October 17, 2018

Don Rucker, M.D.
National Coordinator for Health Information Technology
U.S. Department of Health and Human Services
200 Independence Avenue, SW
Washington, DC 20201

Dear Dr. Rucker:

The College of Healthcare Information Management Executives (CHIME) and the Association for Executives in Healthcare Information Technology (AEHIT) are pleased to submit comments on the request for information (RFI) published in the *Federal Register* on August 24th on the Electronic Health Record (EHR) Reporting Program established under Section 4002 of the 21st Century Cures Act.

CHIME is an executive organization dedicated to serving chief information officers (CIOs), chief medical information officers (CMIOs), chief nursing information officers (CNIOs) and other senior healthcare IT leaders. With more than 2,700 members, CHIME provides a highly interactive, trusted environment enabling senior professional and industry leaders to collaborate; exchange best practices; address professional development needs; and advocate the effective use of technology to improve the health and healthcare in the communities they serve.

AEHIT was launched in 2014 under CHIME to provide an education and networking platform to healthcare's senior IT technology leaders. Together, our members are responsible for the selection and implementation of clinical and business technology systems that are facilitating healthcare transformation. They are also among the nation's foremost health IT experts on a range of issues, including telehealth, and many of our members' organizations treat patients in underserved areas. We welcome the opportunity to share our insights with the Commission.

I. Key Recommendations

Our recommendations are outlined in greater detail in the body of our letter, however, they can be summarized as:

1. **We advise against ONC establishing a complex rating methodology for scoring vendors. Instead, we recommend ONC work collaboratively with private sector benchmarking entities and using stakeholder feedback to identify a set of metrics like the 10-20 pieces of information needed by providers for contracting / purchasing (i.e. estimated costs, security and application programming interfaces (APIs)).**

2. **ONC should review the Department of Defense's (DOD) data dictionary and determine whether this could be recycled for the purposes of reporting Medicare quality data and whether this could be leveraged as a best practice.**
3. **ONC should consider establishing benchmarks by which to monitor interoperability progress among vendors.**
4. **Patients need better education on the risks of using APIs and ONC should partner with their federal partners and stakeholders on this.**

II. Background

Section 4002(a) creates Public Health Service Act (PHSA) section 3001(c)(5)(D) and instructs the U.S. Department of Health & Human Services (HHS) to ''require, as a condition of certification and maintenance of certification'' that health IT developers satisfy certain requirements, including submitting certain reporting criteria. HHS is required to develop an ''Electronic Health Record Reporting Program'' (EHR Reporting Program). The Cures Act requires the reporting criteria to address the following five categories:1) security; 2) interoperability; 3) usability and user-centered design; 4) conformance to certification testing; and 5) other categories, as appropriate to measure the performance of certified EHR technology.

As a preliminary matter, while we appreciate that ONC and Congress have recognized the need for more transparency for EHR end-users, we nonetheless feel what is being asked is too onerous for the providers as purchasers of these systems even if it helps them evaluate products. Vendors should be developing products which are inherently more useable and interoperable and the burden for ensuring this occurs should fall less on providers and occur prior to these systems even reaching the hands of clinicians. As ONC monitors vendors' interoperability capabilities they should consider establishing benchmarks by which to monitor progress. For example, goals could be set that calls for having 70 percent all EHR data to be exchanged / consumed (structured and unstructured), with 80 percent of all EHRs being able to do this nationally, and with more than 90 percent having an electronic master patient index (EMPI) matching without intervention. Further stakeholder input could be sought in arriving at these metrics.

Finally, as we have previously communicated, our members remain very concerned with privacy and security of patient information. Cybersecurity threats and emerging challenges associated with the use of APIs pose real concerns and our members continue to worry about the release of data to third parties at the request of patients without their clear understanding of how their data could be used.

III. Cross-Cutting Topics

Contained in the RFI are dozens of questions posed by ONC to solicit feedback on this new reporting program. CHIME responses to several of these questions are detailed below.

Q. What, if any, types of information reported by providers as part of their participation in HHS programs would be useful for the EHR Reporting Program (e.g., to inform health IT acquisition, upgrade, or customization decisions)?

