THE AMERICAN HEALTH QUALITY ASSOCIATION
7918 Jones Branch Drive
Suite 300
McLean, VA
www.ahqa.org

October 17, 2018

Dr. Don Rucker
National Coordinator for Health Information Technology
HHS Office of Security and Strategic Information (OSSI)
200 Independence Avenue, SW
Washington, DC 20201

Dear Dr. Rucker,

Thank you for the opportunity to comment on the *Request for Information Regarding the 21st Century Cures Act Electronic Health Record Reporting Program*.

Our organization, the American Health Quality Association (AHQA), represents the Quality Innovation Network-Quality Improvement Organizations (QIN-QIOs) and their quality improvement partners throughout the United States, Puerto Rico, the Virgin Islands, and the outer Pacific Islands. Our association's goal is to make health care better, safer, and available at a lower cost.

As organizations charged with working with providers, beneficiaries, families, and stakeholders to improve health quality practice and delivery, QIN-QIOs are keenly interested in the electronic health record (EHR) reporting program.

Below are our comments regarding selected elements included in the RFI:

Security

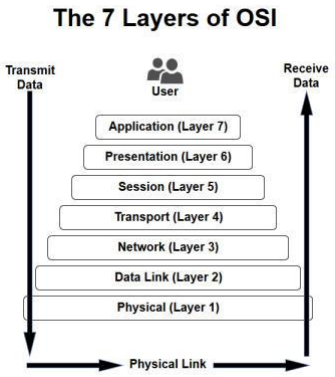
What reporting criteria could provide information on meaningful differences between products in the ease and effectiveness that they enable end users to meet their security and privacy needs?

AHQA believes that meaningful differences between products could be incorporated into the EHR certification process where the EHR products attest to which piece(s) of the HIPAA Privacy and Security Rule they address and satisfy. This information should be put into layman's terms for the certification process. Those who are operating within health care need an easily accessible and easy to understand way to ascertain where they are as an organization in terms of all information technology security.

In addition, although HIPAA applies to the entire covered entity, in our experience, through the Meaningful Use (MU) Rule and the certification of EHRs, a misunderstanding of "EHRs can make the provider HIPAA compliant" continues. Health IT developers can only go so far in ensuring the security of a covered entity. Developers can only meet certain privacy and

security criteria. So, the question remains, who bears the burden of compliance of the system? Currently, burden is on the provider, but security must now encompass more than just the EHR.

When looking at the Open Systems Interconnection (OSI) levels (see image below), security must occur at multiple layers, including the application, presentation, session, transport, network, and data link. Both the privacy and security rules apply at the user layer.



There is encryption by the user, at rest and in transit; providers can't solely rely on EHR vendor for encryption.

MU Stage 3 requires end-user encryption, not server encryption. We recommend that MU Stage 3 be updated to include more than just EHR functionality and quality measures.

We also recommend that the Security Risk Analysis (SRA) be expanded so that providers and hospitals know exactly what to address. The expansion should include hardened servers, DMZs (demilitarized zones), all computers within an office or hospital, passwords, copy machines, fax machines, etc. This information should be written in layman's terms for the certification process so personnel looking to procure a new system can easily identify the areas of security each vendor has to offer.

This rule should mandate that encryption is turned on for both end-user AND server devices or ANY device that has access or is connected to the EHR, such as smartphones.

Proof through reporting could include the following:

- Identification of encryption methodology for all office-based devices;
- Evidence of the SRA that providers fill out for either MU or the Quality Payment Program (QPP)—all providers outside of those realms have no requirement to comply outside of HIPAA;
- Information System Activity Review sample analyses;
- Results of vulnerability and penetration testing;
- Data integrity and audit controls, non-repudiation (review of audit logs);
- Access control mechanisms; and
- Encouraging the use of direct secure messaging encrypted e-mail for exchanging health information.

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.

HIPAA security and audit tools would be useful from a Health IT user perspective and we suggest these should be part of base health IT products. Additionally, the Certified Health IT

Product List (CHPL) entries for each EHR and health IT product should display all related security capabilities.

What information about a certified health IT product's security and privacy capabilities and performance have acquisition decision makers used to inform decisions about acquisitions, upgrades, or use to best support end users' needs? How has that information helped inform decision-making? What other information would be useful in comparing certified health IT products on security and privacy (e.g., compatibility with newer security technologies such as biometrics)?

AHQA recommends creating an action plan within practices to implement appropriate security measures to safeguard the confidentiality, integrity, and availability of electronic protected health information (e-PHI) to better protect patients' health information.

We also encourage regular assessment of a practice's adherence to the Technical Safeguards as indicated in an SRA through secure passwords, backing up data regularly, virus checks, penetration testing, vulnerability testing, and data encryption.

