American Hospital Association

Liberty Place, Suite 700
325 Seventh Street, NW
Washington, DC 20004-2802
(202) 638-1100 Phone
www.aha.org

March 15, 2010

David Blumenthal, MD, MPP
National Coordinator for Health Information Technology
Department of Health and Human Services

[Submitted electronically]

Re: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology (Ref: Rin 0991-AB58)

Dear Dr. Blumenthal:

On behalf of our more than 5,000 member hospitals, health systems and other health care organizations, and our 40,000 individual members, the American Hospital Association (AHA) appreciates the opportunity to comment on the interim final rule (IFR) specifying the initial set of standards, implementation specifications and certification criteria for electronic health record (EHR) technology published in the January 13, 2010 *Federal Register* (*Federal Register* Vol. 75, No. 8, p. 2013).

America's hospitals seek to move toward an e-enabled health care system where all hospitals meaningfully use EHRs to improve patient care and safety and achieve national goals for improved health. They share the administration's vision of a health care system where widespread use of interoperable EHRs supports improved clinical care, better coordination of care, fully informed and engaged patients, and improved public health. They also work every day to ensure adequate privacy and security for patients and their personal health information.

The AHA and its member hospitals have participated in development of health information technology (IT) standards for many years. The AHA was a founding member of the National Alliance for Health Information Technology (NAHIT), which brought together a diverse set of stakeholders from across the health care spectrum to address standards issues. The movement toward standards adoption and greater interoperability will facilitate the ease of sharing health information so that clinicians and patients have the information they need to provide treatment and promote health, in the form and at the time they need it.

The AHA greatly appreciates the hard work that the Office of the National Coordinator for Health Information Technology (ONC) has put into developing the IFR. We also appreciate the close coordination by ONC and the Centers for Medicare and & Medicaid Services (CMS) to ensure that the certification criteria and standards correspond to the meaningful use criteria that will be established under the Medicare and Medicaid EHR incentive programs.

This comment letter addresses issues of concern to our members as they seek to implement certified EHR technology and meet CMS' requirements for meaningful use. In it, we echo many comments also submitted by the College of Healthcare Information Management Executives (CHIME). CHIME represents chief information officers (CIOs) and other health information management executives who will bear responsibility for implementing EHRs in hospitals across the country.

Our comments first address how certification of EHR technology can best support providers as they work to meet the meaningful use definition. We then turn to specific recommendations on implementation issues and the need to clarify how certification policy should apply to the complex EHR systems deployed by most hospitals and some eligible professionals. In addition, we make a number of recommendations to align the certification criteria with our comments to CMS on the Notice of Proposed Rule Making (NPRM) for the Medicare and Medicaid EHR incentive programs. We close by examining the specific certification criteria and the proposed privacy and security standards.

CERTIFICATION FOR MEANINGFUL USE

The primary purpose of certification is to give health care providers a degree of assurance that the health IT, and in particular EHR technology products, they purchase will perform as promised. That is, certification is meant to support providers in achieving meaningful use. Certification is not intended to impose an additional burden on providers.

Scope of Responsibility. **In this vein, the AHA believes that there needs to be a clear distinction between the responsibilities of health care providers and the responsibilities of vendors of health IT products.** Health care providers have rightfully been asked to take the lion's share of responsibility for meaningfully using EHR systems and supporting technologies. Vendors of health IT products must ensure that their EHR systems meet the certification criteria to support meaningful use. This segmentation of responsibility – providers responsible for meaningful use of EHRs and vendors responsible for development and certification of products – builds on past experience in the health care IT space and provides a platform for efficient adoption of health care IT going forward. Certification policy should actively reinforce this division of responsibility.

Implementation Timelines. **In addition, rational timelines are needed. We recommend a lead time of one year between finalization of the certification criteria and certification of vendor systems. Providers need an additional two years between the time when certified products are available in the market and when providers nationwide are expected to implement and begin using them to meet the meaningful use criteria.** Because of the lead time needed to implement complex EHR systems, change workflows and train staff, it will become increasingly important for vendor development of products – and the certification of those products – to be achieved in advance of the deadlines to which providers are expected to be held responsible under regulations that will specify meaningful use requirements. Insufficient lead time for implementation, product development and certification places an unfair burden on hospitals and eligible professionals, raising implementation costs and potentially jeopardizing patient safety.

