

**IUS Group 1 Assignment:**

• Principles of Proper Conduct for ONC-ACBs -262

• Surveillance and maintenance – 262

• Transparency and Disclosure Requirements -269

• Complaints Reporting -296

• Open Data Certified Health IT Product List (CHPL) - 274

• Adaptations and Updates of Certified Health IT -296

• Decertification – 298

**Group 1 Members**

1. Steven Stack- Lead

2. David W. Bates

3. Paul Egerman

4. Rollin (Terry) Fairbanks

5. Anne Pollock,

6. Alisa Ray

| | **1. “In-the-Field” Surveillance and Maintenance of Certification Page #262** | | --- | | **We propose to adopt new requirements for “in-the-field” surveillance under the ONC Health IT Certification Program. Our proposal would build on ONC-ACBs’ existing surveillance responsibilities by requiring ONC-ACBs to initiate in-the-field surveillance of certified Complete EHRs and certified Health IT Modules in certain circumstances and in accordance with certain standards and procedures described below. Our proposal would also clarify ONCACBs’ responsibilities for requiring certified Health IT Module and certified Complete EHR developers to take corrective action in instances where the technology fails to conform to the requirements of its certification. (Continued on page #263)** |   The group agrees that we support robust, increased focus on surveillance of certified products. It is important to address the need to assess how these EHRs are actually working in real world deployment. We are supportive of ONC’s intent to prioritize implementation surveillance to health IT capabilities related to interoperability, patient safety, and privacy and security. Surveillance results could be useful for informing future rounds or enhancements for certification. ONC must define what is meant by onsite surveillance (Observations? Video? Retrospective navigation data?) . This exercise must be carefully thought out, with well-defined measurement objectives, and very clearly documented methodologies  EHR implementations as well as updates can be problematic. The process must be reasonable and considerate with regard to burden placed on end user.It is unclear how this will be evaluated in the field, especially in the context of the uniqueness of each user group and context of use.  A crucial point of clarification includes the “unit of analysis” for certification. The program was designed to evaluate software in a laboratory once, and then the benefits accrue to all users that install and use that software product. Vendors/developers are accountable. As written this regulation could change that unit of analysis to “the software as implemented”. Given that users/providers make many configurations and customization decisions, each of these affect the ability of the software to perform against the certification criteria. Are we asking each Lab/Cert Body to test and certify each custom implementation? If there is a fail, who is accountable—vendor/developer or user/provider? Is the vendor accountable for providing guidance in best practices and lessons learned from prior implementations?  When the EHR is not working as expected, the end user is not easily aware of the cause of the dysfunction (and my not even be aware that the dysfunction exists). We agree with the intent of the statement “Requiring Complete EHR developers to take corrective action in instances where the technology fails to conform to the requirements of its certification” but caution that this has the potential for unintended consequences and should not produce additional burdens to providers or health system purchasers.  **Areas of clarification needed:**   * Clarification of how HIPAA impacts onsite surveillance, patient and provider protections. * What weight should Certifiers give to poor product implementation on the part of the provider?   + How can “poor” or “good” performance be objectively determined?   + What compels them to participate? Is this an official “audit”?     - Providers have limited time and staff to accommodate this review and clinical operations must not be negatively impacted. Audits must be sensitive to these concerns.     - What federal ruling gives Certifiers the authority to “audit” the vendor product implementation at the provider site?     - Is this voluntary or mandatory on the part of a provider?     - How will this criteria prevent “cherry picking” of customers - If random customer names are requested from the vendor, Certifiers are sure to receive contacts at only successfully implemented customer sites.   + As part of Lab/Certifier vendor relationship, the new surveillance process will need to be built into new customer agreements at time of application, and current vendor customers agreements must be altered to reflect new charges   /fees. The timing should reflect this. This process should not produce additional burdens to providers or health system purchasers.  Recommendation: Many of the concerns can be addressed by a more rigorous and protocol driven complaint process, with periodic public reporting mediated and monitored by the ACBs. This may be a more cost-effective method of gathering the information. ONC-ACBs do not have access to vendor customer lists to promote this on their own. But ONC, working with CMS, could do this effectively. |
| --- | --- | --- |
| **2. Transparency and Disclosure Requirements Page #276** |
| We propose to revise the principles of proper conduct for ONC-ACBs in order to provide for greater and more effective disclosure by health IT developers of certain types of limitations and additional types of costs that could interfere with the ability to implement or use health IT in a manner consistent with its certification. We believe that these additional disclosure requirements are necessary to ensure that existing and potential users and implementers of certified health IT are fully informed about these implementation considerations that accompany capabilities certified under the ONC Health IT Certification Program. (Continued on page #276) |