A. Our members have identified several pieces of information that could be added to the reporting program to make the purchase and review of vendors more comprehensive and valuable:

a. Product Information:

i. Estimated costs, though we recognize gathering this data could be challenging and more stakeholder input may be warranted to determine how this could best be achieved. Examples of data which our members would find helpful include:

i. Base install product estimated cost (production system hardware, software and services)
ii. Estimated cost (hardware, software, and services) for redundant (or highly redundant) system – including definitions of what they believe redundant is.
iii. Estimated cost (hardware, software, and services) for test system
iv. Estimated cost (hardware, software, and services) for training system

ii. Average number of upgrades provided yearly – do these upgrades include changes from regulatory agencies? How quickly do changes in regulatory agencies become available in the base product?

iii. Are upgrades included in base install product cost? If not, provide estimated costs for upgrades. Are upgrades required?

iv. Average time from security patch identification to implementation?

v. Are there additional estimated costs to implement security patches?

vi. Average time for customer optimization request to incorporation into the product; it would also be helpful if customers understood how these optimizations were prioritized).

b. Implementation: Vendors need to be transparent about what type of implementation is needed otherwise this can impact billing, estimated costs to support and usability. As one member described it when she, "looks at vendors they need transparency about what interfaces are included in a system and the cost of what is an add-on. Maybe the system is capable of connecting to this exchange or that but is it an add-on? Is there a licensed cost and is there a vendor fed to implement?"

1. **Estimated costs:** Cost was raised time and time again by our members as a key piece of information that is needed when reviewing products. Again, recognizing gathering this data could be challenging, they are interested most in knowing what the base price of implementation is and what the additional costs would be. Examples include:
   a. Estimated implementation (service costs) for base installation;
   b. Estimated training (service costs) for base installation;
   c. Estimated customization costs (including licenses and service implementation costs); and

d. Estimated costs for interfaces (licenses and services costs) with other data exchanges.

2. **Timelines**
   a. Currently there is not enough time between the publishing of the new standard and when it needs to go into effect, thus more information is needed from vendors on their average turnaround time from when a regulatory change is enacted to having software that can be installed and implemented.
   b. The ability to meaningfully share data between providers requires the vendors and providers to work together on use cases (workflows), a full vendor software development lifecycle and adequate time for hospitals and providers to implement. Projects of this magnitude should really have 18-24 months between regulation publishing and regulatory effective date.

c. **Ongoing support:** Very few systems have best practices for downtime. As one member noted, "Not a single vendor out there that can provide good downtime (procedures or alternatives); especially for doctors if they are cloud-based – what is vendor philosophy on downtime?" Another reported they, "have seen too many contracts where if you want any redundancy or disaster recovery you have to pay more and it's a little line in the contract. It's bad to find out after you have a disaster about what the vendor offers. Some vendors are moving towards solutions for absolute fail over so they don't have down time."
   i. Estimated costs of ongoing support maintenance contract fees, what is and is not covered (i.e., required regulatory changes, etc.).
   ii. Is an ongoing contract required?
   iii. Are upgrades included in the ongoing maintenance fees? What is the definition of an upgrade, is it an enhancement to a current version or does the upgrade include version changes as well?
   iv. Are security patches included in ongoing maintenance fees? How long from the time of a security risk being identified by the operation system manufacturer, will an approved patch be certified and approved for installation?
   v. Downtime procedures
      1. What kind of tools can vendors offer like doing registration using a shadow system?
      2. If a virus eats up a provider's instance of their system, what is their guarantee of recovery time?
   vi. Upgrade and patch testing procedures
      1. How long is my system down when I get upgrade?
      2. How long is the shadow system down? (i.e. some vendors do M-F, 9-5 but most is not clear when you get into contracts)
      3. Is service after hours an extra estimated cost?
      4. How often are the mandatory upgrades?

d. **Standards:** Members still report frustration with data sharing. Without a defined set of standards defining structural data standards interoperability challenges will persist. The ability to accurately

and efficiently share discrete data between vendors requires detailed data standards and definitions including naming conventions and taxonomies. Today, this does not exist which creates confusion for providers.

Also adding significant effort and complication is the lack of a standardized agreed upon unique patient identifier. As one member noted, he has one vendor for their hospital and another for the ambulatory side plus some other systems and they still need interfaces. Matching patient data is fraught with errors because of the lack of a defined unique identifier and our members continue to assert the ability to accurately match patients to their records will foster better interoperability and improve patient safety.

