March 4, 2010

David Blumenthal, MD, MPP
National Coordinator for Health Information Technology
U.S. Department of Health and Human Services
200 Independence Avenue, SW
Washington, DC 20201

Dear Dr. Blumenthal:

The HIT Standards Committee (HITSC) members identified and prioritized several recommendations on security of information and the privacy of consumers as detailed in 45 CFR Part 170, Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record (EHR) Technology.

The following recommendations were developed by the Privacy and Security Workgroup of the HITSC, refined by discussion with the full Committee, and adopted by the HITSC. The Privacy and Security Workgroup has reviewed the subject interim final rule (IFR) and is herein presenting to you our collective comments and recommendations for consideration. Should you or the ONC staff have any questions about these comments and recommendations, or needs for further clarification, please do not hesitate to contact us.

REVIEW PROCESS

To keep our review focused on identifying any significant issues that we believe should to be addressed even after the IFR's finalization date of February 12, we asked our workgroup members to respond to a set of questions relating to the overall approach, the adopted privacy and security certification criteria, the adopted privacy and security standards, and questions for which the IFR solicits responses from reviewers.

1. Is the general approach of certifying "EHR Modules" and "Complete EHRs" reasonable and implementable? Are the definitions reasonable?
2. Are the privacy and security certification criteria adopted (see Table 1, p 2028 and Regulation §170.302(o-v) on p 2046) reasonable and sufficient to adequately protect health information within the Stage 1 meaningful-use timeframe? Are any of these criteria insufficiently specific to be used to test and certify Complete EHRs or EHR Modules, with reasonable assurance that the technology will effectively support the delivery of health care as well as the achievement of Stage 1 meaningful use? (solicitation p 2029)
3. Are the privacy and security standards adopted (see Table 2B, p 2035 and Regulation §170.210(a-e) on p 2044) reasonable and sufficient to adequately protect electronic health information within the Stage 1 meaningful use timeframe?

4. Should the domain name service, directory access, and consistent time, or any other function or service, be reconsidered for inclusion as a required capability for Certified EHR Technology? (solicitation p 2035)
5. Is the functional standard adopted for accounting of disclosures for treatment, payment, and healthcare operations (see Table 2B, p 2035 and discussion on pp 2036-2037; and Regulation §170.210(e) on p 2044) reasonable and technically feasible? What is the technical feasibility of collecting other data elements, including reason for the disclosure and to whom the disclosure was made? (solicitation p 2037)
6. Do you perceive any gaps in the IFR with respect to privacy and security standards, implementation specifications, and certification criteria?

Our individual workgroup members conducted a thorough review of the IFR and provided detailed comments, which were consolidated and synthesized into the general and specific comments we offer herein.

GENERAL COMMENTS

Comment: We want to stress that to adequately protect the security of information and the privacy of consumers, EHR technology certification is only one consideration. The meaningful-use Notice of Proposed Rule Making (NPRM) stresses the importance of analyzing security and privacy risks – based upon the identified risks, enterprises must then adopt appropriate policies and practices essential to protecting information and creating trust. The HIT Policy Committee is defining security policies, and the ONC will be using a number of mechanisms to provide guidance and resources to support eligible professionals and hospitals in implementing appropriate policy, procedures, and technology to assure that health information is protected and consumers' privacy is preserved. As only one step in the process, we want to stress that EHR technology certification alone cannot address all of the necessary components of a strong framework of information and consumer protections.

In general, we are pleased with the approach the Rule has taken in specifying functional requirements instead of constraining choices to a single technology standard or several standards. This approach seems well suited for creating technology-neutral standards and for avoiding premature obsolescence of the rules. This approach undoubtedly will allow developers greater flexibility and opportunity for innovation.

At the same time, this approach creates some ambiguity that translates into risk, and in some cases could impede interoperability. The use of "e.g." in Table 2B of the Preamble makes good sense to us in that it anticipates evolving technology while at the same time provides developers some indication of standards that will be deemed acceptable for certification. We considered recommending that these examples be brought into the body of the Regulation as well. However, as technology continues to advance, even these examples are likely to change over time. So we concluded that the IFR authors' decision not to include the e.g.'s in the body of the Regulation is a sound one. We believe that the ongoing responsibility for providing developers such "example standards" that have been deemed acceptable for certification appropriately should lie with the certification program, since the body of certifiers will need to maintain proficiency in certifying the full range of compliant approaches and solutions. We recommend that as the ONC develops the certification program, it include in its planning a framework and processes for maintaining a current list of example acceptable technology standards that meet the Rule's functional standards and for establishing the process to actively and rapidly enable standards to advance in ways that are tied to implementation and use and not dependent on the pace of regulatory changes.