Lastly, we recommend that EHR vendors be required to provide documentation that they have adequate security controls in place on all their products and services using a security framework (e.g., FISMA 800-53, HITRUST Certification).

<u>Usability and User-Centered Design</u>

Describe the availability and feasibility of common frameworks or standard scores from established usability assessment tools that would allow acquisition decision makers to compare usability of systems.

AHQA recommends that the Centers for Medicare and Medicaid Services (CMS) and the Office of the National Coordinator for Health Information Technology (ONC) develop a set of comparison standards that are applicable for all health IT product types (e.g., EHR, interface, analytics tools) that describe and rank the quality and level of interoperability.

We also recommend that CHPL include health rankings of how the health IT products are using already developed standards, such as HL7, LOINC, SNOMED, and QRDA.

Supports the cognitive work of clinical users (e.g., displays relevant information in useful formats at relevant points in workflow)?

A foundational specification based on a clinical user type or specialty should be developed so users and implementers can determine how much customization would be necessary if they were to choose a certain health IT product solution for their particular specialty. At the present time, there is tremendous variation between the capabilities and user-centered design approaches of the EHR systems on the market. Clear explanation and documentation of the workflow that is necessary to support basic assessment data is critical for decision-makers to know and understand when selecting a system. Additionally, functionality inherent in the base/foundation system must be clearly delineated from what is available with

customization (which would require time, training, and often additional budget expenditures).

Reflects the ability of implementers to make customization and implementation decisions in a user-centered manner?

Health IT software customization inhibits interoperability. If CMS and ONC wish to improve interoperability they should push health IT developers to implement and suggest to their users a foundational build that will support quicker and easier paths to interoperability among systems. We would support a CHPL ranking of how well a certain health IT product is close to a foundational build. However, it must also be known that in order to reduce provider burden and ensure that EHR systems meet organizational workflow needs, customization must be possible. Identifying that delicate balance is paramount to ensuring that systems achieve interoperability standards as well as provide enough flexibility to meet the nuanced and varied needs of the provider or organization. Ideally, with proper codification of data elements transmitted through the CCDA or other document architecture, any and all EHR systems would be able to consume this data in a meaningful manner, without stifling requisite customization.

What usability assessment data, if available, are less resource intensive than traditional measures (e.g., time motion studies)?

"Number of click" studies, using time- and task-tracking software added to health IT software, are easier to deploy to track software use analytics than a human consulting workforce. Audit logs, periodic staff interviews, and workgroups are also beneficial in determining the usability of a system.

Who should report audit log data and by what mechanism?

AHQA recommends that CMS and ONC allow for automated health IT reporting to a central repository to reduce burden on health care providers and health IT users.

How feasible would it be to implement usage monitoring tools (e.g., for time spent on specific tasks)?

AHQA recommends that a common set of frameworks be developed, similar to QRDA formats and reporting mechanisms, to allow for automated reporting on elements such as time spent on specific tasks, time to close a note, time it takes to complete an order entry, time to assess a patient via a SOAP note, time it takes to discharge a patient, and others. EHR systems should also include elements of usage monitoring that include number of clicks to complete a history and physical; general nursing assessment; medication reconciliation and review of the Prescription Drug Monitoring Program (PDMP), as applicable; accessing diagnostic data; population health management assessment; and other elements of the chart regularly reviewed for continuity of care and safe patient management. Finally, monitoring the usefulness and time needed to collect and reconcile a consolidated clinical document architecture (CCDA) document must also be included.

<u>Interoperability</u>

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

Product Integration is a suitable means for assessing interoperability. In addition to the number, type, and names of products/devices for which the EHR vendors have established interfaces, AHQA requests that the vendors voluntarily report the technical standards they have employed (e.g., HL7 version) along with any documentation about their APIs (e.g., FHIR sandbox documentation). The EHR vendors are inconsistently approaching the development of these integration tools, and additional guidance may improve consistency of approach.

Additionally, the subjective reviews on ease of installation, use, and interface costs by function should be systematically collected, perhaps through a selected vendor (e.g., a vendor from Appendix 1). These reviews should be obtained (e.g., via surveys) from the clinical community along with companies actively collaborating with the EHR vendors on their SMART on FHIR integrations, as these companies have a working knowledge of the ease of interaction and use across the EHR vendors.

Finally, federal agencies that survey providers (HHS/CMS) should systematically collect and share data directly obtained from health care providers about their experiences with their respective EHR data systems and the providers' thoughts on EHR integration. Efforts can be coordinated through a private sector vendor as described previously.

What other domains of interoperability (beyond those already identified and referenced above) would be useful for comparative purposes?

AHQA proposes considering the evaluation of the EHR solutions' ability to interface with additional data system types, such as public health registries, population health/census information, federal/state/local agencies, Prescription Drug Monitoring Program registries, Health Information Exchanges, and All Payer Claims Databases.