Finally, privacy and patient consent challenges continue to plague our system frustrating providers and vendors and complicating greatly the exchange of information. CHIME continues to assert that 42 CFR Part 2 rules around patient consent for behavioral health and substance abuse must be aligned with the Health Insurance Portability and Accountability Act (HIPAA) rules.

Q. Types of reporting criteria for health care providers, patients, and other users of certified health IT products would be most useful in making technology acquisition, upgrade, or customization decisions to best support end users' needs?

A. Our members identified several reporting criteria that would be helpful to make more useful technology acquisitions and customizations. They include:

a. **Customization and upgrades**: Understanding customizations and upgrades are crucial and it's important that providers have a good command of what is entailed when they are signing contracts, especially from a cost perspective. ONC may want to consider reviewing the relationship between being able to meet Promoting Interoperability requirements (formerly Meaningful Use) and the relationship to vendor issues. There are EHRs where practices were taken by surprise when they learned vendors were not going to upgrade to the next version of certified software.
   i. What are the estimated costs of customizations?
   ii. What is the testing plan for customizations?
      a. Many vendors don't allow for testing – should be required.
      b. Is there a testing environment? Some vendors – especially larger ones have this but not all do and there can be extra estimated costs associated with this. Software development best practices would call for a full test environment and system testing before anything was put into production.
   iii. How frequently are upgrades released?
   iv. Ideally this should happen on cyclical basis (i.e. quarterly).
   v. Cost should not exceed more than 10-20 percent of the cost of the overall system
   vi. What is the upgrade schedule and are you required to take upgrades?

b. **APIs:** Current state APIs offered by the major EHR vendors are very patient-focused. Although this works well for development of applications that give individual patients more access to their personal health record, it does not address the needs around populations of patients. In order to for all parties to participate in value-based care agreements, the exchange of data between those parties is crucial. One major component is to identify a population or cohort of patients based on some therapeutic criteria, be it medication, device, implant or any other therapy in order to obtain clinical results to determine the efficacy of the therapy. As proponents of value-based health care agreements as a means to control costs for patients, providers and payers, EHR companies could broaden their API offerings from what is publicly available today. In doing so, the impact of external sources being allowed to directly query provider's transactional databases for populations of patients should be taken into account. Today's APIs do not easily allow for this, so it places undue burden on providers by forcing them to generate many unique reports for each VBHC agreement they enter. Population level APIs exposed to partners would allow for standard and more secure options for trading aggregated data to support value-based care programs.

   This all said, we are very concerned about the possibility for exploiting weakness in APIs as was evidenced earlier this month in a wide-spread breach with a major technology company that resulted in approximately 500,000 accounts being breached. The breach stemmed from a vulnerability in their API which exposed records for thousands of people. In fact, the exact number of those breached is not known. We believe there is a widespread misunderstanding that APIs will solve interoperability.

   While they certainly hold promise and hold part of the solution to addressing interoperability challenges, there are risks and several issues we feel have failed to be adequately addressed by policymakers. First and foremost is APIs facilitate access between EHRs and third parties. We believe patients must be better informed about the use of APIs and that this responsibility cannon fall squarely on just providers. One way this could be addressed is by informing patients before they grant a third-party access to their data, that the app developer addresses a handful of questions with the purpose of further educating patients on whether they truly want to trust this third party or not. For instance:

   - Do you sell identifiable information?
   - If yes is it used only for research?
   - Do you use the data for marketing?

   ONC could work with the Federal Trade Commission (FTC) on this issue since third-party apps are governed by this agency.

   Also, as we have highlighted previously, there are many costs associated with providers establishing API interfaces. We fear that our members will be called out as data blockers when in fact the root issue is cost and complexity that cannot easily be solved by APIs alone. Providers who are navigating this are going to struggle mightily to afford what essentially amounts to another massive

wave of interfaces. As one member noted, he has "2750 interfaces and 9 EMRs and they don't talk well together so when you say a health system is info blocking it's just they aren't good at sharing."

Finally, it is also worth noting that vendors are reporting being overrun with requests by third parties to connect with them. One vendor we spoke with said they have been hit with 500 requests in just one week.