Recommendation: Incorporate into the ONC Strategic Framework and the EHR technology certification program a framework and processes for specifying and maintaining a current list of example technology standards that address the base level of functionality specified in the standards for EHR certification, and that meet the implementability criteria established by the Implementation Workgroup .

SPECIFIC COMMENTS AND RECOMMENDATIONS

Question 1: Certification of EHR Technology

Is the general approach of certifying "EHR Modules" and "Complete EHRs" reasonable and implementable? Are the definitions reasonable?

Comment: While we support the notion of certifying both "Complete EHRs" and "EHR modules" that can be integrated into a Complete EHR, such a modular approach presents challenges relating to how the integrated set of modules will work together to provide uniform enforcement of privacy and security policy across an enterprise – and how eligible professionals and hospitals can be assured that their "Certified EHR Technology" will enable them to meet the Health Insurance Portability and Accountability Act (HIPAA) privacy and security requirements. We assume that the forthcoming Notice of Proposed Rule Making (NPRM) will clarify how the modular approach will work, and we offer these comments as input into the development of that NPRM.

The IFR introduces the notion of certifying both "EHR Modules" and "Complete EHRs," though the definitions are a bit ambiguous. The definition of "EHR Module" (pp 2022 and 2043) implies that such a module can be independently certified, but the definition of "Certified EHR Technology" (pp 2022 and 2043) seems to suggest that only "Complete EHRs" or "combinations of EHR Modules"(as a whole) can be certified. We believe the intent is to "certify" Complete EHRs and individual EHR Modules, and then to offer reimbursement to eligible professionals and hospitals that use "Certified EHR Technology," which can be either a single certified Complete EHR or a set of EHR Modules, each of which has been certified and which together can achieve the meaningful-use objectives.

Aside from this apparent ambiguity, we see two primary issues relating to the certification of EHR Modules:

a) An EHR Module is required to meet only "one" certification criterion. This presents issues for both software and hardware components designed to provide an EHR function and for components designed specifically to provide security functions. For example, could a software/hardware product whose sole purpose was to encrypt and decrypt information (certification criterion 4 of the privacy/security objective) be certified as an "EHR Module" even though it had no EHR-specific attributes? Is HHS prepared to certify the vast array of security products that may be presented as "EHR Modules" because they meet one of the security certification criteria? On the other hand, can an EHR Module that enables a user to electronically record, store, retrieve, and manage ambulatory orders, but provides no security capabilities, be certified?

b) The IFR states that combinations of EHR Modules used together to achieve meaningful use are not required to be certified together (p 2023) and that the eligible professional/hospital is responsible for assuring that the selected modules will work together (p 2022). This is a necessary clarification because the combinatorial complexity of attempting to certify distinct combinations of modules creates a practicality impediment. However, assigning this responsibility to the eligible professional/hospital ignores the complexities of security integration and the need for assurance that security policy can be enforced consistently across all of the integrated modules. Security and privacy are cross-cutting sets of requirements and attributes implemented through policies and practices, and can only be evaluated across a complete system. The overall objective of assuring that privacy and security policies are enforced through technology and operational practices lies squarely at the system or entity level. However, if an enterprise's EHR technology is provided by a collection of certified EHR modules, the enterprise should be able to assume that each of these modules has been built to address the privacy and security certification criteria as they relate to the functional purposes and environment for which that module was designed. In some cases a module may rely on its environment to provide the necessary security functionality. In other cases, the module may need to take responsibility for some of the security functionality, such as audit logging, while leveraging the platform to provide more broad-based security functions, such as access control and secure communications.

The IFR is not clear regarding whether each EHR Module submitted for certification must meet all of the security certification criteria, or whether a given EHR Module submitted for certification can focus exclusively on the one or more healthcare criteria it purports to meet and ignore the security certification criteria (i.e., assume that some other EHR Modules will address those criteria). Requiring that each EHR Module meet all of the security criteria would introduce unnecessary complexity and could impede providing integrated protection wherein the privacy and security policies were uniformly enforced across the enterprise. But requiring only that "some" EHR Modules provide the required security functions, without gaining some level of assurance that the other EHR Modules would use (and not undermine) the security functions would not provide the security protection required. Ideally, one would want each security certification criterion (service) to be the responsibility of a single component – and every EHR Module would use that component to provide that service. Unfortunately, that may not be practical for Modules developed by different organizations.