While the timelines established in the *American Recovery and Reinvestment Act of 2009* (ARRA) make it difficult for the first round of certification criteria to be established well in advance of the date by which providers must use certified products, the future timelines must be more rational, orderly, and predictable. We recommend that, in the future, new certification criteria be finalized at least three years before providers are expected to be using the new functionality covered by those certification criteria. For example, if providers are expected to submit data to a personal health record in 2015, certified products that support providers in meeting that objective should be available in 2013. To provide vendors sufficient to develop products that meet certification criteria, those criteria should be established by at least 2012.

Without this transition time, providers across the country will be implementing continually "beta test" versions of EHR products and vendors will struggle to simultaneously install and upgrade products for all of the nation's hospitals and physicians. Market constraints, including insufficient vendor capacity and existing workforce shortages, limit the level of demand that can be met at one time. Tight deadlines and high levels of demand also can create conditions that raise the price of products, installations, and consulting services. As detailed in our comment letter to CMS, our members are already experiencing these market distortions in contracting for and installing EHRs.

We also note that market stability would be best served by having the long-term vision established today. Laying out the full requirements for meaningful use will allow vendors to "build it once" and afford providers the opportunity to plan ahead and install new functionalities at a pace that makes sense for their institutions. Changes to certification criteria that recognize developments in standards harmonization are to be expected, and welcomed. However, a continual two-year change process that requires simultaneous, nation-wide implementation of new functionalities risks institutionalizing the difficult market effects noted above.

To address the tight timelines established in the ARRA, the AHA recommended that CMS adopt a "grandfathering provision" under which existing systems that hospitals use to meet meaningful use objectives could be accepted as "certified" for a period of three years. All upgrades to existing systems or deployment of new systems, however, would be required to be certified under the new federal process. **We urge ONC to provide technical support to CMS in crafting a "grandfathering provision" for currently installed systems that allow providers to meet the final meaningful use criteria.**

IMPLEMENTATION ISSUES

The definitions of EHR technologies in the IFR provide a good framework for discussing certification, but do not encompass the real complexity of EHR systems deployed in hospitals. The hospital field seeks clarity on what pieces of its EHR system need certification and clear statements that common practices will not lead to a need for additional or separate certifications.

To that end, we agree with the statement in the IFR that "we are not requiring the certification of combinations of certified EHR Modules, just that the individual EHR Modules combined have each been certified to all applicable certification criteria in order for such a 'combination' to meet the definition of Certified EHR Technology."

The AHA recommends that ONC add clarifying language to this statement that:

- **States that in order to meet the certification requirements, a hospital only need to attest that its EHR system (either modules or a complete EHR) includes pieces that have been certified against the meaningful use objectives it must meet;**
- **Acknowledges that a hospital's EHR system (whether comprised of EHR modules or a complete EHR) may also include auxiliary components and feeder systems that are used to meet meaningful use objectives but do not need separate certification;**
- **Recognizes that hospitals will install interfaces and other programs to connect EHR modules, complete EHRs and supporting IT systems that do not need to be certified;**
- **Recognizes that hospitals may customize and make modifications to EHR technology that was certified by a vendor without needing additional certifications; and**
- **States that hospitals will not be held responsible for having certified EHR modules for functionalities that no vendors support.**

To be eligible for incentive payments, providers must use certified EHR technology. The IFR provides a multi-stage definition of "certified EHR technology" to mean:

> A Complete EHR or a combination of EHR Modules, each of which 1) meets the requirements included in the [statutory] definition of a Qualified EHR and 2) has been tested and certified in accordance with the certification program established by the National Coordinator as having met all application certification criteria adopted by the Secretary.

The IFR specifies that a "Complete EHR" has been developed to meet all of the applicable certification criteria adopted by the Secretary of the Department of Health and Human Services (HHS), while a combination of "EHR Modules" can be "any service, component, or combination thereof that can meet the requirements of at least one" of the certification criteria adopted by the Secretary. The IFR further states that providers who choose to combine multiple EHR modules must ensure that the modules work together and that, together, they meet all of the certification criteria.