Q. How can data be collected without creating or increasing burden on providers?

A. **Quality Measures:** Our members continue to report ongoing frustration with quality measure data reporting and that pulling data still requires a lot of "massaging" before it can be submitted. One way this may be able to be addressed is though the DOD's data dictionary. We recommend ONC review the DOD's data dictionary and determine whether this could be recycled for the purposes of reporting Medicare quality data and whether this could be leveraged as a best practice.

NCPDP: There is significant confusion around the interaction with Continuity of Care Documents (CCDs), Carequality, Commonwell, and Medicare Part D around the National Council for Prescription Drug Programs (NCPDP) standards requirements. Therefore, it would be helpful to know:

a. Which NCPDP standards are supported by the vendor?
b. Do they go beyond what is required under CEHRT?
c. What is the estimated cost for upgrading?

Q. What recommendations do stakeholders have to improve the timeliness of the data so there are not significant lags between its collection and publication?

A. Due to the different needs of different stakeholders, we recommend instead that the government use a standard release cycle of updated regulations which will then help vendors release updates in a more predictable manner.

Q. **For what settings (e.g., hospitals, primary care physicians, or specialties) would comparable information on certified health IT be most helpful?**

A. Any place there is certification, however, it is probably needed most by clinicians not affiliated with Integrated delivery networks (IDNs). Specifically, in this order: primary care, hospitals then specialists. And, under hospitals we would split hospitals into: critical access (priority 1); community hospitals (priority 2); large academic medical centers (priority 3); and IDNs (priority 4).

Q. How could HHS encourage clinicians, patients, and other users to share their experiences with certified health IT?

A. While KLAS already asks this question on every survey, we believe if there was one question to ask it would be how likely a provider would be to recommend their EHR to someone else.

IV. Categories for Reporting EHRs

Q. **What categories of reporting criteria are end users most interested in (e.g., security, usability and user centered design, interoperability, conformance to certification testing)? Please list by priority.**

A. Time and time again our members reported cost to be an extremely important topic. There remains a dearth of information available when making contracting decisions and far too often the case is the true cost of upgrades and implementation are unknown up front. Specifically, they are interested in getting the vendors to report an estimated range for total costs of ownership over a certain length of time (i.e., five years) as they recognize pinpointing a single cost could be challenging and a range could still be helpful for comparison purposes. For instance, they need this information on implementation and ongoing support as noted earlier. They also need information on what percent of their license spend is on implementation as it varies significantly vendor to vendor. Knowing estimated costs up front can help a provider project their estimated operating costs and some vendors will give models of the costs during the purchasing process.

Further, we recommend:

1. Against ONC establishing a complex rating methodology for rating vendors as we believe this is already being done to some degree in the private sector by entities like KLAS;
2. ONC using stakeholder feedback, identify a set of metrics like the 10-20 pieces of information needed by providers for contracting / purchasing and then share this with external entities to bolster existing industry benchmarking studies.
3. List estimated costs in the way of ranges.

And, on the topic of conformance testing, the top thing we believe ONC could do to improve this is to provide a sufficient number of test patients with enough data across setting of care since there is much variability around this.

Q. What reporting criteria could provide information on meaningful differences between products in the ease and effectiveness that they enable end users to meet their security and privacy needs?

A. The following items would be helpful in better informing a purchaser of the vendors security posture:

1. A complete security risk assessment should be made available. This is especially true for cloud-based vendors since there is very little transparency around these vendors' cyber posture and procedures. We find that for smaller providers using cloud-based vendors they automatically assume they are secure. And, the Office for Civil Rights' (OCR) risk assessment document must be the basis for this. We would caution, however, that the security risk assessment should be

made available to customers upon request; we recommend against making this publicly available as this could raise security concerns for vendors and providers.