Recommendations:

1) Assuming the intent is to certify Complete EHRs and individual EHR Modules, and not to collectively certify combinations of EHR modules, we recommend revising the definition of "Certified EHR Technology" to read "*Certified EHR Technology* means a Complete EHR, or a set of EHR Modules, either of which: (1) meets ..."

2) To address the security integration issues, we recommend that for EHR Modules submitted for certification, each privacy and security certification criterion be deemed "addressable" in the same sense that the implementation specifications in the HIPAA Security Rule are "addressable." This would require that for each "addressable" security certification criterion, each EHR Module submitted for certification would need to either 1) include the security capability (inherently or through the use of other components integrated with the Module), or 2) provide an explanation of why the criterion is not relevant to the healthcare functionality the Module provides and the context of its purpose and operation, and an explanation of how the security capability is addressed. Adapting the definition given in 45 CFR 164.306, an "addressable" certification criterion would be one for which an EHR Module developer must:
(1) Assess whether the certification criterion is a reasonable and appropriate safeguard in the environment for which the EHR Module is designed for use, when analyzed with reference to the

likely contribution the criterion will make to protecting the entity's electronic protected health information; and
(2) As applicable to the EHR Module —
(A) Implement the certification criterion within the EHR Module if reasonable and appropriate; or
(B) If implementing the certification criterion in the EHR Module is not reasonable and appropriate—
(1) Document why it would not be reasonable and appropriate to implement the certification criterion in the EHR Module; and
(2) Implement an equivalent alternative measure if reasonable and appropriate.

The Privacy and Security Workgroup, and its domain expert consultants, are seriously concerned that EHR Modules that are certified to provide specific healthcare functionality hold the potential to undermine the overall privacy and security policies of the eligible professional/hospital attempting to use it meaningfully. This is a real risk that needs to be recognized and effectively mitigated. We offer an example of how it might work within the normal software-development life cycle. Every software module is designed and specified for a specific set of use cases, and targeted at a specific set user profile. One need only examine a marketing brochure from any EHR product vendor to identify what those use cases are and the types of users and operational environments for which the product is designed. When designing an EHR Module, the developer would need to examine each security certification criterion and determine how it applies to that Module's use cases within the context of the targeted environments and user base, then decide how the criterion will be met for that Module. When submitting the EHR Module for certification, the developer would include documentation explaining the results of this exercise, including the applicability of each security criterion, the security functionality built into the Module, and how the Module integrates with external security services. (Note that this explanation should also be contained in user documentation distributed with the product.)

Question 2: Certification Criteria
Are the privacy and security certification criteria adopted (see Table 1, p 2028 and Regulation §170.302(o-v) on p 2046) reasonable and sufficient to adequately protect health information within the Stage 1 meaningful-use timeframe? Are any of these criteria insufficiently specific to be used to test and certify Complete EHRs or EHR Modules, with reasonable assurance that the technology will effectively support the delivery of health care as well as the achievement of Stage 1 meaningful use? (solicitation p 2029)

Criterion	Comments
(o) Access Control	Reasonable and sufficient; acceptable specificity.
(p) Emergency Access	Reasonable and sufficient; acceptable specificity.
(q) Automatic Log-off	Reasonable and sufficient; acceptable specificity.
(r) Audit Log (1) Record Actions (2) Alerts	Provision (r)(2), "provide alerts based on user-defined criteria," is beyond what is required by HIPAA and the American Recovery and Reinvestment Act (ARRA), and thus seems to lack legal foundation. Audit alerts are