However, many hospitals do not use a single EHR system. Instead, they may integrate different systems from a number of vendors. Even those facilities that install a main enterprise system routinely supplement it with other products meant to achieve specific needs, such as department-specific systems for surgery or the radiology department. They also may have a clinical data repository, or separate systems for infection control or oncology. One AHA member that supports the EHR infrastructure for dozens of hospitals notes that its facilities use what many would consider a single enterprise system, or Complete EHR, but wrap about 200 separate products around the core system to deliver all of the functionality needed to support advanced clinical IT systems and information exchange. **We do not believe that it is in the best interest of hospitals – nor the government – to require that all best-of-breed systems, or those that combine a base system with add-on components, conduct a separate, on-site certification.**

In addition to products from vendors, many hospitals also write custom programs to generate specific reports or provide specific decision support functions, including, for instance, evidence-based order sets derived by clinical staff. Certification requirements also must take into account the fact that some health care organizations that purchase certain vendor products are given access to the code underlying software applications, and then slightly change the code to adapt it to their circumstances. Such customization does not materially affect the underlying product and its capabilities, and provisions must be made to enable providers to make modifications in code without requiring re-certification of products. Such modifications should not be confused with self-development of applications, where providers create specific applications from scratch to meet their organizations' purposes.

It also is possible that, with providers using EHR modules as components of their EHR systems, there may be some meaningful use objectives for which no vendors may seek certification of their products. In that event, providers should not be held accountable for seeking certification of those modules.

Given the array of programs that comprise a hospital's EHR system, ensuring that the system is certified against all of the meaningful use objectives will be a challenging exercise, particularly during the next two to three years, as EHR vendors certify products and work with customers to upgrade existing systems and/or install new systems.

This complexity and transition to a new regulatory structure begs many questions. For example, clarity is needed around whether:

- An organization's clinical data repository needs to be certified.
- A laboratory system needs to be certified if an organization reports laboratory data to public health entities via an EHR.
- An organization can generate quality reports using modules that are not certified if it reports the data to CMS via a system that is.
- An organization is required to certify all 50 (or 100, or 200) products that it uses.
- Recertification is needed if an organization customizes a product that previously was certified by a vendor.

We believe that our recommended clarifying language presented above will help create a simple and clear approach to certification of complex systems. In addition, hospitals and eligible professionals will need clarification from agencies administering this program in order to fully understand the certification requirements. **To that end, we encourage ONC to work with CMS to provide clear guidance that establishes minimum requirements for demonstrating that a hospital EHR is certified. Given that this is a new, permanent part of the Medicare program, these requirements should be subject to notice and comment. We note that hospitals will submit attestations to CMS about their certification status, which conveys a legal compliance burden that could result in significant penalties if hospitals and enforcement agencies have differing understandings of the specific requirements.**

MODIFICATIONS TO THE CERTIFICATION CRITERIA TO CONFORM WITH AHA COMMENTS TO CMS

We appreciate the close collaboration between the ONC and CMS in producing two related health IT rules – the CMS proposed rule on meaningful use criteria and the ONC interim final rule on certification. In particular, the certification criteria in the IFR closely track the proposed meaningful use objectives.

The AHA made a number of recommendations to modify the proposed meaningful use objectives, as you will note in the attached copy of the comments we submitted to CMS, and as we describe below. We remain hopeful that CMS will respond to our comments by making significant changes in the meaningful use criteria and other related policies. If CMS makes changes to the criteria, corresponding changes would need to be made to the IFR.

The AHA urges ONC to take all necessary regulatory steps (including publishing a final rule or, if necessary, a second interim final rule) to make such changes as expeditiously as possible. EHR vendors and open source developers need as much lead time as possible to bring certifiable products to market.

We believe it would be a serious mistake to defer publication of a final rule, so as to leave the interim final rule in place, or to fail to make sufficient changes to the interim final rule in response to stakeholder comments.

Certification of ability to generate of health IT functionality measures. **ONC should include certification criteria for the generation of the health IT functionality measures in the final meaningful use rule from CMS that require a percentage or numeric response using data from the EHR. When certifying modular EHR products, certification would only require generation of the associated measure.**

The certification criteria included in the final rule should explicitly specify that certified EHR technology must be capable of performing the calculations and generating all numeric health IT functionality measures required to demonstrate meaningful use of the technology. CMS states in its NPRM (p. 1903), that the agency does "not believe that demonstration of meaningful use should require use of certified EHR technology beyond the capabilities certified" through the federal certification process.