| The work group agrees there is a need for further certification and product transparency. We appreciate that ONC has cited the AMA’s remarks in their v2015 health IT certification NPRM regarding the costs associated with health IT and information exchange (pg. 278). We agree with and appreciate ONC’s acknowledgment that, “health IT developers not disclosing known material limitations or additional types of costs associated with the implementation or use of certified health IT creates a substantial risk…” and therefore support the proposal to expand which information health IT developers are required to disclose.   * We support the notion (pg. 283) of a more specific cost structure to include all costs and fees physicians would be required to pay for any EHR function (MU related or not) outside the monthly service contract. * Information on costs should include relevant factors including volume of transmissions, geography, interfaces, and exchange partner technology. * It would be assistive to eligible providers who need to have a relatively clear understanding of costs (in dollars) without the additional burden of calculating their own estimation of vendor fees and prices, to have vendors publish a range of prices for each service, interface, or extra function. * Eligible providers and hospitals should be able to easily understand what the overall cost will be for their system implementation, customization and what costs are associated with transmitting data and perform the daily functions required for patient care.   In the spirit of transparency, vendors should collect HISP/HIE fees and/or pricing information and provide it to the customers ONC should list this information publically on their website.  Also in the spirit of transparency, known issues from previous implementations (flaws, safety risks, functional deficiencies) should be shared openly with potential and existing customers. Contracts should not prohibit customers from sharing information on their own (positive or negative) including screen shots and other information (helpful to demonstrate lessons learned) regarding aspects of a custom feature, training and implementation questions or reporting tools, and other functional elements. |
| **5. Complaints Reporting Page #296** |
| **We propose that ONC-ACBs provide ONC (the National Coordinator) with a list of complaints received on a quarterly basis. We propose that ONC-ACBs indicate in their submission how many complaints were received, the nature or substance of the complaint, and the type of complainant (e.g., type of provider, health IT developer, etc.). We believe this information will provide further insight into potential concerns with certified health IT or the ONC Health IT Certification Program and give ONC a better ability to identify trends or issues that may require action including notification of the public. We propose to include this new requirement in § 170.523(n). (Continued on page #296)** |
| The work group is supportive and agrees with complaint information being publically posted online. In order to be actionable and meaningful, Vendor / complainant should be identified.   * This exercise must be carefully thought out, with well-defined measurement objectives, and very clearly documented methodologies. The process must be reasonable and considerate in regard to burden placed on end user as well as the vendor. A process that uses the ACBs through ANSI Accreditation standards might include: * Keep publically available records of customer complaints and their outcomes (ongoing or closed). * Include detailed transparent processes. Example, standard categories of reporting, by product and version number. * Ease of complaint process, standard categorization of complaints should include certification elements as well as service related elements * User complaints within the scope of the certification criteria or testing process should be the priority, however, complaints about problems beyond the scope of certification, such as poor customer service, should be logged and counted, (additional action by the ACBs or ONC may not be warranted). |
| **3. Open Data Certified Health IT Product List (CHPL) Page #288** |
| In the initial rulemaking that we used to establish the Temporary Certification Program, we indicated that the National Coordinator intended to make a master CHPL of all Complete EHRs and EHR Modules tested and certified by ONC-ATCBs available on the ONC Web site and that the CHPL would be a public service and would be a single, aggregate source of all the certified product information ONC–ATCBs provide to the National Coordinator (75 FR 36170). Since 2010, we have maintained the CHPL and as the ONC Health IT Certification Program has matured, ONC-ACBs have continued to report the products and information about the products they have certified to ONC for listing on the CHPL. (Continued on page #289) |
| The workgroup is supportive of ONC’s open data initiative. Opening the CHPL up to further public consumption will help the industry and health IT consumers compare and contrast products—leading to better design and enhanced competition. It may also open up innovation with assistive apps that make use of that data. There is a need for more clarity on the API functionality mentioned on pg. 290. Will the ACBs use this feature to upload data onto the CHPL or is it intended for download only?   * Developers/Vendors at ATL/ACBs should know at program launch what the open data elements are and how defined. * Note that ATLs/ACBs maintain contracts with their customers with confidentiality provisions—they may encounter proprietary information in the course of their inspections. Defining what is “open” up front simplifies liabilities for all. * The work group believes that additional data element should be required in the open data file as an important step in transparency and consumer choice. * Listing the number of times the same version of health IT has been tested * The facility where the testing took place. * Audit of the CHPL data by ACBs for completeness of submission |