Criterion	Comments
(3) Display and Print	actionable only if they are triggered close to the time the event occurs. For example, firewalls typically provide alerts in near real-time so that an intruder can be stopped before doing damage to the enterprise. Providing such real-time alerting requires audit processing and decision support capabilities that are not typically provided by today's EHR products. Further, providing this capability across multiple EHR modules produced by different vendors would require the capability to merge audit records into a common data model and common vocabulary for recording audit events, neither of which exists as a standard today. We believe this requirement is beyond what can be justified by HIPAA and ARRA, and beyond what should be required for Stage 1 meaningful use certification. However, should this criterion persist, it would not be specific enough to test. For example, would "when a new month begins" or "when the disk is 95% full" be acceptable "user-defined events?" With respect to audit display and printing, the requirement to "Electronically display and print all or a specified set of recorded information upon request or at a set period of time" [§170.302(r)(3)] is not sufficiently specific to be used for testing. Recommendations: 1) Delete criterion (r)(2) from the IFR as it has no legal foundation, and we believe the technical solution required is beyond what should be expected for Stage 1 certification. 2) Require that audit records be displayable and printable in a structured format designed for human review.
(s) Integrity (1) In Transit (2) Detection	We see a need for clarification that integrity protection applies to the full range of data transfer, including devices, web, or transfer on removable media. Regarding (s)(2), "Detect the alteration and deletion of electronic health information and audit logs, in accordance with the standard specified in §170.210(c)," while this is a reasonable functional requirement, the required capability is beyond what the referenced standard (SHA-1) can support. Also, the IFR needs to clarify that the capability to "detect alteration in transit" requires only that integrity checks be performed on a transmission channel, and that the integrity of the message payload need not be independently verified. For 2011, no standard should be referenced for detecting changes in data at rest. Recommendation: Revise §170.302(s)(1) to read: "(1) *Data Transfer*. Verify that electronic transmissions of health information, and health information transfers to electronic media, have not resulted in any alteration of the data transferred, in accordance with the standard specified in § 170.210(c)."
(t) Authentication	We believe that requiring the exchange of identity assertions between

Criterion	Comments
(1) Local (2) Cross Network	enterprises (e.g., covered entities), using the Integrating the Healthcare Enterprise (IHE) Cross-Enterprise User Assertion (XUA) profile and the Security Assertion Markup Language (SAML) [Table 2B and §170.302(d) on p 2046] is beyond what is needed, and what is technically feasible, for Stage 1. To be clear, XUA/SAML is not a standard for authenticating the identity of users or entities (e.g., systems, software applications), but rather a standard for sharing information regarding an authenticated user between entities – commonly known as "single sign-on" (SSO). SSO has not been broadly implemented even within healthcare enterprises, and SAML implementations between enterprises is well beyond common practice in any industry. We understand and agree with the significance of federated authentication by Stage 2, when the exchange of structured health information between enterprises will become more pervasive, hopefully facilitated by trusted intermediaries to mediate identity challenges between enterprises. However, we see no compelling need for federated authentication for Stage 1, when most exchanges are based on a one-way model of communication to generate or produce something that is "pushed" to the recipient based on a reporting requirement or in response to a specific request negotiated out of band. Exchanges performed through an intermediary, such as electronic prescribing, do not depend on cross-enterprise authentication of users as the transaction does not involve a user request for information. We believe a much more reasonable criterion – and indeed a "gap" in the IFR certification criteria – would be the capability to authenticate the two end-points of a network exchange between two enterprises before establishing a trusted path between them. Although the criteria cover both encryption and integrity-protection of information exchanged between two entities over a network, they do not include the authentication of the communicating entities (i.e., systems, applications). Authenticating the entity to which one is connecting is essential for confidentiality protection, care quality, and patient safety. One would not want to connect to a rogue system that would push malicious code into a healthcare enterprise for the purpose of interrupting operations or denying access to critical resources. Several use cases are relevant here. For example, two hospitals within an integrated delivery network may need to routinely exchange health information between them. A physician may need to access an EHR provided by an application service provider. A consumer may need to access her personal health record provided by her physician. Whether one or both ends of the connection need to be authenticated is a policy decision. But from a certification perspective, at a minimum, an EHR system that offers the capability to connect to people, applications, and enterprises over the public Internet should be required to provide the capability to mutually authenticate