In Attachment B of our comment letter to CMS, the AHA made specific recommendations on ways to re-specify measures so that they can be reported from the EHR (including, for example, alternative measures for computerized provider order entry and incorporation of clinical lab-test results into the EHR as structured data).

Without automated measure generation, we are concerned that EHR users will be left in the illogical position of conducting burdensome manual activities to prove that they have become meaningful users of electronic technology.

Certification of new objectives recommended by the AHA. **ONC should include certification criteria for all new objectives included in CMS' final rule on the EHR incentive programs.**

The AHA's comments to CMS also include a recommendation to expand the meaningful use criteria for hospitals to encompass 12 objectives recommended by the HIT Policy Committee for 2013 or 2015. Attachment A of our letter includes descriptions and measures for those recommended additional objectives. We also note that many of these additional objectives are foundational components of an inpatient EHR that have been included as certification criteria under the CCHIT Inpatient EHR Certification**.**

Removal of certification criteria for administrative transactions. **The AHA recommends that ONC remove the certification criteria related to electronic claims submission and electronic insurance eligibility verification from the IFR.** We also recommended removal of these criteria in our comments to CMS.

These administrative activities already are addressed under the HIPAA Administrative Procedures regulations and overseen by CMS. Hospitals already face a financial penalty for submitting paper claims. These electronic activities are undertaken through existing claims processing systems, which almost always are integrated with clinical EHR systems, although they are rarely part of the EHR installation.

Including billing activities in the meaningful use objectives would require hospitals to upgrade existing functional billing systems to new products that have been certified through the federal EHR certification process. This would create unnecessary work and expense and take hospital IT staff away from implementation of the clinical systems that are at the heart of meaningful use. There is no apparent benefit to this requirement.

ADDITIONAL COMMENTS ON CERTIFICATION CRITERIA AND STANDARDS

Concern over certification criteria for medication reconciliation. **To avoid potential safety concerns, the AHA recommends changing the certification criteria for medication reconciliation to read: "Display simultaneously two or more medication lists and provide tools for the clinician to perform medication reconciliation that will result in a single list."**

The criteria, as written, read: "Electronically complete medication reconciliation of two or more medication lists (compare and merge) into a single medication list that can be electronically displayed in real time."

Medication reconciliation is not just about comparing and merging. It requires an intelligent look at the medication list for potential drug-drug interactions, duplicative medications with similar indications and effects but different names, and other such problems. A merged list can be problematic in practice because it automates a process, but may not have the capability to apply all of the relevant clinical logic. Automated systems can and should support medication reconciliation by clinicians, but should not merge lists without clinical input.

Support for a single standard for patient summary records. **The AHA urges ONC to adopt a single standard for patient summary records, the HL7 CDA CCD.**

The IFR allows use of either the Health Level Seven (HL7) Clinical Document Architecture (CDA) Release 2 (R2) Level 2 Continuity of Care Document (CCD) or the ASTM CCR to electronically exchange a patient summary record. We disagree with this approach and believe that the sharing of health information across providers is best facilitated with adoption of a single standard for patient summary records. The CCD is a more robust standard that is also much easier for a person to ready natively. The health care field is ready to transition to a single standard for patient summary records, and such a move will facilitate interoperability in a more timely fashion.

Certification criteria for quality reporting. **The proposed quality measures are not yet ready for automated reporting, but when they are, vendors should be certified based in part on their system's ability to accurately and reliably collect and report these data. At a minimum, the first certification criterion under quality reporting should read: "1. ACCURATELY calculate and electronically display quality measure results as specified by CMS or states."**

While reporting on clinical quality measures through certified EHR technology may sound like a straightforward task, it is not. Each measure is created by collecting many different data elements from relevant patient records. These elements are used to determine whether the patient should or should not have received the test, medication or treatment being measured, and then to determine if the patient did receive it.

