May 2, 2016

Karen B. DeSalvo, M.D., M.P.H., M.Sc.
National Coordinator for Health Information Technology
Department of Health and Human Services
200 Independence Avenue, SW
Washington, DC 20201

Attention: RIN 0955ï AA00
Submitted electronically to: http://www.regulations.gov

Dear Dr. DeSalvo:

The College of Healthcare Information Management Executives (CHIME) appreciates the opportunity to submit comments regarding the regulation proposed by the Office of the National Coordinator (ONC), ñONC Health IT Certification Program: Enhanced Oversight and Accountability,òpublished March 2, 2016.

CHIME is a professional association representing more than 1,800 chief information officers (CIOs) and other top information technology executives at hospitals and clinics across the nation. CHIME members have frontline experience in implementing the kinds of clinical and business IT systems needed to realize healthcare transformation. Healthcare CIOs share the vision of an e-enabled healthcare system as described by the many efforts underway at the Department of Health and Human Services (HHS).

I. Background

Presently, ONC delegates its authority to Accredited Certification Bodies (ACBs) to issue certifications for health IT. In the rule ONC proposes to: expand its authority to review health IT, including certified electronic health records (EHR), independent of an ONC-ACB; address testing issues in a timely and direct manner, which it says does not exist today; and provide greater transparency around surveillance and testing results of certified health IT.

II. Recommendations

We recommend that ONC:

1. **Collaborate with the Centers for Medicare and Medicaid Services (CMS) to minimize the impact of suspended or decertified products on provider reimbursement.**
2. **Use termination of certified health IT as a last resort.**
3. **Provide safe harbors for providers with products under appeal or that become decertified.**

III. Authority and Scope

CHIME appreciates ONCôs efforts to address real-world challenges that providers face in implementing health IT systems. Our members have interpreted this proposal as one that is aimed, in part, at addressing a number of the complaints received by clinicians concerning the ñusabilityò of their EHRs and from other providers, including our members, who have raised concerns that some systems do not perform as intended, such as failing to calculate quality measurement data correctly. Further, we appreciate ONCôs goal of providing, ñgreater accountability for health IT developers under the Program and provide greater confidence that health IT conforms to Program requirements when it is implemented, maintained, and used.ò We also support ONCôs efforts to first work with vendors on compliance issues before moving directly to a pathway that could lead to decertification.

The Health Information Technology for Economic and Clinical Health (HITECH) requires ONC to establish a voluntary certification program for health IT. Accordingly, healthcare providers are required to use a certified EHR as part of their participation in Medicare. ONC notes that it delegated authority to certify products to the ONC- ACBs, whose scope is generally limited to ñconformance determinations for health IT evaluated against adopted certification criteria with minimal determinations for health IT against other regulatory requirements.ò In some cases, ONC notes, ñthese non-conformities may pose a risk to public health or safety, including, for example, capabilities (certified or uncertified) of health IT directly contributing to or causing medical errors.ò Presently, however, thereôs no mechanism to address such non-conformities.

HITECH also amended the Public Health Service Act (PHSA) and required ONC to perform specified statutory duties including, ñkeeping or recognizing a program or programs for the voluntary certification of health information technology (section 3001(c)(5) of the PHSA), in a manner consistent with the development of a nationwide health information technology infrastructure.ò The law also requires that ONC must accomplish this in a manner that allows for the electronic use and exchange of information that accomplishes 11 objectives. These items include, but are not limited to, securing health information, improving quality, reducing medical errors, providing the right information at the point of care, improving care coordination, ensuring rapid response to public health threats, managing chronic disease, improving competition, and reducing health disparities.

IV. Avoiding Unintended Consequences

We recognize the 11 issues outlined above merit additional attention and are critical to a high-performing healthcare system, however, we are concerned with a variety of unintended consequences that could result from this proposal. **We urge ONC to consider these concerns before finalizing this proposal.** As such, the majority of our comments focus on the policy implications surrounding how the proposed expanded authority would be executed.

A. Practicality of the Scope

ONC has said it plans to use its expanded authority judiciously. Specifically the agency states, ñWe emphasize that our primary goal in all cases would be to correct non-conformities and ensure that certified health IT performs in accordance with Program requirements. In this regard, our first and foremost desire would be to work with the health IT developer to remedy any non-conformity in a timely manner.ò ONC expects this to be ñrelatively infrequentò and would ñfocus on situations that pose a risk to public health or safety.ò

First, the authority ONC is citing under the PHSA contains such an expansive and exhaustive list that we are concerned that addressing it will exceed ONCôs resources. Second, using this list as a possible list of ñnon-conformitiesò could mean that virtually all vendorsô certifications could be at risk, which would have a domino effect on providers. There is evidence highlighting challenges involving health IT pertaining to patient safety, medical errors, barriers to coordination of care, and quality improvement, to name a few. While some may be rooted in issues related to certified health IT, many may not. For instance, a March 2015 Joint Commission alert[1] cautions that health IT presents new challenges to healthcare organizations and could lead to a sentinel event. The alert notes that some events were the result of human error, while others were the result of design flaws. Further, the CEHRT program was never designed *primarily* to address many of the 11 items listed above. That being said, CHIME strongly supports any efforts that will help health IT systems become safer tools for delivering patient care.