Criterion	Comments
	both ends of the connection, and to encrypt and integrity protect health information exchanged over the link. Both of the two standards specified for the encryption and integrity-protection of exchanges, Transport Layer Security (TLS) and Internet Protocol Security (IPsec), support the authentication of end points. Both IPsec and TLS are end-to-end security schemes that require the authentication of at least one of the end points before establishing the secured channel. The principal difference between the two is that IPsec operates at the network level (Layer 3 in the Open Systems Interconnection (OSI) reference model), while TLS operates above that at the transport level (OSI Layer 4). So IPsec is used to protect data flows between two Internet nodes, between two security gateways (e.g., firewalls or routers), or between a security gateway and an Internet node. TLS (also known as Secure Sockets Layer, SSL) is used to protect data flows between two applications, or between a client and a service. An IPsec gateway will protect everything transmitted through it over the Internet. Applications need not be specifically designed to use IPsec, nor even be aware that their transmissions will be IPsec protected. In contrast, the use of TLS must be incorporated into the design of applications, and the establishment of the TLS channel is usually visible to users. IPsec and TLS can be used together to provide “defense in depth” – all transmissions over IPsec-protected Internet links will be protected, plus transmissions between the two TLS end points will be private. Note that IPsec and TLS are not mutually interoperable. That is, an IPsec gateway cannot establish a link with an application designed to establish secure TLS channels. Depending upon the functions and operational environments for which the EHR technology submitted for certification is designed, the vendor may choose to implement IPsec, TLS, or both. The HIPAA Security Rule and ARRA require that each covered entity and business associate perform an annual security risk analysis. Based on the risks identified, each eligible professional/hospital will need to determine when IPsec-secured networks and TLS-secured application channels need to be used to achieve meaningful use. The capability to establish a mutually authenticated, encrypted, and integrity protected trusted path between two enterprises or entities is a very reasonable and feasible objective for Stage 1, and can be supported by existing referenced standards (TLS, IPsec, AES, SHA). Once such a channel is established, users can log into systems in other enterprises to achieve the objective of inter-enterprise exchanges, while postponing the “single sign-on” capability enabled by the exchange of identity assertions (XUA/SAML capabilities) until 2013 or 2015.

Criterion	Comments
	Recommendations: 1) Remove requirement for cross-network authentication, and reconsider for 2013. 2) Revise cross-network authentication certification criterion to read: "Verify that the identity of an entity seeking access to electronic health information across a network is the one claimed in accordance with the standard specified in §170.210(d)." Revise standard §170.210(d) as recommended in our discussion of Question 3 below.
(u)Encryption (1) General (2) Exchange	We believe that the "General" certification criterion (u)(1) is reasonable and sufficient as stated. However, we observe that "user-defined preferences" could be interpreted as person-level proclivities, when decisions about when and what to encrypt are generally based on policies established by and for the enterprise. We recommend revising the "General" criterion to clarify both its applicability and its dependence upon local policy. Recommendation: Revise the "General" criterion to read "Encrypt and decrypt electronic health information according to enterprise security policies in accordance with the standard specified in §170.210(a)(1)."
(v)Accounting of Disclosures	We agree with the certification criterion for accounting of disclosures as articulated in §170.302(v). However, we suggest that the expectation for capturing and recording a "description of the disclosure" be clarified to allow for construction of the accounting in post-processing rather than requiring the capture of all data elements in real time. Just as a system may use an internal identifier to represent a user or patient, translating it into an actual name only when it is needed for human consumption, a system should be allowed to represent a "description" using abstractions that would enable a human-consumable "description" to be generated through post-processing of system events. In this way the need for real-time recording of disclosure-related events could be minimized, creating the desired result with minimal real-time burden on the EHR system. A further benefit is that multiple system events could be combined in post-processing to create a more cogent description of the disclosure than would be possible in real time. Recommendation: Revise this criterion to read: "Create a record of disclosures made for treatment, payment, and health care operations in accordance with the standard specified in § 170.210(e)."
§170.304(g) Timely Access	The use of the phrase "online access to their clinical information" is problematic and inconsistent with the language used in the relevant Stage 1 meaningful use objective "Provide patients with timely electronic access

Criterion	Comments
	to their health information...” [Ref Table 1 on p 2027]. If “online access” is interpreted as providing a consumer real-time access to the same record used by her provider, then this requirement is beyond what is required by HIPAA and ARRA. Similarly, if “online access” is interpreted as requiring every family physician to provide a Web portal for patients to view their information, this too is beyond what is required by HIPAA and ARRA. If “online access” is interpreted as enabling a consumer to view her full record, but does not enable her to download it to her home computer or copy it to her USB drive, then this criterion falls short of what is required by HIPAA and ARRA. The HIPAA Privacy Rule gives consumers the right to access or obtain a copy of their own protected health information (PHI), and ARRA gives them the right to an “electronic copy” and to request that an electronic copy be sent to a designated person or entity. Consumers should be provided an electronic copy of their health information that can be copied to and viewed from their home computer, or sent to another person or entity (e.g., PHR vendor) in a format usable by that person or entity. “Online access” that does not allow the consumer to download a a copy of his health information is insufficient, and “real-time online access” is beyond what HIPAA or ARRA require – and may not be what consumers want either if they are unable to create a copy (i.e., document) of their health information. Also, we recognize the potential value of personal health records (PHRs) for supporting and facilitating personal medical decision making, public health surveillance, and collaboration between consumers and their doctors and health researchers. All of these secondary uses are supported by consumers and enabled by semantic interoperability, including both standard messaging and controlled vocabulary. So we recommend that the ONC establish as a priority for the HIT Policy and Standards Committees the development of recommendations for policy and standards to facilitate the use of PHRs for these purposes. Recommendations: 1) Revise to read: “Enable a user to provide consumers with electronic access to their health information, including, at a minimum, lab test results, problem list, medication list, medication allergy list, immunizations, and procedures, and to provide a copy of the consumer’s personal health information in an electronic format that is usable by the consumer.” 2) Establish as a priority for 2013 the specification of messaging, content, and vocabulary standards for sending/transferring the electronic record to a PHR vendor. 3) Publish guidance for developers and eligible professionals and hospitals on how to provide consumers timely electronic access to their health