Comment on whether State Medicaid agencies would be able to share detailed attestation-level data for the purpose of developing reports at a more detailed level, such as by health IT product. If so, how would this information be useful to compare performance on interoperability across health IT products?

AHQA supports granting State Medicaid agencies the ability to publish data for the purposes described above, upon the condition that this effort is not required of these agencies. Given this assumption, it seems that some State Medicaid agencies may have the means to publish granular data and should be encouraged to do so. If publishing guidelines are established, this may guide a direct comparison of EHR products across state lines, indicating potential national variance in implementation.

How helpful would CMS program data (e.g., Quality Payment Program MIPS Promoting Interoperability Category, Inpatient Hospital Promoting Interoperability Program, Medicaid Promoting Interoperability Programs) related to exchange and interoperability be for comparative purposes? What measures should be selected for this purpose? Given that some of these data may be reported across providers rather than at the individual clinical level, how would this affect reporting of performance by health IT product?

AHQA supports EHR vendor criteria that includes the base functionality to readily collect, generate, report, and export all required HHS/CMS (Medicare/Medicaid) quality measures such as defined by MIPS and Medicaid EHR incentive programs.

What other data sources and measures could be used to compare performance on interoperability across certified health IT products?

AHQA proposes identifying measures that may assess adherence to established standards and industry specifications, such as measuring the ability of an EHR vendor's product to generate CDA files utilizing the HL7 FHIR specification. AHQA also welcomes broader support for a single version of FHIR and adherence thereof by EHR vendors.

Conformance to Certification Testing

How should the categories listed in the RFI be prioritized for inclusion/exclusion in the EHR Reporting Program, and why? What other criteria would be helpful for comparative purposes to best support end users' needs (e.g., to inform health IT acquisition, upgrade, and implementation decisions)?

AHQA prioritizes the following categories:

Accessing and exchanging information and data from and through health information exchanges

The interoperability/HIE (health information exchange) landscape varies from state to state, so using product integration to assess it would be very biased toward the specific geography. Some states have taken a market-based approach while others have taken a state-based approach. The cost associated with HIE interfaces, as well as subscriptions, is highly variable based on the state. Awareness of what HIE solutions are provided by the vendor, as well as the general use cases for HIE, is an area where much education is needed. Cost associated with HIE subscriptions, as well as the usefulness of the data, is particularly important for small and specialty clinics.

Accessing and exchanging information from other health care providers or applicable users

Improved care coordination across settings requires efficient, timely flow of patient information between provider organizations. Poor access to this information is a primary contributor to adverse events such as hospital readmissions; improving data sharing should improve care coordination and overall health care quality. Moreover, with the opioid epidemic, it is critical for providers to have immediate access to the PDMP and other tools to review and identify any drug seeking behaviors or risks exhibited by their patients.

Accessing and exchanging patient-generated information

There are more and more examples of patient-generated data—through EHR portals and movements such as Open Notes where patients/families review clinical notes/records and provide needed changes back to providers. Additionally, wearables and other connected devices generate troves of e-health data that may be relevant to ongoing care management, especially for chronic care management.

Patient Reported Outcomes represent another area of opportunity for regularly obtaining information directly from patients about their ongoing health status. These data are typically not collected through standardized digital means, thus hampering patient care and research.

What data sources could be used to compare performance on these categories across certified health IT products?

AHQA recommends improvements in reporting post-EHR Certification issues back to the ONC. The current Certified Health IT Complaint process could be made more user friendly to encourage a more transparent reporting of issues. In our experience, the current process is too general and the follow-up steps are not clearly identified.

We believe that practices may find it valuable to include the number of complaints the ONC has received for individual products. We also recommend more transparency by CEHRT (certified EHR technology) from attestations from the Medicaid Promoting Interoperability Incentive program or MIPS reporting. The ease of reporting quality data via individual products should also be made available.

Inclusion of aggregate de-identified user performance could also be a data point that would be beneficial for EHR vendors to report. Users seeking to upgrade or implement a system may find this information valuable in informing their decision on how user-friendly, reporting capable, and readily available other aspects of support are with a given system.

Please comment on different types of information, or measures, in this area that would be useful to acquisition, upgrade, and customization decisions in the ambulatory setting as opposed to inpatient settings.

In our experience, cost data for each of these decision groups would be useful so that a provider can get a sense of the general cost required, especially in terms of customizing applications to meet clinic-specific needs. If available, the vendor's rate of successful deployments would also be useful, including de-identified data about the practices in which the vendor has deployed its products, such as size and type of practice.