Third, much of ONCôs proposal appears to center around patient safety, though itôs also clear the authority it seeks extends well beyond these issues. Our members have expressed concerns that patient safety is a complex topic and the proposal may not adequately account for the various ways providers deploy systems. They have also expressed concern that patient safety has become a catchall phrase that can mask other problems with EHRs, such as clinician frustration with workflow. We have similar concerns around medical errors. We caution ONC to proceed carefully here.

Finally, we note that the Version 2015 certification requirements added a number of additional mandates, including ñin-the-fieldò surveillance, requiring Authorized Testing Bodies (ATBôs) to ensure that certified Health IT modules can perform certified capabilities in a production environment (when implemented and used), enhanced surveillance of mandatory transparency requirements, and non-conformity and

[1] Joint Commission Sentinel Event Alert, Issue 54, March 31, 2015.

corrective action reported to the Certified Health IT Products List (CHPL) beginning in CY 2016. Moreover, there is an added emphasis on patient safety throughout the regulation.

B. Impact on Providers' Ability to Meet Medicare Requirements

Increasingly, CMS has made the policy decision to require use of certified EHRs as a condition for payment. Our members are concerned that ONC's proposal could negatively affect their ability to meet CMS requirements and their ability to receive reimbursement for a range of federally-administered programs, including alternative payment models. Without proper safeguards, providers using a decertified product, or one under appeal, are at risk of failing to comply with CMS regulations. This is especially worrisome since an appeal could last months and possibly years. ONC states that remedies for those who end up with decertified products are outside the scope of this regulations. We are troubled that this has not been taken into greater consideration. We are specifically interested in knowing whether products under appeal will jeopardize a provider's Medicare reimbursement. Will providers be eligible for hardships should their EHRs lose certification not just for Meaningful Use, but all CMS programs that warrant a certified health IT product? How long will they have to secure a compliant product? **We urge ONC to clarify how they plan on protecting providers from unnecessary violations of meeting Medicare payment policies if they are using products that are under appeal or have been decertified.**

There are also significant implications for a provider should their health IT lose certification. CMS estimates that the cost of purchasing new health IT to ranges from $33,000 to $649,836,000. In addition to having to purchase and deploy new technology, providers could be faced with staggering financial losses. Physicians are required under the Medicare Access and CHIP Reauthorization Act of 2015 to use certified technology. The financial impact of having to replace an IT system could put some physicians out of business. Providers could also face such tradeoffs as purchasing a new EHR or investing in other opportunities to improve patient care. By our estimates, the cost for some providers whose product becomes decertified could run into the billions.

The cost to a hospital for failing to meet the Meaningful Use requirements alone are a whopping millions of dollars for larger providers and thousands, if not hundreds of thousands, for others. Most hospitals balance sheets do not include the cost for failing to meet Meaningful Use and capital budgets are done years in advance; the uncertainty that could arise from a product under review by ONC could create significant challenges from a budget planning standpoint. Adding yet another way for providers to fail Meaningful Use ï for reasons outside their control ï is very concerning to our members. Finally, the financial toll of failing to meet Meaningful Use or other Medicare programs will undoubtedly result in fewer resources providers have to invest in technology or services that directly benefit patients. **We urge ONC to consider how to guard against the possible devastating financial impact decertification could have on patients and providers.**

C. Impact on Vendors

Again, CHIME shares ONC's concerns surrounding the impact of health IT on patient safety. Nonetheless, we caution that the scope of this proposal could also have unintended consequences for

vendors as well. We are concerned with the burdens this could place on vendors who are already devoting significant resources to meeting ONC certification requirements, often at the expense of meeting the needs of providers and the patients they serve. Without the appropriate protections in place, we worry that the scope of this new program could deter vendors from tackling challenges identified by their clients (our members) or devoting sufficient resources to delivering innovating products that again, will ultimately benefit patient care. Clearly, a balance needs to be struck where patient safety issues are prioritized but vendors are not caught up in an endless cycle of regulatory requirements that hurt their ability to meet provider and patient needs.

