

May 2, 2016

Karen DeSalvo, MD, MPH, MSc
National Coordinator for Health IT
U.S. Department of Health and Human Services
200 Independence Ave, SW
Washington, DC 20201

Dear Dr. DeSalvo:

On behalf of the Healthcare Information and Management Systems Society ([HIMSS](http://www.himss.org)), we are pleased to provide written comments to the Office of the National Coordinator for Health Information Technology (ONC) in response to the [ONC Health IT Certification Program: Enhanced Oversight and Accountability Notice of Proposed Rulemaking](#) (NPRM). HIMSS welcomes the opportunity to leverage our members' expertise in commenting on this NPRM, and we look forward to continuing our dialogue with ONC on enhancing the ONC Health IT Certification Program.

HIMSS is a global, cause-based, not-for-profit organization focused on better health through information technology (IT). In North America, HIMSS focuses on health IT thought leadership, education, market research, and media services. Founded in 1961, HIMSS North America encompasses more than 64,000 individuals, of which more than two-thirds work in healthcare provider, governmental, and not-for-profit organizations, plus over 640 corporations and 450 not-for-profit partner organizations, that share this cause.

HIMSS welcomes ONC's continued focus on enhancing and maintaining the ONC Health IT Certification program. We remain supportive of the Medicare and Medicaid Electronic Health Record (EHR) Incentive Program and its associated Health IT certification program, and recommend that any additional changes to these programs focus on furthering public health and safety, encouraging simplification, promoting innovation, and reducing the workflow and reporting burden on providers and developers.

In this letter, we provide our comments to the three major components of this NPRM. We are generally positive on the new paradigm for oversight of ONC-Authorized Testing Laboratories (ONC-ATLs) as well as the transparency and availability of surveillance results. We do however, have some questions and concerns regarding ONC's proposal for direct review of certified health IT.

While the NPRM's stated goals are to enhance program oversight and health IT developer accountability for the performance, reliability, and safety of certified health IT, HIMSS encourages ONC to use this rule to promote a climate of continuous improvement through policy actions rather than punitive approaches that focus on certification suspension and/or termination processes. For example, emphasizing the use of Corrective Action Plans (CAPs) designed to identify and remedy non-conformities so that a Complete EHR or Health IT Module can maintain its certification may be of more overall benefit to the health IT community than other

tactics or proposed approaches. When studying the implications of this rule, it is imperative that ONC keep providers and ultimately patients at the forefront when considering any further changes related to certification processes.

ONC Direct Review of Certified Health IT

ONC proposes that, in addition to review of certified health IT by ONC-Authorized Certification Bodies (ONC-ACBs), it would directly review certified health IT and act when necessary to “promote health IT developer accountability for the performance, reliability, and safety of health IT.” ONC also emphasizes its ability to work with developers in a timely manner to remedy any technology solutions that do not conform with certified health IT. The intention is to in a timely manner and across all customers, potentially eliminating the need for suspension and/or termination processes. These provisions are framed as a complement to current paths of review for certified HIT through ONC-ACBs and “provide an additional tool to address public health and safety issues that may arise.”

The proposed rule provides ONC with very broad discretion to review certified health IT. It anticipates that such review would be used relatively infrequently and would focus on situations posing a risk to public health or safety, but believes “there could be other exigencies, distinct from public health and safety concerns, which for similar reasons would warrant ONC’s direct review and action.”

The focus on public health and safety and “other exigencies” is grounded in ONC’s statutory responsibility to keep or recognize a certification program(s) “in a manner consistent with the development of a nationwide health information technology infrastructure that allows for the electronic use and exchange of information and that, among other requirements: ensures that each patient’s health information is secure and protected, in accordance with applicable law; improves health care quality; reduces medical errors; reduces health care costs resulting from inefficiency, medical errors, inappropriate care, duplicative care, and incomplete information; and promotes a more effective marketplace, greater competition, greater systems analysis, increased consumer choice, and improved outcomes in health care services (see section 3001(b) of the PHSA).” Non-conformance with any one of these goals, even if the goal was not part of certification, would be a basis for certification suspension or termination.

