Richard Gibson, MD, PhD
President and CEO
The Health Record Banking Alliance
PO Box 91325
Portland OR 97291
(503) 313-7837
www.healthbanking.org

4 September 2018

SUBMITTED ELECTRONICALLY VIA REGULATIONS.GOV

Ms. Seema Verma
Administrator
Centers for Medicare & Medicaid Services
U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201

RE: CMS 1693-P: Medicare Program; Revisions to Payment Policies Under the Physician Fee Schedule and Other Revisions to Part B for CY 2019; Medicare Shared Savings Program Requirements; Quality Payment Program; and Medicaid Promoting Interoperability Program

Dear Administrator Verma:

I am writing on behalf of the Health Record Banking Alliance[1] (HRBA), which promotes technology to enable consumer-owned and controlled longitudinal, lifetime, aggregated, computable, easily used, digital health records stored securely in consumers' accounts in private sector repositories. HRBA is committed to three key principles:

1. Each patient's records should be functionally stored in one place (but not all patient records in the same place);
2. Each patient should control access to his/her own medical records; and
3. Medical records should be stored under patient control by a trusted organization.

[1] The Health Record Banking Alliance is recognized as a business league by the Internal Revenue Service under Section 501(c)(6) of the Internal Revenue Code.

Regulatory Context

CMS should consider these comments in the context of comments HRBA filed earlier this year with the Office of the National Coordinator for Health Information Technology (ONC). Those comments respond to ONC's proposed implementation of the Trusted Exchange Framework and Common Agreement (TEFCA). They point out that both HITECH and the Cures Act require ONC to promulgate a national digital health data exchange standard. The Cures Act amends HITECH to reinforce Congress's intent that ONC must fulfill this mandate. The Cures Act adds detailed specifications of features and functions — engineering design requirements — that must be part of the exchange standard ONC proposes, adopts, and implements.

Despite these statutory requirements, ONC has neither implemented nor proposed in TEFCA a national digital health information exchange standard. HRBA addressed those issues in its TEFCA comments, submitted 20 February 2018. HRBA's purpose in these physician payment reform comments, rather, is to point out the practical regulatory consequences created by the absence of a national health data exchange standard. Such a standard would publish annually, eliminate options, specify particular profiles and implementation guides, and allow 24x7x365 online testing by developers, vendors, payers, and providers to ensure compliance.

The absence of a national digital health data exchange standard is a barrier to routine, secure, affordable, convenient exchange of health records. Its impact is nationwide. It creates unnecessary, otherwise intractable barriers to health information exchange. Patients, clinicians, medical institutions, and regulators (among others) are denied the benefits of digital information exchange with the ease and functionality that Congress has long sought.

In particular for purposes of CMS's proposed rule here, these barriers complicate and frustrate CMS's attempts to meet its statutory obligations and to design efficient regulations that comply with HITECH and the Cures Act. CMS, like ONC, must design regulations to attempt working around the fact that health records by and large remain siloed rather than exchangeable. CMS's and ONC's definitions of "interoperability" and "interoperable" thus continue to be artifices. That is, they permit clinical data systems to be certified as "interoperable" for purposes of regulatory compliance even though those systems, and the regulatory framework itself, fail to meet the fundamental requisites of HITECH and the Cures Act regarding digital data exchange.

In these comments, HRBA takes these regulatory deficiencies as a given condition. HRBA recognizes that CMS's regulatory proposals must perforce be based on the fiction that ONC's existing and proposed regulatory framework for promoting "interoperability" is consistent with applicable statutes (HITECH and Cures) even though it is not. Thus HRBA's approach is to identify inconsistencies and discrepancies in the physician payment reform proposal that CMS must do its best to address, even though none of these proposed regulations can compensate for the lack of a data exchange standard.

Therefore, nothing here should be interpreted as HRBA's retracting or otherwise departing from its comments on TEFCA. In HRBA's view, ONC's TEFCA proposal remains unworkable as an

engineering systems design and as a regulatory scheme to implement data exchange under HITECH and Cures. Those deficiencies have a direct, negative impact on the regulatory options open to CMS as it seeks to fulfill its regulatory responsibilities. So HRBA's task in these comments is to address as practical matters the operational barriers CMS is facing. CMS must deal with Certified Electronic Health Record Technology that, in fact, should not be certified under HITECH and Cures because it does not meet the *statutory* requisites for digital health data exchange.