2. Vendors should identify whether or not they are a member of an ISAO and ISAC.
3. Vendors should be required, to remain certified, to have annual security and penetration testing performed and the results should be made available to providers upon request.
4. Source code security analysis.
5. Whether they employee 2-factor authentication and what options there are for this (what is the 2nd factor?).
6. Encrypted Database features.
7. Role-based access control and if these roles are set or able to be configured. Also, how information on how the vendor handles staff with dual or multiple roles.
8. Whether they follow the NIST standards for password protection.
9. How they handle audit trails and reports.
10. How they handle patient consent opt-in agreements and what other technologies are required to implement this (i.e. Ipad, signature pad, etc.) so total estimated cost of implementation can be known.
11. Custom privacy policy and terms of conditions for portals.
12. Payment Card Industry Data Security Standard compliance for credit card transactions.
13. Gag clauses continue to frustrate our members and restrict sharing known vulnerabilities. Therefore, more transparency around whether these are required would be helpful. While medical device manufacturers governed by the Food and Drug Administration are instructed to report cybersecurity vulnerabilities that pose a risk to patient safety and that cannot be mitigated within 60 days, there is no parallel requirement for EHR vendors. Conceivably something akin to this policy could be helpful so long as sharing these vulnerabilities was done carefully so as not to invite bad actors who could further exploit these identified risks. This said, greater protections for sharing known vulnerabilities are needed. First, while the Cybersecurity Information Sharing Act of 2015 permits the sharing of information with certain limitations, providers still remain challenged in securing favorable contract language that permits the sharing of such information. Further, providers worry that sharing vulnerabilities, even if contracts allowed it, risks inviting unwanted audits thus safe harbors for engaging in vulnerability sharing are needed.

Q. Describe other useful security and privacy features or functions that a certified health IT product may offer beyond those required by HIPAA and the ONC Health IT Certification Program, such as functions related to requirements under 42 CFR Part 2.

A. Automated features associated with patient privacy would be very helpful and desirable for providers. Vendors should be able to track right of access, automate and track fulfilment requests such as when a patient has requested an amendment to their record. Also, automating patient preferences around restrictions associated with sharing records, as well as, accounting for disclosures. Finally, having the

capability for patients to file complaints via a patient portal would also be helpful. Managing any of these requests is a challenge for providers of any size thus knowing whether these features exists would provide utility for providers.

Additionally, a large burden on providers today centers around patient identification. There exists technology that does not necessitate a patient making a personal visit to the hospital to establish their identity. Thus, having information on a system's capacity to handle patient identification would also be helpful.

Q. Discuss the merits and risks of seeking a common set of measures for the purpose of real world testing that health IT developers could use to compare usability of systems.

A. We recognize that it could be hard to compare across a common set of measures, but we believe the total estimated cost of ownership would be very helpful.

Q. Comment on the feasibility and applicability of usability measures created from audit log data.

A. While providers must have audit logs to help meet the Health Insurance Portability and Accountability Act (HIPAA) requirements, our members were unclear how they could be comparable. Our members do not feel they would be a "make or break' item they would use to inform purchasing. That said, more recently some of our members are using them in more unique ways to obtain data. For instance, one member reports his organization is using audit logs to review safety issues and look for patterns around dispensing caps and drug diversion. And, there could be some larger group practices that are interested in audit log functionality and some vendors do offer some basic functionality around them.

Separately, we believe it would be helpful to have someone evaluating vendors' claims as being "HIPAA compliant." We understand HHS does not recognize this term.

Q. **Please comment on the usefulness of product integration as a primary means of assessing interoperability (as proposed in the EHR Compare Report).**

A. Accessing product integration is not enough to assess the interoperability of a product. In order to consume data received, providers need data files and discrete fields and there are always gaps they are trying to close. For instance, did the patient get their diabetic exam somewhere else and if so were the results shared? Or, is the patient a smoker and are they on a cessation plan; if so has that data been shared? As noted earlier, we believe there could be merit in using the DOD's data dictionary. And, even if the entire dictionary could not be used, work could be done to match the data standards with those required for meeting data standards in meeting Promoting Interoperability through the use of certified EHRs. Then you have data you can put it into context.

Q. **What additional information about certified health IT's conformance to the certification testing (beyond what is currently available on the CHPL) would be useful for comparison purposes?**

A. As noted several times throughout our letter, more cost transparency would be very helpful.

V. Conclusion

CHIME and AEHIT appreciate the opportunity to comment on the HER Reporting Program and look forward to discussing our ideas in greater depth with ONC. Should you have any questions please reach out to Mari Savickis, vice president, federal affairs at mari.savickis@chimecentral.org.

Russell Branzell, FCHIME, CHCIO
CEO & President, CHIME

Clint Perkinson
Director, Information Technology
Vice Chair, AEHIT