The measures currently are specified so that a well-trained and knowledgeable clinician or medical record abstractor can cull relevant data elements from wherever they may be embedded in a patients' hospital record. With few exceptions, they have not been specified in such a way that the necessary data elements can be consistently and accurately collected from an electronic record where the clinical judgment of a well-trained abstractor does not enter into the decisions. When such re-specification has been completed, the new specifications must be tested to ensure the accurate and reliable collection of the data. This testing has been done with the current manual specifications used by hospitals across the country, and in virtually every case, important lessons were learned during the testing phase and the specifications were altered to ensure the data collection would produce the most accurate results possible. This crucial testing step should not be left out of the e-collection process.

Since the measures have not been e-specified, except for the measures of stroke and venous thromboembolism that CMS contracted to have re-specified, it would be impossible for any vendor to have embedded appropriate specifications in their EHR product at this point. But once the specifications are available, the testing of this function should be completed as part of the certification process to ensure that data collection is performed by the system accurately. Each hospital should not have to learn after the product has been purchased and installed that the claims made about the product's ability to collect and report these data are wrong. And since these data are publicly reported to assist patients and their families in making decisions about where to go for care, the federal government should ensure through the certification process that the products are capable of generating accurate data. This can be done through the use of "dummy datasets" that test whether vendor products generate the expected values for various quality metrics or other tests of reliability and validity.

Quality reporting standards and implementation specifications. **Due to the lack of appropriate e-specifications for hospital quality measures, the AHA recommended that CMS delay quality reporting as an objective of meaningful use until 2012 or later.** Further, there appears to be a great deal of confusion about which architectures are appropriate for and able to be used for hospital data collection.

Automated quality reporting is an important function of the meaningful use of electronic health records. However, development of "e-measures" is really just getting started. Most of the measures proposed by CMS have not yet been specified for automated collection.

ONC has adopted the CMS Physician Quality Reporting Initiative (PQRI) 2008 Registry XML Specification (and the related implementation specifications, the PQRI Measure Specifications Manual for Claims and Registry) as a standard for quality reporting. However, PQRI is a physician quality reporting program and hospitals have been reporting performance data through an entirely different system, with different data specifications and conventions. **There has been no test of whether this standard will work for reporting hospital data, but since the systems are so different, it is hard to imagine that it will work without modification.**

There is an HL7 draft standard for trial use (DSTU) called "Quality Report Document Architecture" (QRDA) that allows for quality reporting on 3 levels, (1) a single patient data set for a single measure, (2) an aggregate set of data from multiple patients for the same measure / measure set, and (3) a summary report of # in numerator, # in denominator, #exclusions, and calculated result. This standard, however, has not had a lot of use and has not yet been balloted for all three levels.

We do not believe that either recommended system can be judged appropriate for hospital data collection unless tested. Since the interim final rule provides no assurance that the PQRI-related standard and implementation specifications would work in a hospital setting, **we ask that ONC review this issue in collaboration with CMS and in the context of the ongoing pilot of reporting hospital quality measures from EHRs.**

There already are standards for the electronic collection of the hospital quality data. They are in use currently by every hospital data vendor that submits data to the Iowa Foundation for Medical Care (IFMC) and to The Joint Commission. They have the advantage of being in wide use and having been tested over several years. This does not make them perfect, but it does make them feasible. IFMC and the largest hospital data vendors should be consulted for their advice and recommendation on how to make the electronic data collection system work. In addition, it may be that the core measures vendors have an important role to play in actually generating measure data for reporting based on data from provider EHRs.

<u>Standard for reporting to public health agencies</u>. **The AHA believes that it would be preferable to defer adoption of a standard for reporting to public agencies until a single, national standard is feasible.**

For the vocabulary standard for submitting data to public health agencies for surveillance or reporting, ONC adopts as a standard, "According to applicable public health agency requirements." We are concerned that this could be problematic for hospital systems

with facilities in two or more states, as their EHR technology would have to meet whatever standards each state elects to use.