While some of the workflow information is proprietary to a given system, it would be beneficial for EHR vendors to provide examples of clinical/operational workflows necessary to support reporting and documentation. Additionally, clear and detailed information on the data and analytics components of the system must be provided. Many systems are unable to readily pull necessary quality measure performance data, which makes it challenging for clinicians and practices to determine their performance. Furthermore, EHR systems must be more forthcoming with their ability to submit data to CMS or other regulatory bodies on behalf of the clinician or organization.

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?

Currently, the conformance information available in CHPL does not indicate to the user what is required; only what it has or does not have, as designated by a checkmark. Our suggestions for improvements include the following:

- The conformance standards that are shown in CHPL should include more of the details related to the specific conformance item. For example, with audit reports, it should indicate what auditable events it can report on, such as time stamp initial entry, modification, or exchange of data, and identify the actor/principal taking the action as required by users' scope of practice, organizational policy, or jurisdictional law.
- To capture information regarding end-user experience and product performance outside of the structured certification environment, ONC should consider providing a vendor scorecard using MIPS aggregated data that demonstrates end-user success rates in submitting data, average MIPS scores, or any other national initiative that is a CMS or ONC priority.
- To enforce security, all health IT applications must adhere to the rules established to control access and protect the privacy of health IT information. Identify which security measures assist in preventing unauthorized use of data and protect against loss, tampering, and destruction.
- Health IT applications should support chains of trust with respect to authentication, authorization, and privilege management.
- Information regarding decertification, surveillance, and non-conformance is currently available on the site, but ONC may want to consider posting litigation or class-action lawsuits pending with vendors that are the result of an inability to meet reporting requirements, information blocking, or other issues with the software resulting in loss to client health care organizations.
- All practices are required to complete a security risk assessment. As part of this assessment, health care organizations need to obtain a copy of the Disaster Recovery Plan (DRP). It may be helpful to practices for CHPL to make vendor DRPs available on the CHPL website or to have a link to each DRP for ease of access.

What mechanisms or approaches could be considered to obtain such data?

Force standards conformance. For example, demographic data remains a barrier for interoperability. HL7 standards address demographic data, but are not widely adopted or enforced, yet to exchange data through an interface or HIE, the EHR must translate that data into that standard.

MIPS data is available through CMS and could be de-identified and aggregated to provide the number of MIPS participants for each software product and the average score of the Eligible Clinicians. Scores for each MIPS category could also be averaged and made available according to specific vendors.

Litigation or class actions regarding vendor product functionality could be part of the self-reporting requirement for certification. This information could also be obtained by the certifying entity through surveillance and environmental scans.

What barriers might exist for developers and/or end users in reporting on such data?

The burden of providing this information to the CHPL website should lie with ONC and CMS and would not create a burden or barrier of reporting for developers or end users. The issue may be in sharing MIPS data among separate divisions of Health and Human Services.

Additionally, MIPS aggregated or averaged data could present a challenge; the data could be flawed, as some vendors may have low numbers of MIPS participants or serve specialists with a low number of clinical quality measures available to report (i.e., having a low number of participants or quality measures could skew the data). In our experience, there is also a lag time of six to eight months between MIPS reporting and availability of Eligible Clinician scores, which could be a barrier in providing timely information.

Finally, end users may find information regarding litigation or class action data, but it may be prejudicial, especially if the vendor is exonerated of any wrongdoing.

Other Categories for Consideration

What criteria should be considered to assess health IT performance in generating quality measures, reporting quality measures, and the functions required for supporting population health analytics (e.g., bulk data export)?

AHQA recommends the following criteria for consideration:

- Currently there are several ways to report quality and population health metrics like the Quality Reporting Document Architecture (QRDA), Qualified Registry, Qualified Clinical Data Registry (QCDR). The EHR Reporting Program should simplify the options available to providers, facilities, and hospitals that report quality and population health metrics.
- CMS should remove the cap of the number of measures that QCDRs can submit on behalf of a reporter.
- The QRDA file format and reporting methodologies should be simplified and implemented at the minimum level in each certified EHR product. Additionally, vendor developers should implement the minimum set of Clinical Quality Measures (CQM) that work across their representative health IT products, which would give quality reporters options to report clinical quality measures.
- CMS should work to develop a core set of population health reporting measures, similar to the CQM reporting methodology.
- AHQA supports EHR vendor criteria that include in base functionality the ability to readily collect, generate, report, and export all required HHS/CMS (Medicare/Medicaid) quality measures, such as defined by MIPS/QPP and Medicaid EHR incentive programs.

Thank you for the opportunity to comment above on the request for information. We believe our observations, comments, and recommendations are aligned with and in support of ONC, as well as the long history and demonstrated successes of the QIN-QIOs in partnering with HHS to achieve substantive improvement in health care quality.

Regards,

Alison Teitelbaum, MS, MPH
Executive Director