Our comments center on the assertion that the best clinical, financial, and satisfaction outcomes for patients arise from full patient engagement in their care. Patients with a complete, comprehensive, lifetime, unified health record that they can share with any physician or family caregiver are able to interact with providers more confidently and better understand their conditions and their care. Further, personal health records are the ideal repository for a patient's genomic data and patient-generated health data from mobile phone apps and personal devices. We believe that an ecosystem will develop where patients and their caregivers will benefit from mobile phone app advice based on a comprehensive store of patients' data. To achieve that vision, some adjustments need to be made in electronic health record (EHR) patient portals, the use of C-CDA document templates, and application programming interfaces (APIs). In the following pages, we address the rule changes proposed by CMS 1693-P in the areas pertinent to personal health records and patient access to data.

Individual Sections and Specific Recommendations

III.E.4.a. Proposed Change to Objective 6 (Coordination of Care Through Patient Engagement)
Therefore, we propose to amend § 495.24(d)(6)(i) such that the thresholds for Measure 1 (View, Download, or Transmit) and Measure 2 (Secure Electronic Messaging) of Meaningful Use Stage 3 EP Objective 6 (Coordination of care through patient engagement) would remain 5 percent for 2019 and subsequent years.

We agree with keeping the thresholds for View, Download, and Transmit and Secure Electronic Messaging at 5 percent for 2019 and retaining the HIT certification program.

Patient self-efficacy is the key to better health and more efficient use of health services. Providers, payers and communities that serve patients will be increasingly dependent on information outside of their own domains. Patients can act as intermediaries of information and exchange. The ecosystem to achieve this will depend on standards that are universally required for all EHR vendors and providers.

III.H.3.h.(5)(f)(iv)(B) Proposed Removal of the Patient-Generated Health Data Measure

We are proposing to remove the Patient-Generated Health Data (PGHD) measure to reduce complexity and focus on the goal of using advanced EHR technology and functionalities to advance interoperability and health information exchange.

As finalized in the 2015 EHR Incentive Programs final rule at 80 FR 62851, the measure is not fully health IT based as we did not specify the manner in which health care providers would incorporate the data received.

We disagree with this proposal. PGHD must remain a required measure.

There exist apps today that permit patients to generate health data and share them using standard formats. Patient-Generated Advance Care Plans (traditionally called "advance directives") use an HL7 standard that is consistent with the Meaningful Use C-CDA standard, and there are companies that can generate and share Personal Advance Care Plans documents with providers using the same transport mechanisms that support sharing any other standard C-CDA document. There are applications that allow a user to take the C-CDA document they have downloaded from their patient portal or received via Direct secure messaging. Patients can then annotate it with feedback using standard C-CDA Clinical Notes templates that carry proper Data Provenance stating that the information was authored by the patient. The annotations provide data quality improvements, care planning information, and essential outcome information that can be collected only from the patient.

The problem is that many EHRs are not taking action to implement workflows for accepting PGHD. This is a form of information blocking. The measure is needed to monitor progress on a very real and present opportunity to engage patients in the co-creation of their health records, to help reduce the cost of unwanted care, and to improve the accuracy and completeness of health records. The technology exists to observe and measure rapid increases in the amount of PGHD being accepted into EHR systems It is critical to track if progress is being made or if PGHD is being blocked from inclusion.

The technology exists and there are HIT vendors supporting consumers generating PGHD from wearables and mobile phone apps. More PGHD, if done correctly, may lead to reductions in physician burden. Many patients can do much of data entry required to fill out their Family History, Social History, Past Medical History, and the like, instead of handwriting the information on clipboards in each provider's office. Harvesting and re-using PGHD from all those forms that patients fill out today could become a tremendous time-saver for physicians. For that reason alone, the measure should not be removed.

III.H.3.h.(5)(f)(iv)(D) Proposed Removal of the Secure Messaging Measure

We are proposing to remove the Secure Messaging measure as it has proven burdensome to MIPS eligible clinicians in ways that were unintended and detracts from MIPS eligible clinicians' progress on current program priorities.

As outlined above, we believe that the Secure Messaging measure does not align with the current emphasis of the Promoting Interoperability performance category to increase interoperability or reduce burden for MIPS eligible clinicians. In addition, we believe there is burden associated with tracking secure messages, including the unintended consequences of workflows designed for the measure rather than for clinical and administrative effectiveness.

We disagree with this proposal. Secure Messaging must remain a required measure.

The free flow of health information depends to a great degree on consumers and patients who trust that their protected health information can be transmitted and received in ways that protect their privacy. Absent that trust, patients will withhold information and/or not participate in the exchange of protected health information that drives new business relationships, more efficient care, and engaged, cost-conscious patients. Assertions that secure messaging is "burdensome" are severely out of date. Demonstrated successfully by DirectTrust and the August 2018 ONC interoperability meeting, there is no question that secure messaging can be used to enable integration of data within the broader workflows of the provider community.

