May 17, 2019

Donald Rucker, MD
National Coordinator for
Health Information Technology
U.S. Department of
Health and Human Services
330 C Street, SW
Washington, DC 20201

Honorable Seema Verma
Administrator Centers for
Medicare and Medicaid
U.S. Department of
Health and Human Services
200 Independence Avenue, SW
Washington, DC 20201

Dear Dr. Rucker and Administrator Verma:

Thank you for this opportunity to provide public comments on the proposed rules listed in the Federal Register March 4, 2019:

> CMS-9115-P, "Medicare and Medicaid Programs; Patient Protection and Affordable Care Act; Interoperability and Patient Access for Medicare Advantage Organization and Medicaid Managed Care Plans, State Medicaid Agencies, CHIP Agencies and CHIP Managed Care Entities, Issuers of Qualified Health Plans in the Federally-Facilitated Exchanges and Health Care Providers"
>
> and
>
> RIN 0955-AA01 "21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program"

These rules affect a broad spectrum of important items. Our comments will specifically address the area of patient identification, which continues to be a deterrent for ease of interoperability and results in significant increased cost in the delivery of healthcare at all junctures.

Many of us, serving in a variety of roles across the healthcare industry, believe that the ability to uniquely identify a patient at the point of care and in support of the accurate exchange of patient care information, should be the very core foundation of healthcare information. In fact, to do less, is unacceptable.

For the sake of brevity, suffice it to say that we acknowledge the significant work that HHS, ONC and many professional organizations have done over several decades in describing the need and evaluating potential solutions for uniquely, securely, and privately identifying patients across the continuum of care. And yet the problem persists, and we have failed to execute a universal solution.

In proposing this rule, you have listed patient identification as the first entry under “Challenges and Barriers to Interoperability”. These barriers were stakeholder feedback at the request of HHS, and as such, we recognize again the value and importance of finding solutions. You state “we seek comment for future consideration on ways for ONC and CMS to continue to facilitate private sector efforts on a workable and scalable patient matching strategy," and solicit novel potential solutions.

In proposing this rule, you have listed patient identification as the first entry under “Challenges and Barriers to Interoperability”. These barriers were stakeholder feedback at the request of HHS, and as such, we recognize again the value and importance of finding solutions. You state “we seek comment for future consideration on ways for ONC and CMS to continue to facilitate private sector efforts on a workable and scalable patient matching strategy," and solicit novel potential solutions.

We think that blockchain derived self-sovereignty is new and fertile solution space for resolving patient identity across healthcare. Self-sovereign identity is being increasingly explored in the context of healthcare[1,2].

In the last decade, much has evolved in our collective understanding of the problems of data exchange. At the same time, there have been significant advancements in technology, including the ubiquitous use of personal computing devices. There is a growing appreciation for the value of empowering the patient to control their healthcare journey.

With the increasing ubiquity of smartphones, it is becoming more practical for patients to hold and manage significant computing resources. These resources can be deployed so that patients can take a more active role in the management of their health identity and better solve the vexing problem of matching identities across healthcare.

Self-Sovereign Health Identity is a specialized form of self-sovereign identity that equips people to identify their health information distributed across healthcare. Self-Sovereign Health Identity is not a new or alternative patient ID; rather it is the correlation of the patient IDs that exist in the information systems across healthcare held by and under the sovereignty of, the person. Importantly, it is not a single number for identifying the patient such as the never implemented Universal Health Identifier authorized by HIPAA. It is not a single number that can unlock a patient’s entire health history which was the primary objection to the implementation of the Universal Health Identifier. And, it’s adoption does not require modifications to existing information systems.

An important criterion that the 21st Century Cures Act imposes on APIs subject to the proposed rules is that “no special effort is required”. We think that patient ID proofing as defined by

1 https://github.com/WebOfTrustInfo/rwot8-barcelona/blob/master/draft-documents/how-ssi-will-survive-capitalis-m.md#abstract

2 https://www.ibm.com/blogs/blockchain/2018/06/self-sovereign-identity-unraveling-the-terminology/

HIMSS[3] requires special effort, and, to the extent that the APIs are subject to the proposed rules they will require patient ID proofing, they may not meet this criterion. Instead, we think Self-Sovereign Health Identity should be considered as a better approach.

We have prepared a brief conceptual description of how Self-Sovereign Health Identity could work to solve this pervasive problem in healthcare: https://youtu.be/Nooq8k-s2iw

A technology concept description follows this letter.

Thank you for the opportunity to provide commentary to these important rules. Please feel free to contact Calvin Wiese (407)810-3944, calvin.wiese@kalibrateblockchain.io, https://www.linkedin.com/in/calvin-wiese-451b61b if you have questions or would like additional information.

With Regards,

Calvin Wiese President and CEO
Kalibrate Blockchain

[3] https://www.himss.org/sites/himssorg/files/Patient_Portal_Identity_Proofing_and_Authentication_Final.pdf

Self-Sovereign Health Identity *Technology Concept*

Self-Sovereign Health Identity equips people to identify their health information distributed across healthcare.

With Self-Sovereign Health Identity, core functions commonly performed in health information are shifted to patients where they are more suited for performance. Powerful, personal computing devices are now commonplace through which sophisticated information management functions can be personally performed at points of care.

Self-Sovereign Health Identity is an index of the person's biometrics and the patient IDs used in each information system distributed across healthcare. Self-Sovereign Health Identity is not a new or alternative patient ID; rather it is the correlation of the patient IDs that exist in the information systems across healthcare.

All aspects of the Self-Sovereign Health Identity are subject to the will of the person. Self-Sovereign Health Identity is self-hosted; it can be hosted on the person's smartphone, it can be hosted by the person's own server, it can be hosted by any third-party hosting provider. It can be un-hosted. All at the will of person.

The degree of protection and security of the Self-Sovereign Health Identity is subject to the will of the person; any degree the person chooses can be employed.

With Self-Sovereign Health Identity persons can:

- Identify themselves at points of care with the patient ID that the point of care information system knows them by.
- Cross-reference their patient IDs in health transactions using standardized PIX transactions.
- Enable any app to identify their information in other health information systems with no special effort.

- Points of care can biometrically validate the identity of patients.

As such, it can be used without modification of the existing information system distributed across healthcare. Existing information systems distributed across healthcare can increase the usefulness of Self-Sovereign Health Identity by making low-complexity modifications.

Self-Sovereign Health Identity has inherent advantages over existing provider managed identities.:

- 1:1 patient ID matching reduces the opportunity for matching errors.
- Third-party trust relationships are not required.
- Cross-referenced transactions are not subject to HIPAA.

Blockchain is especially well suited for Self-Sovereign Health Identity. It's robust scalability, affinity for self-sovereignty and distributed autonomous network derivable superproperties make it an attractive technology for instantiating Self-Sovereign Health Identity.