PRIVACY AND SECURITY STANDARDS

Privacy/security certification in the EHR module approach. **The AHA recommends that the IFR be revised to specify that, for EHR modules submitted for certification, each privacy and security certification criteria shall be deemed "addressable" in the sense that certain implementation specifications in the HIPAA Security Rule are addressable.**

This approach would require that for each addressable criterion, each EHR module submitted for certification would need to either include that capability or provide an explanation of why the criterion is not relevant to the module's EHR functionality and the context of its purpose and operation. Additionally, the definition of "certified EHR technology" should be revised to designate more clearly that a complete EHR or a set of EHR modules, either of which meets the requirements included in the definition of a qualified EHR is "certified EHR technology. The recently released NPRM outlining the certification process may offer a more appropriate regulatory forum for addressing security functionality questions that the module approach used in this rule has created, and the AHA anticipates offering further suggestions on that rulemaking to ensure that questions related to the integration of security functionality are appropriately answered.

The IFR provides for the certification of EHR modules as well as complete EHRs. An EHR module is defined in section 170.102 of the rule as "any service, component or combination thereof that can meet the requirements of at least one certification criterion adopted by the Secretary." The EHR module approach raises questions about how an integrated set of modules will work together to provide the core capabilities related to privacy and security that cross-cut an EHR system of an organization and, therefore, how eligible hospitals and professionals can be assured that their certified EHR technology when it is assembled from these multiple modules "may assist . . . to improve their overall approach to privacy and security."

Since the current definition requires that an EHR module meet only one certification criterion, it would seem that a hardware or software product designed specifically to provide an EHR-specific functionality that includes no security capabilities could be an EHR module. In addition, a hardware or software product whose sole purpose is to meet a single security criterion like encryption and decryption might be an EHR module. Under the interim final rule, however, combinations of EHR modules used together are not required to be certified together and it is the clear responsibility of the eligible hospital or professional to assure that the selected modules will work together.

Certification under these circumstances ignores the complexities of security integration and the importance of assuring that security policy can be enforced consistently across all

of the integrated modules. Such certification provides no guarantee to eligible hospitals and professionals that any specific combination of modules will be sufficient to assist them in improving their overall approach to privacy and security and offers no assurance that any module designed solely to provide security functionality will integrate and work effectively with any specific or combination of modules providing EHR-related functionality. The IFR further complicates the process by including a definition of "certified EHR technology" in section 170.102 that seemingly contemplates that only "complete EHRs" or a "combination of EHR modules" (as a whole) can be certified.

Security and privacy functionality, however, is a cross-cutting set of requirements that can only be evaluated as a complete system. In some cases, a module may rely on its environment to provide the necessary security functionality while in other cases a module may offer some specific security functionality while leveraging the general EHR platform to provide more broad-based security functions. A requirement that each module meet all of the security criteria would introduce unnecessary complexity and may not guarantee – or might inhibit – integration necessary to achieve uniform level of security enforcement throughout the organization's EHR system. On the other hand, a requirement that only some EHR modules provide the security related functionality without assuring that the other EHR modules selected would use – and not undermine – this security functionality does not guarantee effective security protection within the organization's EHR system.

Accounting of disclosures for treatment, payment and health care operations. **The AHA recommends that the certification criteria and standard for the accounting of disclosures be delayed at least until the updated rule for accounting of disclosures is issued by the HHS Secretary to ensure that these technical specifications are appropriately harmonized with the specific obligations that the forthcoming accounting of disclosures rule establishes.** Note that the HIT Policy Committee does not include the objective of providing patients with an accounting of disclosures for treatment, payment and health care operations until 2015.

The IFR requires that certified EHR technology have the capability to "record disclosures for treatment, payment and health care operations" (section 170.302(v)). Specifically, certified EHR technology must be capable of recording the date, time, patient and user identification and a description of the disclosure (section 170.210(e)). However, the rule establishing the obligation for covered entities to provide such accounting and outlining the related implementation specifications is not required by statute to be released until June 2010. In addition, the HHS Secretary has the option to delay implementation of this rule until 2013.

The AHA also believes that it is important to understand that the electronic capture of data elements per se does not equate to the direct generation of an accounting of disclosures report that can be read and understood by a patient. The electronic data must be "translated" for human consumption, which requires resources and considerable time from dedicated staff with specific knowledge and skill to decipher and process machine readable data and generate an individualized report that can be provided to a patient.