ONC states that it could suspend certification at any time if it believes that the certified health IT “poses a potential risk to public health or safety, other exigent circumstances exist concerning the product, or due to certain actions or inactions by the product’s health IT developer as detailed”. Per 170.580(d)(1)(i), “ONC would suspend a certification issued to any encompassed Complete EHR or Health IT Module of the certified health IT if the certified health IT was, but not limited to: “contributing to a patient’s health information being unsecured and unprotected in violation of applicable law; increasing medical errors; decreasing the detection, prevention, and management of chronic diseases; worsening the identification and response to public health threats and emergencies; leading to inappropriate care; worsening health care outcomes; or undermining a more effective marketplace, greater competition, greater systems analysis, and increased consumer choice.” This listing is also justified as based on ONC’s duties per section 3001(b).

Specifically, the proposed rule includes provisions to:

- Directly review certified health IT, independent of and in addition to an ONC-ACB's role;
- Enable ONC to assess non-conformities, including those that pose a risk to public health and safety (but including other HITECH HIT priority areas that the certification program is intended to support), which may be caused by the interaction of certified and uncertified capabilities within certified health IT;
- Prescribe comprehensive corrective actions for developers to address nonconformities, including notifying affected customers;
- Enable ONC to suspend and/or terminate a certification issued to a Complete Electronic Health Record (EHR) or Health IT Module;
- Institute processes for prohibiting further testing and certification of any health IT that a health IT developer brings to ONC if a found non-conformity is not first corrected or will be corrected through release of new certified health IT; and
- Establish an appeals process for developers.

Overall, HIMSS has concerns on the duplication of effort suggested in this approach given the enormity of the work that needs to be accomplished in the health IT community. ONC has a major task in ensuring that ONC-ACBs and testing laboratories are sound, adequately funded, and resourced directly or in the context of the applicable community. Such a process should also involve a reporting process to ONC to keep them informed of the work that is being done, the risk mitigation that is taking place and if necessary, the interventions enacted to support the community. If there are flagrant breaches of acceptable behavior, those can be addressed on an as-needed basis in a disciplinary or punitive manner. HIMSS notes that this approach would allow health IT innovation and development as well as a prudent responsiveness to proceed in identifying and mitigating the impact of potential concerns as they arise.

The proposed high-level certification criteria by which ONC would determine the need for intervention are very broad and include “[t]he potential risk to public health or safety” and the nebulous “or other exigent circumstances” without a defined set of specific criteria that can guide product development and implementation. HIMSS asks ONC to better define this high-level need for intervention by the agency so that the health IT community can better understand under what circumstances ONC would use this proposed authority. HIMSS is hopeful that in clearly defining the need for intervention, ONC would create guidelines for when this new authority would be utilized.

Ultimately, HIMSS recommends that ONC should only very rarely need to intervene due to ONC-ACB limitations, and should refine the applicable language dealing with such limitations and focus its efforts only on the most exigent safety-related issues and not address all of the strategic goals set out for ONC in the Health Information Technology for Economic and Clinical Health (HITECH) Act. In addition, ONC should only focus on conformance, including safe conformance, to certified capabilities that have gone through the regular process to develop certification criteria and not to an ad hoc and implied set of new criteria as is proposed.

Notice of Potential Non-Conformity or Non-Conformity

HIMSS endorses the idea that any notice of potential non-conformance should be defined by current certification criteria functionality to which the product is certified. In addition, “non-

conformity” should be specifically identified to whether it applies to specific certification criteria or the broader bases for evaluation proposed by ONC. A thorough initial and follow-up process for evaluating the alleged non-conformity is encouraged to avoid wasting resources on trivial complaints or unnecessary investigations. We encourage ONC to promote discussion between the developer and the ONCACB regarding complaints or surveillance-related potential nonconformities as a first step in determining whether a potential non-conformity notice should be issued.