Secure messaging and its role in opioid addiction prevention: Patient education and communication is fundamental to encouraging the appropriate use of pain management medications. Secure messaging ensures that patients can communicate confidentially with all of the community services that help them. If secure messaging is removed and not encouraged, patients, providers, and community services will be loath to communicate electronically, keeping all members isolated and in the dark.

III.H.3.h.(5)(f)(iv)(E) Proposed Removal of the View, Download or Transmit Measure

We are proposing to remove the View, Download or Transmit measure as it has proven burdensome to MIPS eligible clinicians in ways that were unintended and detracts from their progress on current program priorities.

Stakeholders have indicated that successful submission of the measure is reliant upon the patient, who may face barriers to access which are outside a clinician's control.

We vigorously object to this proposal.

EHR companies have spent substantial resources making the patient's EHR data available to the patient. Many patients use EHR-connected patient portals to request refills, schedule appointments, and send messages to their care team. Patients already have logins and passwords to patient portals and it is convenient for them to download their data from within the portal.

Instead of removing the requirement to provide View, Download, and Transmit capabilities, CMS should instead make it easier for patients to download their data into a personal health record by requiring portals to allow patients to enter the electronic address (URL) of their PHR. Further, EHR-connected portals should be required to allow patients to request that any new data that the EHR receives be automatically downloaded to the patient's PHR. This way, the patient builds a comprehensive, longitudinal, unified health record automatically after every provider encounter. View, Download, and Transmit already exists in all CEHRT and adding PHR address entry and automatic updating are very little burden for EHR vendors and no burden at all to providers, because both functions are automatically managed by software.

IV.A. Request for Information on Promoting Interoperability and Electronic Healthcare Information Exchange Through Possible Revisions to the CMS Patient Health and Safety Requirements for Hospitals and Other Medicare- and Medicaid-Participating Providers and Suppliers

- If CMS were to propose a new CoP/ CfC/RfP standard to require electronic exchange of medically necessary information, would this help to reduce information blocking as defined in section 4004 of the 21st Century Cures Act?

Unquestionably yes. There are specific, modest requirement changes that could help reduce information blocking. Very little new functionality is required to make 2015 Edition CEHRT patient data more available to patients and their designated apps and to do so without any significant labor on the part of providers. CMS should work with ONC to ensure that future editions of CEHRT require that EHR patient portals allow patients to enter their secure Direct messaging address or the URL of their approved third-party app to receive their patient data and to automatically receive any additional data whenever the provider's EHR receives new data. Also, CMS should work with ONC to ensure that future versions of U.S. Core Data for Interoperability (USCDI) capture all of the patient's data at a given facility, as required by HIPAA, using all 12 of the standard C-CDA document templates, which can be cross-mapped to FHIR resources, which use the required Application Programming Interfaces (APIs).

National and international standards exist for transmitting nearly all patients' data in EHRs, namely the 12 C-CDA document templates and the equivalent FHIR resources for APIs. These standards are listed in ONC's Interoperability Standards Advisory. But these consensus standards do not yet adequately support interoperability in clinical practice because they

contain too many optional fields for important data and there is not an easy way for a provider or EHR vendor to test their ability to send or receive fully conformant C-CDA documents. CMS and ONC need to establish which version and profile is expected each year for a given standard. All providers receiving CMS funding should be required to use that standard, version, and profile for that year, and expect that there will be modest updates in the versions and profiles each successive year. Self-service testing, available 7x24x365, is crucial for developers, payers, and providers to be sure that their messages are compliant with current standards. If EHR vendors are given adequate notice of next year's changes, and providers, payers, and vendors expect progressive, incremental annual updates, then the burden on providers would be reasonable and more data can flow to patients and other providers.

- Should CMS propose new CoPs/ CfCs/RfPs for hospitals and other participating providers and suppliers to ensure a patient's or resident's (or his or her caregiver's or representative's) right and ability to electronically access his or her health information without undue burden? Would existing portals or other electronic means currently in use by many hospitals satisfy such a requirement regarding patient/resident access as well as interoperability?

Yes. Until secure and affordable FHIR APIs are commonplace in the consumer marketplace, patients and caregivers continue to need access to patient data via EHR-connected patient portals. As noted above, modest changes to patient portals will allow patients and their caregivers to sign up once to have their data flow automatically to a third party app of their choosing (a PHR or equivalent) after the first and every subsequent visit. Further, the patient or caregiver can point the portals of all of the patient's providers to the same PHR and collect their EHR, genomic, and patient-generated data in one place as Administrator Verma described at the Blue Button 2.0 Developer Conference in Washington DC on 13 August 2018.

