Technology (CEHRT):
Unfortunately, the unfunded EHR mandate, which mandates doctors and facilities use a *government-certified* EHR—combined with the permissive HIPAA data-sharing rule, and with the unethical "meaningful use" regulations—has eliminated patient privacy rights for most Americans, allowing their data to be shared broadly without their consent. Only patients who pay cash and 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.

Other dangers of the EHR include making patients vulnerable to hackers and health system shutdowns. Witness the frequent news reports about ransomware attacks. Importantly, today's government-certified EHR **diverts 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.

> "For some physicians, 90% of their eight-hour shifts are spent on EHRs." per Becker's Clinical Leadership (September 13, 2024). Nurses spend up to 41% of the workdays in EHRs.

The EHR is also coercive. It forces:

- physicians and nurses to report on their patients, violating confidences and the patient-doctor relationship.
- physicians and clinic staff to ask intrusive questions that have nothing to do with that visit.
- physicians to follow treatment protocols determined by executives, administrators, and officials far from the bedside or exam room rather than employ critical thinking skills.
- doctors to avert their 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.

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 purchase, install and use the government EHR "meaningfully."

The government EHR, in combination with the permissive HIPAA rule, has opened the exam room door, violating patient rights and letting untold number of third parties into private lives and confidential conversations—virtually, through public and private HIEs, including the eHealthExchange, which digitally share patient data nationwide as permitted by HIPAA, and physically, through the uninvited physical and virtual "scribes" recording every word patients say.

> **REQUEST: End the EHR mandate and rescind useless quality metrics and MU regulations.** Stop this costly and dangerous system that is designed for data collection, surveillance (of both patients and doctors), and third-party control instead of patient care and accurate record keeping.

Value Based Care (VBC):
Some look at value-based care as the future of treatment. However, the proposed benefits of value-based care are outweighed by the significant disadvantages. A *Forbes* article published April 12,

2022, states **"...value-based care will be the latest strategy we undertake to erode the most precious asset we have in the American healthcare system: the trust of the people we serve."**

We have six primary concerns with any advancement of VBC:

1) **No uniform definition of 'value'**. There is no good way or agreed upon way to answer the questions of "what is value" or "who determines value," nor does the industry agree upon a definition of value. A patient, doctor, clinic/hospital, administrator, insurer, public health official, etc. will each have their own definition of value.

2) **Denial of access to second opinions and specialty care.** The equations that define value under value-based care may reduce the patient's access to a second opinion. This is especially apparent through denial of access to specialist care. Under fee-for-service care, referrals to specialists are commonplace, however under value-based care, referrals often only happen when a patient needs a procedure a generalist physician is unable to do themselves.

3) **Patients dismissed prematurely from hospitals**. Because value-based care is always seeking to lower the cost of treatment, patients are often sent home from hospitals before they are ready. Networks look to lower the number of days patients spend in a hospital regardless of the need a patient may have.

4) **Limited treatment choice for patients**. Value-based networks often prioritize the hospitals they contract with based on cost instead of quality. However, this prioritization limits the treatment choices available for patients, especially when it comes to specialized care. As well as access to drugs, since networks tend to only cover drugs with significant evidence base, or non-branded generic drugs, or older drugs with a lower cost. This harms patient access to lifesaving, new, and innovative treatment.

5) **Prioritizes money over quality of care**. Value-based care is primarily concerned with cost of treatment over the needs of patients. This increases risk to patients who may not receive effective care or the treatment they need in a timely manner.

6) **Increases data collection of patients and use of PHI**. VBC models inherently rely on data collection and analysis of medical, financial, and personal information of patients and health care practitioners. This is done without the consent of the individual(s) and often without their knowledge that it is even occurring.

REQUEST: End the value-based payment structure. Instead pursue policies that returns the power of the purse to patients who can then make their own determinations of value and quality – and they will spend their resources accordingly.

The current Health Technology Ecosystem is based on unconstitutional laws and rules, including HIPAA, the HITECH Act's EHR mandate, and the Affordable Care Act. Requested rescissions will restore patient rights and patient privacy rights.

Sincerely,

Twila Brase, RN, PHN
Co-founder and President