Accounting of disclosures reports are likely to be created not through real-time event processing, but rather through post-event analysis of stored information retrieved from the system. Thus, it is important that the capabilities of an EHR system allow for the generation of the accounting of disclosures after the fact rather than in real time, minimizing the need for real time recording of events and lessening the real-time processing burdens on the EHR system. Therefore, we recommend that, when ONC includes the accounting of disclosures certification criterion in its future rulemaking, it be revised to read: "create a record of disclosures of treatment, payment and health care operations." Accordingly, the related certification standard should read: "create a record of disclosures of treatment, payment and health care operations" that appropriately includes only data elements specified in the accounting of disclosures rule as finalized by the Secretary of HHS.

Timely electronic access to information by patients. **The rule should be revised to ensure that EHR technology includes the capacity for a user to provide patients with electronic access to their health information and to provide a copy of the patient's personal health information in electronic format.**

The IFR specifies that certified EHR technology must be capable of providing patients with online access to their clinical information, including at a minimum lab test results, problem list, medication list, medication allergy list, immunizations and procedures (section 170.304(g)). However, requiring capabilities for "online access" by patients to their clinical information would seem to be insufficient to meet the meaningful use objective of providing patients with timely access to their health information. To the extent that online access means that patients have the ability to view their medical information but not the ability to print, download or copy the information, the requirement falls short of what HIPAA and HITECH provide. HIPAA gives consumers the right to access or obtain a copy their own PHI and HITECH provides a right to obtain an electronic copy and to request that an electronic copy be sent to a designated person or entity.

On the other hand, if online access means that the patient would have real-time access to the same record used by a provider, then the requirement exceeds what is required by HIPAA and HITECH. HIPAA currently provides a 30-day window with the possibility of a one-time 30-day extension for covered entities to provide patients with a copy of their medical information. It is important that ONC's requirement be consistent with the provisions and implementation specification in the HIPAA rule related to patients' rights to access their medical information as well as with any provisions and implementation specification HHS develops to implement HITECH's requirements related to a patient's rights to an electronic copy of his or her personal health information which are expected as part of a forthcoming rule from HHS. Thus, we urge ONC to coordinate with the Office for Civil Rights' rulemaking in finalizing this criterion.

Certified EHR Encryption and Hashing Criteria. **ONC should expressly clarify that the encryption and hashing standards contained within the IFR do not impose any**

obligations upon HIPAA-covered entities beyond that which is already required by the HIPAA Security Rule (45 C.F.R. Part 164, Subpart C).

We support ONC's goal of ensuring that certified electronic health records be capable of providing robust encryption and hashing functionality. Moreover, we appreciate ONC's acknowledgement that the IFR is not intended to impose any obligations upon covered entities beyond the provisions of the HIPAA Privacy and Security Rules. Nonetheless, we are concerned that the current phrasing of the IFR is not sufficiently clear with regard to the implications of the encryption and hashing capability requirements for certified electronic health records upon the operating practices of covered entities that adopt such tools.

For good reason, encryption and integrity controls are addressable, not required, implementation specifications under the HIPAA Security Rule. (*See* 45 C.F.R. §§ 164.312(a)(2)(iv), 164.312(c)(2), and 164.312(e)(2)(i)-(ii).) While these are valuable tools for safeguarding sensitive information, there are several circumstances in which the marginal increase in security provided by such measures is outweighed by the resulting financial and operational costs. Accordingly, a covered entity may justifiably conclude that encryption and/or hashing are not reasonable and appropriate in a given circumstance and instead adopt reasonable and appropriate alternative safeguards. For example, protected health information (PHI) at rest within secured networks is commonly maintained in unencrypted form in order to manage financial costs and facilitate ready access for authorized users to perform legitimate tasks, such as providing patient care.

The complications associated with encryption and hashing are numerous. While the encryption or hashing of any one data record typically results in only a marginal increase in file size, when applied over the number of records containing PHI stored within the network of a hospital, the total increase in file size can be substantial. This increase in total file size results in significant financial costs because it requires the acquisition and maintenance of additional servers and related hardware. This also increases energy costs for powering the additional equipment as well as maintaining appropriate environmental conditions (such as temperature and humidity levels) for data center equipment. Furthermore, such increases in file size magnify the financial costs and time needed to back up records containing PHI.