D. Impact on Vendors' Other Products

ONC proposed prohibiting a vendor that has had a product terminated or withdrawn due to non-conformity to obtain certification for any other health IT unless the problems were fixed and implemented with all affected customers or the recertification would fix these issue for all affected customers. We understand the intent of proposed policy and the issue ONC is trying to resolve. While we are sensitive to the need to ensure patient safety issues are appropriately addressed, we are worried that the impact of this policy needs to be balanced about the negative impact this could have on providers. We have two concerns with this and seek clarification around how ONC will operationalize such that unintended consequences do not occur.

First, how does ONC plan on mitigating providersôneed for products that will allow them to meet Medicare requirements? As an example, CMS requires that hospitals use the most recent version of clinical quality measures for electronic specification for each CQM for which the EHR is certified. What happens if a hospitalôs certified EHR does not have all of the required measures or it is not performing as intended and requires an upgrade? Would the vendor be prohibited from offering this upgrade? As another example, consider a provider who has already made a significant investment in time and resources into a certified EHR, but needs to purchase a population health module and finds it more cost effective to purchase one from their existing vendor due to interface costs. Under this policy they would be prohibited from doing so. Finally, a third example involves CMSôrecently announced Medicare Comprehensive Primary Care initiative which may involve additional functionality not already included in a certified EHR. Under this policy a physician may not be able to return to their existing vendor for the needed upgrades rendering them ineligible to participate.

E. Contracts

Our members question the implication of the proposal on their contractual obligation with vendors. Some providers do not have contracts with vendors that require maintaining certification status. Our members report that many of them signed contracts five years ago and some before they had to obtain certified EHRs. They also note it can be very costly to get out of a contract. We are worried that some providers, should their product go under appeal or become decertified, may find themselves in a situation where they are legally obligated to make payments on a system they can no longer use to meet Medicare

requirements. **We seek clarification from ONC on how they plan on addressing these types of scenarios.**

F. Data Blocking

The administration has made it abundantly clear that it will not tolerate data blocking. We wonder how the proposed rule will impact the administrationôs efforts around data blocking. Will ONC go after suspected vendors? As one member reflected, the impact of one of the top EHR vendors being decertified could have far reaching implications for providers. While admittedly an unlikely scenario, it would be helpful for ONC to address these concerns.

V. Transparency

CHIME strongly supports ONCôs efforts around increasing transparency of vendor certified products. We believe this is crucial for a healthy marketplace and will ensure providers are better informed consumers. Additionally, we believe that shining a bright light on the products reviewed for certification will continue to push vendors to ensure their products are working as intended before they are deployed into the market and addressed more rapidly for those already in use.

We also appreciate that ONC has called for vendors to ñnotify affected customersòfor both suspended and decertified products. Additionally, we believe that affected providers should be alerted via email, letter, posted information to the vendorôs website, newsletter and other communication vehicles, as well as, the CHPL. We also urge ONC prior to finalizing the decertification of a product to alert affected customers first.

ONC has called for vendors to submit corrective action plans when non-conforming health IT is identified and to make corrections before the product could continue to be listed on the list of certified products or could be sold or licensed with the certified designation. ONC also notes, ñThe corrective action plan would provide a means to correct the identified non-conformities across all the health IT developerôs customer base and would require the health IT developer to make such corrections before the certified health IT could continue to be identified as ôcertifiedôunder the ONC Health IT Certification Program, or sold or licensed with that designation to new customers.òWe appreciate vendors being required to submit a corrective action plan. However, we remain concerned as detailed earlier about the impact this will have on provider reimbursement with Medicare.

Finally, we seek clarification on how ONC envisions addressing situations that involve non-compliance that are tied to ñuncertifiedòIT. ONC states that if it finds ñthat certified health IT does not conform to Program requirements, ONC would take appropriate action with the health IT developer to remedy the non-conformityé remedying a non-conformity may require addressing both certified and uncertified capabilities within the certified health IT.òProviders are confronted with a host of challenges related to security which are mounting with a growing ñInternet of Things.òToday, device manufacturers are neither

mandated to meet cybersecurity or interoperability mandates as part of the review process they must undergo for Food and Drug Administration (FDA) approval.

VI. Conclusion

In conclusion, CHIME appreciates the intent behind ensuring providers have systems that meet certification requirements and are performing at the highest optimal level. We strongly support the need for systems to be safe for patients. Nonetheless, we urge caution in moving forward with this rule until the issues we have outlined above can be addressed to the satisfaction of those buying and using these systems. It will be critical to reduce the regulatory complexity and allow market forces to drive innovation as providers move into new models of care and reimbursement.

Sincerely,

Russell Branzell, FCHIME, CHCIO
CEO & President, CHIME

Marc Probst, CHCIO
Chairman, CHIME Board of Trustees & CIO, Intermountain Healthcare