A notice of potential non-conformance defining the specific certification criteria and alleged non-conformance should always be the first step in addressing a complaint that the product is not conforming as certified. HIMSS is unsure how ONC could be in a position to send a notice of definite non-conformance without first engaging the developer in discussions, sending a notice of potential non-conformance in nearly all cases is the wrong approach.

This notice of potential non-conformance should be handled through a formal receipt verification mail process to ensure that the health IT developer is aware, and not relied upon only through email notification. Once the developer receives the potential nonconformity and assesses it, the developer should have to acknowledge the issue if there is a non-conformance with which they agree or provide documentation to ONC for review that there is no nonconformance. This rule should define the timeframe for this initial response and subsequent CAPs.

It is important to note that the number of days should be defined in terms of business days. Once a non-conformance is confirmed, ONC should issue the notice of non-conformance and the developer should initiate the process to submit a CAP. With a CAP underway, HIMSS recommends that there be no further action or sanction on the developer working to correct the problem unless extreme and exigent consequences to health and safety are determined, thus allowing the CAP to be fulfilled without imposing any sanctions on the health IT developer (unless the CAP is not fulfilled).

We are also concerned that the proposal for Records Access is very broad and appears to go well beyond what is required for ONC-ACB surveillance, especially given the proposed broad scope of the basis for direct review. The final language should be more narrowly focused on records that directly bear on the specific certified capabilities affected by the non-conformance and only materials relevant to the issue at hand.

Overall, HIMSS suggests that review by an ONC-ACB should be the typical process to address concerns about non-conformance. We ask that more specific circumstances be defined in the final rule to when ONC would exert direct review.

Suspension

HIMSS recommends that ONC or an ONC-ACB only consider suspension appropriate when an extraordinary, exigent, and unambiguous risk to public health and safety exists and the developer had a complete failure to cooperate. Until the extent of the potential risk is actually determined and confirmed, suspension should not be applied.

Such punitive action without just cause serves little useful purpose and could needlessly alarm

providers and cause them concern about using products that are in fact conformant. Certainly, health IT modules could be questioned and/or alleged as being non-conformant or associated with events labeled “patient safety,” when in fact, the complaint is not accurate, in whole or in part. There must be clear policies to address real non-conformities; however, no assumption of guilt should be taken without following the proper implemented policies.

ONC has requested comment on the appropriate timeframe for a health IT developer to notify affected or potentially affected customers of the suspension. Assuming the limitations for the basis of suspension are being clearly defined by patient safety or public health, HIMSS supports the idea that health IT developers already have policies and procedures in place to define such parameters through their quality management system and there is no need for ONC to attempt to define or impose a specific minimum timeframe.

HIMSS strongly discourages ONC from applying suspension of a specific product to other products that the health IT developer may be testing or certifying within the certification program. Any suspension should only apply to the product in question and not to other unrelated products. Suspension across the board could disrupt the health IT developer product development cycle and would have profound effects on additional providers unaffected by the suspended product.

In response to ONC’s request for comment regarding correcting the nonconformity for a certain percentage of customers or certain milestones, HIMSS reiterates that suspension should only be applied in circumstances as defined above. Enabling the correction to the software for the nonconformity and making it available for implementation could take varying amounts of time to implement. HIMSS suggests that an important point for lifting the suspension is the availability of the correction to the customer base and not the absolute implementation by all affected providers as the health IT developer can encourage implementation but cannot necessarily control it.

Termination

The proposed rule states that termination could be implemented without the product in question undergoing a suspension process; however, HIMSS opposes termination as a first step. Complete EHR or Health IT Module certification termination seems draconian as, once certified, it would be unlikely that the entire product would be corrupted by an identified weakness or fault. The level of dependence on these systems for healthcare delivery—as evidenced by recent ransomware situations—reflects that greater harm could come from taking an EHR or Module offline rather than imposing a limited focus on correcting the problem or eliminating the faulty portion of the product to address the identified failure.