Encrypting and/or hashing data records can impose a notable impact upon the performance of information systems. For health care providers, this may interfere with the ability to provide medical treatment in an expeditious fashion. Time taken to decrypt PHI, that is otherwise protected by comprehensive network security safeguards, could result in critical delays during sensitive medical treatments. Moreover, the increased performance demands of frequent encryption and decryption, or hashing, could increase the likelihood of system breakdowns that may threaten the availability of PHI for many authorized users; this could have significant implications for a hospital's ability to provide urgent medical care.

Accordingly, it is a commonly accepted practice to maintain records within secured, network perimeters in an unencrypted state. For example, control SC-28 of the Recommended Security Controls for Federal Information Systems and Organizations does not recommend encryption for unclassified sensitive data at rest within an organizational information system. (*See* NIST Special Publication 800-53 (August 2009) at p. F-120.) Alternative safeguards such as firewalls, network demilitarized zones, rigorously enforced access control procedures, network activity monitoring, and location of network equipment within physically and environmentally secured facilities provide reasonable and appropriate protection for PHI at rest within the network infrastructure of covered entities.

Finally, we appreciate ONC's stated goal of using the encryption and hashing capability criteria for certified electronic health records as a method to encourage health IT vendors to make encryption and hashing functionality more commonly available in their products. *See* 75 F.R. 2034 (January 13, 2010). One of the primary historical limitations on the adoption of encryption and hashing procedures by covered entities has been the scarcity of such features in commonly available health information technology. However, there are other factors limiting the adoption of encryption and hashing technology among covered entities. These factors include, but are not limited to:

- The financial and time costs of acquiring and implementing network infrastructure (e.g., servers and related collateral) necessary to handle the increased performance demands of continuous encryption, decryption and hashing;
- Research, development and production lead time necessary for manufacturers of specialized medical diagnostic and treatment systems to introduce new products capable of handling continuous encryption, decryption and hashing; and
- The technological challenges posed by attempting to integrate such complex functionality into small devices with limited memory, power, and processing capacity (e.g., portable end-user devices, such as PDAs and other handheld devices, as well as implantable medical devices).

Therefore, we caution ONC not to presume that encouraging greater availability of encryption functionality within certified electronic health records will lead to a dramatic increase in encryption of data by covered entities in the immediately foreseeable future. The aforementioned limits will likely continue to lead many covered entities to justifiably conclude that encryption, decryption, and/or hashing of PHI at rest within secured networks is still not a reasonable and appropriate safeguard.

For these reasons, we believe it is important for ONC to continue to acknowledge that the certification criteria for EHR technology impose requirements only upon the capabilities of certified EHRs, not upon the actual manner in which such tools should be used in practice. Reaffirmation that PHI maintained on secured networks need not be encrypted so long as a covered entity has met its obligations under the HIPAA Privacy and Security Rules to analyze its circumstances and establish reasonable and appropriate alternative

safeguards would provide substantial reassurance to covered entities. In addition, we urge ONC to maintain this approach with regard any future rulemakings concerning certified EHR technology.

Audit logs. **The AHA is concerned that the audit alerting criterion goes beyond what is required by HITECH and HIPAA and also exceeds the current capabilities of products in the market; therefore, we recommend that it be eliminated from the interim final rule.**

The IFR specifies that certified EHR technology must be capable of generating an audit log (section 170.302(r)(1)) by recording the date, time and the patient and user identification when electronic health information is created, modified, deleted or printed as well as an indication of which such action occurred (section 170.210(b)). It further requires that the technology "provide alerts based on user-defined events (section 170.302(r)(2))." Real-time alerting requires audit processing and decision support capabilities that most products currently do not provide. To provide this functionality across multiple EHR modules requires capabilities that do not exist today to merge audit records into a common data model and vocabulary for recording audit events. Further, the use of the phrase "based on user-defined events" in the criterion could easily be misinterpreted or misunderstood to extend beyond "entity-defined" events to include individual patient preferences.

America's hospitals are committed to moving toward an e-enabled health care system and share the vision of interoperable data exchange supported by standards-based EHR systems. We look forward to working with you and other federal partners to ensure that the new federal programs being installed to support the transition to widespread use of interoperable EHRs are effective and successful.

Thank you for the opportunity to share our concerns and comments. If you have any questions, please contact me or Don May, vice president for policy, at (202) 626-2356 or dmay@aha.org.

Sincerely,

Rick Pollack
Executive Vice President
Enclosure