Criterion	Comments
	information.

Question 3: Privacy and Security Standards
Are the privacy and security standards adopted (see Table 2B, p 2035 and Regulation §170.210(a-e) on p 2044) reasonable and sufficient to adequately protect electronic health information within the Stage 1 meaningful use timeframe?

Standard	Comments
(a) Encryption and decryption of electronic health information (1) General (2) Exchange	Because the encryption standard does not specify the algorithm to be used, it lacks the specificity needed to assure that secured communications will be established. In order to secure a channel using symmetric encryption, both end points must have implemented the same encryption algorithm. Also, this standard precludes the use of public-key (asymmetric) encryption for protecting the confidentiality of information (e.g., email encryption). The standard needs to be worded to allow the use of both symmetric and asymmetric encryption. We support the adoption of the Advanced Encryption Algorithm (AES) as the standard for symmetric encryption. However, this functional representation of the standard can be met by either AES or a proprietary algorithm. §170.210(c) specifically calls for the use of the secure hash algorithm "SHA-1 or higher" as the standard for protecting the integrity of electronic health information. We see no justification for specifying "SHA-1" and not "AES." To clarify that AES is the adopted standard for symmetric encryption, while allowing the standard to withstand improvements in encryption technology, we recommend replacing the current standard with a specific requirement for "AES or its successor." Recommendation: We suggest revising §170.210(a) to read as follows: "(a) Encryption and decryption of electronic health information. (1) The Advanced Encryption Algorithm (FIPS PUB 197 Advanced Encryption Standard (AES), November 26, 2001), or its successor, must be used for symmetric encryption. (2) Exchange. The capability to establish a secure communication channel must be implemented."
(b) Record actions related to electronic health information	The standard calls for certain data to be recorded when electronic health information is "created, modified, deleted or printed." We have two concerns. First, "access" is not included and is a critical action to be recorded. Second, auditing "printing" would be a challenge for most smaller systems, and even for large systems, is not likely to include "print screen."

Standard	Comments
	Recommendations: 1) Add "accessed" to the list of actions that must be audited. 2) Replace "printed" with "exported" in the list of actions that must be audited.
(c) Verification that electronic health information has not been altered in transit	We find the standard reasonable and sufficient, but lacking a specific citation. Recommendation: We suggest adding the standard citation "FIPS PUB 180-3 Secure Hash Standard (SHS). October 2008."
(d) Cross-enterprise authentication	The cross-enterprise authentication standard is well beyond the current state of practice. Based on the IFR Preamble, we interpret the "cross-enterprise authentication" standard as the IHE XUA profile, which uses SAML to pass identity information between enterprises. XUA/SAML used in this way is beyond the current state of practice in any industry. On the other hand, based strictly on the functional description in §170.210(d), one could reasonably argue that the capability to allow an individual to log into a system from outside the enterprise would meet this requirement. Within the context of either interpretation, this standard lacks the specificity needed to allow systems to interoperate. As noted in our comment regarding the authentication certification criterion, XUA/SAML is not really an "authentication" standard, but rather a standard for passing an authenticated identity between systems to achieve what is commonly called "single sign-on (SSO). SAML is not in broad use even within enterprises, and almost never used to cross-authenticate between enterprises. Further, the industry has not agreed upon a common data model to use to represent authentication and authorization information that is passed between organizations. We do not believe it is reasonable to ask developers to implement cross-entity authentication in the absence of a common data model for representing the shared information. We recommend replacing this standard (and certification criterion) with a requirement that products implement the capability to authenticate the end points before establishing a trusted communication path between entities. This standard could be met through the use of either TLS or IPsec. Recommendations: 1) Revise standard §170.210(d) to read: "Authentication of the entities at each end of a protected transmission channel must be implemented." 2) Consider cross-enterprise authentication using XUA/SAML a candidate standard for 2013, within the context of the Implementation Workgroup's