HIMSS urges ONC to reconsider the impact of the proposals regarding termination, including limits on how termination may be cured, potential limits on all products certified via a program ban, and the adverse effect on providers as well as health IT developers with punitive actions. For example, consider the impact of a termination that occurs and applies to all certified products offered by a vendor when it is time for providers to attest, or the questions that will arise about the validity of the health IT used during a reporting period. In addition, prohibiting a developer from updating the certifications for products unaffected by the termination could also have major

negative impact on providers.

Appeal

HIMSS is unclear on the intent and scope of the first basis for an appeal, “(1) ONC incorrectly applied Program methodology, standards, or requirements for suspension or termination.” The “Program methodology, standards, or requirements” must be much more explicit than proposed if this basis is to be sufficient and not be an unreasonable limit on potential appeals. HIMSS seeks a standard definition of “sufficient support” as used in the second proposed basis for an appeal.

HIMSS is concerned that there are no stated requirements for the qualifications of, and oversight for, the hearing officer; and it is also unclear if the hearing officer is an ONC employee or agent. If so, such a role raises conflicts of interest concerns absent specific processes to ensure independence. The hearing officer should have an assured level of independence from ONC management. In addition, the developer should always have the right to a hearing. Furthermore, the decision to hold a hearing should not be at the sole discretion of the hearing officer. Moreover, ONC should have an obligation to provide a written statement for the hearing process, including any and all information, analysis and documentation it used (not just “relied upon”) to come to its determination and make it available to the developer. Finally, we strongly disagree with the provision that “(iii) The hearing officer will neither receive testimony nor accept any new information that was not presented with the appeal request or was specifically and clearly relied upon to reach the determination issued by ONC under paragraph (d)(2) or (e)(2) of this section.” Information that is developed during the course of a hearing should be able to be considered by the hearing officer.

HIMSS agrees with the 30 days as proposed for the hearing officer to render a decision and that extensions should require the consent of both parties. We do oppose, however, that the National Coordinator’s determination, as issued by the hearing officer, would be the agency’s final determination and not subject to further review. Ten calendar days to file an appeal, as opposed to provide notice of intent to appeal, is too short a timeframe. The materials needed for the appeal could be quite lengthy and complex. At a minimum, this time should be expressed as business days. Further, we propose that developers have at least 20 business days to file the appeal. HIMSS suggest that ONC look at the appeals process that the Centers for Medicare and Medicaid Services (CMS) uses for supplier revocation and appeals as they offer a timeline that we would support for the appeals process.

Consequences of Certification Termination

ONC notes that this proposed rule does not address the consequences of certification termination beyond requirements for recertification, especially regarding end users and provider participants in programs relying on certification for incentive and/or penalty eligibility. The consequences of, and remedies for, termination beyond recertification requirements are considered outside the scope of this proposed rule. For example, this proposed rule does not address the remedies for providers participating in the EHR Incentive Programs that may be using a Complete EHR or Health IT Module that has its certification terminated. Although HIMSS supports the idea that ONC and, as applicable, the ONC-ACB should work with the developer to remedy the identified

non-conformity, instituting such an approach without corresponding consideration by CMS on implications for providers in the EHR Incentive Program, and other affected programs is problematic and does not enable full consideration of this proposal.

HIMSS requests that “heightened scrutiny” be specifically defined, extend for six months only, and only apply to the functionality that was the subject of the alleged non-conformance. We strongly oppose the proposed program ban. ONC should not apply termination for a specific product towards other products that the health IT developer may be testing or certifying within the certification program. Any termination should only apply to the product in question and not apply to other unrelated products. Applying termination universally to a health IT developer under the premise that it would cause the health IT developer to address the nonconformity any differently could undermine additional providers who may be in need of other health IT products from the same developer. More generally, termination across the board could totally disrupt the health IT developer product development cycle and would have profound effects on additional providers unaffected by the suspended product. We are unaware of this approach to product suspension in other analogous regulatory programs.