- Are new or revised CMS CoPs/CfCs/ RfPs for interoperability and electronic exchange of health information necessary to ensure patients/residents and their treating providers routinely receive relevant electronic health information from hospitals on a timely basis or will this be achieved in the next few years through existing Medicare and Medicaid policies, the implementing regulations related to the privacy and security standards of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Pub. L. 104–91), and implementation of relevant policies in the 21st Century Cures Act?

Yes, new conditions are needed. It is crucial for CMS to gradually and predictably require that more and more of the patient's data within EHRs be mapped to one of the 12 C-CDA document templates as well as to the appropriate FHIR resources, so that they can be transported to the patient's chosen third-party app "without special effort." Current applications, such as Apple Health, have demonstrated how easy it is for patients to receive their data from their providers' EHRs and store it all in one place, regardless how many providers and different EHRs are involved. But the Apple Health FHIR API is accessing only a very small subset of all the useful patient data in the EHR (e.g., the problem list, medication

list, allergy list, procedure list, vital signs, lab results, immunization list, and smoking status). This is a great start, but gradually and predictably (so that EHR vendors have sufficient time to enhance their FHIR APIs) CMS needs to require more and more of the patient's clinical data in the EHR to be accessible by View, Download, and Transmit C-CDA documents and by FHIR APIs. The most important additional data element is Clinical Notes (e.g., history and physicals, consultation notes, operative notes, procedure notes, pathology notes, diagnostic imaging interpretations, discharge summaries, office visit notes, etc.). To its credit, ONC has suggested that Clinical Notes be included in the 2018 version of USCDI along with Data Provenance.

- What would be a reasonable implementation timeframe for compliance with new or revised CMS CoPs/CfCs/RfPs for interoperability and electronic exchange of health information if CMS were to propose and finalize such requirements? Should these requirements have delayed implementation dates for specific participating providers and suppliers, or types of participating providers and suppliers (for example, participating providers and suppliers that are not eligible for the Medicare and Medicaid EHR Incentive Programs)?

As ONC has suggested with its proposed annually updated USCDI, it is reasonable for CMS to gradually and predictably require that more and more of the patient's data in EHRs be made available via View, Download, and Transmit C-CDA documents and via FHIR APIs, both of which are functional in 2015 CEHRT. Allow EHR vendors a year to make annual modest updates in their EHR patient portals and FHIR APIs and allow providers a year after that to implement that upgraded version. We do not expect EHR vendors and providers to suffer massive new versions each year. In the same way that Microsoft Windows, Apple MacOS, Android, and Apple iOS make regular, small incremental updates to computer and mobile phone operating systems, EHR vendors can make regular, small incremental updates in the data elements sent to patients and their caregivers. The benefit accrues year after year as more and more of patients' EHR data are made available to their chosen repositories or apps.

- Are there any other operational or legal considerations (for example, implementing regulations related to the HIPAA privacy and security standards), obstacles, or barriers that hospitals and other providers and suppliers would face in implementing changes to meet new or revised interoperability and health information exchange requirements under new or revised CMS CoPs/CfCs/RfPs if they are proposed and finalized in the future?

Yes. Patients need to be clearly, securely, and unambiguously identified to avoid the need for patient matching, which has been widely criticized as too risky for patient care. NIST Publication 800-63-3 has specified the criteria for secure patient identification. DirectTrust, its member companies, and multiple federal health agencies are all using versions of this standard to identify providers, payers, and patients. At scale and for a few dollars per patient, each patient can have an unambiguous, secure, replaceable (like a credit card that becomes compromised) digital identity that they can use for healthcare and all their other internet transactions.

Conclusion

In summary, it is important to maintain the momentum of engaging patients in their care by continuing to use existing information technology standards while implementing and learning from new information exchange standards. It is the nature of information technology to have two or three generations of standards in use at any given time. Given time, new standards will be optimized and adopted into common use and the older standards will fall into disuse. The Health Record Banking Alliance strongly recommends that CMS continue to measure View, Download, and Transmit, Secure Messaging, and Patient-Generated Health Data. CMS should continue to support the widely implemented C-CDA standard while eliminating optionality and calling for continuously-available online testing. Transmission and content standards need to be updated annually. Patients need to have a secure, unambiguous digital identity. These steps will assure a robust, sustainable ecosystem of personal health data where patients and families will have access to the information they need to use healthcare resources wisely.

Respectfully submitted,
The Health Record Banking Alliance

By

Richard Gibson MD, PhD
President and Chief Executive Officer
richard.gibson@healthbanking.org