Standard	Comments
	implementability criteria.
(e) Record treatment, payment, and health care operations disclosures	Realizing that the Accounting of Disclosures NPRM is still being developed, we suggest that the Office of Civil Rights (OCR) consider adopting ASTM E2147 (Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems) as the standard for the specifying the data elements that need to be captured in an accounting of disclosures. Also, as noted in our comments regarding Question 2 above, the standard needs to allow for implementations that capture the “description” through post-processing rather than in real-time. Recommendations: 1) Revise standard to read “(e) *Create a record of treatment, payment, and health care operations disclosures.* The date, time, patient identification, user identification, and a description of the disclosure must be included in the record of accounting of disclosures for treatment, payment, and health care operations, as these terms are defined at 45 CFR 164.501.” 2) Consider adopting ASTM E2147 as the standard for specifying the data elements that need to be captured in a record of accounting of disclosures, within the context of the Implementation Workgroup’s implementability criteria.
§ 170.202 Transport standards for exchanging electronic health information	§170.202 adopts the Simple Object Access Protocol (SOAP) and Representational State Transfer (REST) principles as standard protocols for electronically exchanging health information formatted in accordance with the standards adopted under §170.205. Although both of these protocols are commonly used for accessing web services, it is unclear what value including them in this IFR will bring to the industry. These standards seem to conflict with the very section they reference, which requires HL7 messaging, NCPDP SCRIPT, and ASC X12N transactions. Further, none of the certification criteria in Subpart C incorporate SOAP or REST directly or by reference to §170.202. Recommendation: Remove §170.202 from the IFR.

Question 4: Omitted Standards
Should the domain name service, directory access, and consistent time, or any other function or service, be reconsidered for inclusion as a required capability for Certified EHR Technology? (solicitation p 2035)

We have no objection to the specific omission of the domain name service (DNS), lightweight directory access protocol (LDAP), or consistent time from the Rule. Many of the adopted standards require the presence of lower-level standards and services such as DNS, negating the need to specifically list these standards since they will automatically be included by the higher-level functions, as needed.

However, we believe it may be appropriate to specify performance standards such as "timestamps on audit logs must be accurate to within 1 second" – a requirement that could be met using a variety of technical approaches. The accuracy of the time source will become increasingly important as accounting of disclosures is implemented across enterprises. We suggest the ONC consider establishing a standard time source or a maximum clock strata (i.e., distance from a stratum-0 reference clock), which would limit the delay tolerance. We do not consider these standards critical for Stage 1, but recommend they be considered for Stage 2.

Question 5: Accounting of Disclosures Standard
Is the functional standard adopted for accounting of disclosures for treatment, payment, and healthcare operations (see Table 2B, p 2035 and discussion on pp 2036-2037; and Regulation §170.210(e) on p 2044) reasonable and technically feasible? What is the technical feasibility of collecting other data elements, including reason for the disclosure and to whom the disclosure was made? (solicitation p 2037)

While we find the accounting-of-disclosures standard acceptable, we want to comment on the timeline relating to this regulatory requirement; specifically 1) the date proposed for accounting-of-disclosures to become a meaningful-use objective, and 2) the date when all covered entities and business associates are required to comply with this ARRA requirement.

We note an inconsistency in the timeline between ARRA and the meaningful-use objectives recommended by the HIT Policy Committee. According to ARRA, the effective date when all covered entities and business associates must provide an accounting-of-disclosures is 2014, for those entities that acquired an EHR before January 1, 2009, and 2009 (or the date the technology is acquired), for entities that acquired an EHR after January 1, 2009. ARRA gives the Secretary the option to push these effective dates out to no later than 2016 and 2013 respectively. The Rule governing accounting of disclosures is due six months after the Secretary adopts standards – that is, in June of this year. The meaningful use timeline recommended by the HIT Policy Committee identifies providing patients an accounting of treatment, payment, and health care operations disclosures as a 2015 objective.