Oversight of ONC Authorized Testing Laboratories

The proposed rule includes provisions that would enable ONC to conduct direct oversight of National Voluntary Laboratory Accreditation Program (NVLAP)-Accredited Testing Labs. It proposes that such labs apply to become ONC-Authorized Testing Labs (ONC-ATLs). ONC also proposes to establish processes to authorize, retain, suspend, and revoke ONC-ATL status. The proposed approach would create authorization and oversight for testing labs that is intended to be similar and comparable to the approach used for ONC-ACBs.

HIMSS is generally positive to this proposal. However, ONC should carefully implement this process in a way that does not negatively impact the work of testing labs. HIMSS wants to ensure that creating ONC-ATLs does not reduce test lab participation in certification, slow down the overall evaluation process, or generate costs that could be passed on to providers (either directly or indirectly).

Like ONC-ACBs, test labs operate under the structure of one or more International Organization for Standardization (ISO) standards, so HIMSS requests that this new level of oversight be consistent with governing ISO standards. In addition, HIMSS supports the idea of test labs performing only portions of the certification program. In the future, the community could be looking at a test lab that focused its certification program on one capability. For HIMSS, there is no real downside as long as ONC has enough test labs that provide broad-based testing services.

Transparency and Availability of Surveillance Results

Under this proposal, ONC-ACBs would be required to make identifiable surveillance results publicly available on their websites quarterly, beyond the information on non-conformities and CAPs that must be disclosed today. ONC states that this provision is intended to enhance transparency and accountability of health IT for customers and users by providing “valuable information about the continued performance of certified health IT” and that public availability of identifiable results “would provide a more complete context of surveillance by making more

information about certified products available to purchasers and enabling health IT developers to note their continued compliance with Program requirements.”

ONC frames this proposal as making available the mostly positive results of surveillance. It states that surveillance results would include information such as, but not limited to: names of health IT developers; names of products and versions; certification criteria and program requirements surveilled; and outcomes of surveillance. ONC also emphasizes that it does not propose to require that publicly posted surveillance results include proprietary, trade secret, or confidential information (e.g., “screenshots” that may include such information).

HIMSS agrees that the availability of more balanced surveillance results could provide a more complete picture of certified EHRs and other health IT. Given the positive outcomes of these additional surveillance results, ONC and the ONC-ACBs should provide summary results, using both the general approach to information to be released on CAPs and the definition of “results” used in the 2015 Edition Health IT Certification Criteria Final Rule. HIMSS also endorses the idea of posting this surveillance information on the Certified Health IT Product List to ensure that it is truly publicly-available and easily accessible.

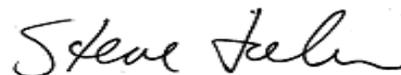
HIMSS suggest that ONC use a definition of “results” that is a ceiling rather than a floor to ensure program consistency, that does not include interim work product or information obtained in the course of surveillance (i.e., disclosure should truly focused on results), and that as proposed, does not include proprietary or business sensitive information. “Results” should emphasize certified capabilities evaluated and not indicate why surveillance took place (e.g., provider expressed concern) as such information could provide a misleading and incomplete picture to consumers of the information. Finally, ONC and the ACBs should clearly indicate that surveillance of specific certified health IT should not imply a problem or potential problem with the underlying technology.

We welcome the opportunity to meet with you and your team to discuss our comments in more depth. Please feel free to contact [Jeff Coughlin](#), Senior Director of Federal & State Affairs, at 703.562.8824, or [Eli Fleet](#), Director of Federal Affairs, at 703.562.8834, with questions or for more information. Thank you for your consideration.

Sincerely,



Dana Alexander RN, MSN, MBA, FAAN, FHIMSS
Vice President, Clinical Advisory Services
Divurgent
Chair, HIMSS North America Board of Directors



H. Stephen Lieber, CAE
President & CEO
HIMSS