| **6. Adaptations and Updates of Certified Health IT Page #296** |
| --- |
| We propose a new principle of proper conduct (PoPC) that would serve to benefit ONCACBs as well as all stakeholders interested in the ONC Health IT Certification Program and the health IT certified under the program. We propose to require that ONC-ACBs obtain monthly reports from health IT developers regarding their certified health IT. Specifically, we propose to  require that ONC-ACBs obtain a record of all adaptations and updates, including changes to user-facing aspects, made to certified health IT (i.e., Complete EHRs and certified Health IT Modules), on a monthly basis each calendar year. We request comment on whether we should require even more frequent reporting. (Continued on page #296) |
| The workgroup is supportive of the new principle of proper conduct (PoPC) and believe this will help provide routinely updated information to ACBs on the status and progress of health IT as it improves. The group further believes that this will provide important information to alert ACBs to irregular events (e.g., multiple updates in a short period of time / few updates over a number of months) that may warrant in-the-field surveillance or further attention.   * Distinctions between “minor” and “major” changes need definitions. These methods should be documented in a protocol that all ATL/ACBs follow. * The developer/vendor community varies tremendously in their development cycles and how they count “updates” or “version revs”. Some developers issue patches/updates almost daily. Other shops have a philosophy where there is no version number change until the next major release. A method for understanding how this variability impacts the utility of the data and comparisons should be identified and piloted prior to mandating a count of changes. * There may be situations where health IT vendors make small, inconsequential changes to software code - these may or may not need to be reported and could add undue burden on health IT vendors. * Specific instances where health IT products are deployed in the field and software changes are made for only one site or installation- would these specific adjustments be included in the requirement to submit multiple reports? (for each site where different “tweaks” of health IT products are in place?) |

| **E. “Decertification” of Health IT – Request for Comment Page #298** |
| --- |
| In the explanatory statement250 accompanying Public Law 113-235 (Consolidated and Further Continuing Appropriations Act, 2015) the Congress urged ONC to use its certification program to ensure certified electronic health record technology (CEHRT) provides value to eligible hospitals, eligible providers and taxpayers. It also stated that ONC should use its authority to certify only those products that clearly meet current meaningful use program standards and that do not block health information exchange. Further, it stated that ONC should take steps to “decertify” products that proactively block the sharing of information. (Continued on page #298) |
| The group is aware and appreciates that ONC has been instructed by Congress to report on products that may be blocking interoperability and to take steps to decertify them. The group is in agreement that this concept requires further consideration and additional rulemaking primarily because this action of decertification would raise real concerns for all stakeholders. There would almost certainly be unintended consequences resulting from this approach.  Concerns discussed included:   * Concern for end users who are using a vendor’s system only to find they are not able to comply with the CMS EHR incentive program because their EHR becomes newly de-certified. * In cases where the de-certification leads to a vendor’s business failure or abandonment of a product. And in cases where patient data lies on vendor-controlled servers, there needs to be provisions to preserve or archive these data for future use. * Burden on providers who must then spend additional time and funds to purchase and deploy a new EHR or who must now accept a CMS penalty because they are unable to purchase and deploy a new EHR. * Other alternatives should be considered in light of the impact decertification would have on all stakeholders. Not only would vendors, hospitals, providers be impacted but also patients would likely experience disruptions. * Information on the process and planning for consequences would need to be outlined before the workgroup could support including this element. (ACBs already have the authority to terminate a product’s certification but this new measure may increase the likelihood of decertification; In a situation where a health IT product is marked for decertification there should be consideration regarding the circumstances (e.g., in-the-field surveillance repercussions), due process, and associated remedies e.g. a correction plan process). * The group strongly believes that the decertification process would need to be very well thought out in terms of violations, process, review, appeal, notification and a myriad of other possible effects – many of which could be more harmful in the big picture. (Patients unable to retrieve data, specialists unable to share records, etc.). * There is no generally accepted definition of data blocking. What objective information would be used to objectively determine an entity is blocking information?   The work group acknowledges and is supportive of value of certification in meeting standards and efficacy of EHRs. The work group would like to increase the emphasis on current regulations that states the expectation that vendors will be transparent in their requirements/contractual terms and will make info available publically, openly portable and transportable, as well as the proposal to enhance the information available on the CHPL site addressed in previous comments. |