Implementing the capability to account for all instances in which PHI is released, transferred, accessed, or divulged in any other manner outside the entity holding the information [per definition given in 45 CFR 164.501], including for purposes of treatment, payment, and healthcare operations, will require not only integrated EHR technology to support the capture of the required information, but perhaps more notably, significant changes in internal enterprise policies, operational practices, and workflow. The requirement to account for disclosures for treatment, payment, and healthcare operations applies only to entities that adopt EHRs. To ensure that this requirement does not discourage EHR adoption, the effective date of January 1, 2011, for covered entities who acquire EHRs after January 1, 2009, should be evaluated once the accounting-of-disclosures rule is released. We will await the final details of the disclosure rule and work with the HIT Policy Committee's Privacy and Security Policy Workgroup to achieve a balance between operational impact and the disclosure goals outlined in meaningful use. We further believe the timelines for regulatory compliance and meaningful-use reporting should be consistent. We are recommending that the ONC organize a discussion between the HIT Policy and Standards Committees' Security and Privacy workgroups to address the timeline inconsistency and to consider what changes may be warranted to accomplish disclosure accountability without discouraging

EHR adoption, while giving enterprises the time they will need to develop appropriate operational procedures and workflow.

We further suggest that the Office of Civil Rights (OCR) consider adopting as a standard the content elements identified for "basic disclosure" in ASTM E2147 (Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems), which include (as applicable):

(1) Date and time of disclosure
(2) Reason for the disclosure
(3) Description of the information disclosed
(4) Identity of the person requesting access
(5) Identity and verification of the party receiving the information
(6) Identity of the party disclosing the information
(7) Verification method of requesting the party's identity

We believe that in general, capturing the data elements identified in this standard is technically feasible, particularly if such information can be gleaned through post-processing of logs of system activities. However, the rules should allow for edge cases where capturing the additional data elements is either not practical or is plainly obvious from the context of the transaction. For example, an e-prescribing transaction log would implicitly capture both the "reason" for disclosure and the "to whom" – so these details of the transaction may not need to be captured in a redundant disclosures log. Similarly, recording the "reason" for a claims submission or eligibility transaction should not be required for every occurrence. The unnecessary collection of disclosure information on every occurrence of these types of transactions would overly burden EHR systems and blur the real reasons for disclosures.

Recommendations:

1) Recommend to the HIT Policy Committee that the meaningful-use measure for accounting of disclosures be moved forward to 2013.
2) The HIT Standards Committee suggests that ONC organize a discussion between the HIT Policy and Standards Committee Security and Privacy workgroups so they may make a coordinated statement regarding the timing of accounting-of-disclosure compliance and meaningful-use timelines, which will inform ONC recommendations to the Secretary.

Question 6: Privacy and Security Gaps
Do you perceive any gaps in the IFR with respect to privacy and security standards, implementation specifications, and certification criteria?

For privacy and security, certification of the security of EHR technology is only one consideration. Most importantly, performing an annual security analysis, and delineating appropriate privacy and security policies and practices are necessary to protect health information and to create trust. ONC will be providing further guidance and support as required by ARRA, through mechanisms such as the Regional Extension Centers and an extensive portfolio of grant programs. With that said, we offer the following comments.

The omission of a certification criterion and standard for authenticating the end points of a transmission channel between enterprises is a critical gap with respect to confidentiality, care quality, and patient safety. We have recommended actions to correct this gap. We strongly believe that implementing the capability to authenticate the end points for trusted connections between enterprises is essential for enabling the health information exchanges expected to be achieved with this rule.

While we agree with the approach of excluding from the body of the Regulation the example standards ("e.g."s) given in Table 2B in the Preamble, this approach presents a gap in functional specificity that creates risk for developers and certifiers. We believe the ONC should address this gap during the development of the certification program by creating a framework and processes for enabling the program to maintain a current list of acceptable standards for meeting these functional requirements.

We wondered whether "role based access control" (RBAC) should be specified within the 2011 rule. Given that most vendors already implement some form of RBAC, including it as a certification criterion and "functional standard" for 2011 is both reasonable and feasible.

Also, the absence of standards for digital signatures was noted by a HITSC member. Since neither HIPAA nor ARRA requires digital signatures, we do not consider this a gap. However, as the electronic exchange of health information between enterprises becomes more commonplace, assuring the authenticity of the source and the integrity of the content will become increasingly important. We recommend the HIT Policy Committee be asked to consider the need for policy and standards around digital signatures.

We appreciate the opportunity to provide these comments, and look forward to discussing next steps for the Committee.

Sincerely,

/Dixie Baker/

Dixie Baker

Chair, Privacy & Security Workgroup

/Steve Findlay/

Steve Findlay

Co-Chair, Privacy & Security Workgroup