230 E. Ohio Street, Suite 500
Chicago, IL 60611-3269
Telephone: 312.664.4467
www.himss.org

March 15, 2010

The Honorable Kathleen Sebelius
Secretary of Health and Human Services
U.S. Department of Health and Human Services
200 Independence Avenue, SW
Washington, DC 20201

Dr. David Blumenthal
National Coordinator for Health Information Technology
Office of the National Coordinator
200 Independence Avenue, SW
Washington, DC 20201

Dear Secretary Sebelius and Dr. Blumenthal:

On behalf of the Board of Directors and members of the Healthcare Information and Management Systems Society (HIMSS), we are pleased to submit written comments on the Department of Health and Human Services interim final rule entitled *Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology Interim Final Rule* that was posted on the Department's website and in the Federal Register on January 13, 2010.

HIMSS is the healthcare industry's membership organization exclusively focused on providing leadership for the optimal use of healthcare information technology and management systems for the betterment of healthcare. HIMSS represents more than 27,000 individual, 400 corporate members, more than 50 non-profit organizations, and 46 chapters nationwide. HIMSS seeks to shape healthcare best practices and policy through its educational, professional development, and government relations initiatives designed to promote the best use of information and management systems in patient care.

As in past responses to HHS, HIMSS has leveraged the subject matter expertise of our members to ensure that our response reflects the broadest level of industry experience. For the response on the guidance document, HIMSS developed a cross-organization work group that represents the expertise of our overall membership. In addition, HIMSS sought input on the response from our steering committee structure, including the following areas of expertise: Ambulatory Information Systems; Enterprise Information Systems; Financial Information Systems; Healthcare Information Exchange; Management Engineering and Process Improvement; Nursing Informatics; Physician Community; Patient Safety & Quality Outcomes; Personal Health Records; Privacy and Security; and Public Policy. We also leveraged the expertise of our Chapter Advocates Roundtable and Legislative & Regulatory Review Task Force to ensure the Board response would reflect the diversity of our membership

As you know, the Health Information Technology for Economic and Clinical Health Act (HITECH Act), Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA) requires the Secretary of the Department of Health and Human Services (the Secretary) to adopt an initial set of standards, implementation specifications,

and certification criteria by December 31, 2009 to enhance the interoperability, functionality, utility, and security of health information technology. HIMSS appreciates the Department's interest in seeking public comment on this issue, and offers the following observations.

Overview and Summary of Recommendations

As HIMSS volunteers worked to develop these comments, several key important themes emerged. These key points are vital to the success of this rule facilitating nationwide electronic health record adoption.

- HIMSS endorses the adoption of one patient record summary standard to support Meaningful Use (MU) in Stage II and beyond and the use of CCD or CCR for Stage I as a glide path to a single standard. This means that the selection of the single standard needs to occur within a 6 month time window so that vendors and providers have the lead time to factor changes into their product and implementation plans. HIMSS membership is concerned that several key items in the required certification criteria are not clearly-defined, and short timelines present huge challenges. It is critical for Health Information Technology stakeholders to have consistency in terminology related to terms. Stakeholders need significant advance time for the industry to deliver and test the products and have clearly understandable language to do that – not doing that raises the risk of failure and the likelihood that we can deliver a quality outcome in time. To give an example, "structured data" and "structured reporting" are part of the certification criteria, but the terms are not clearly defined. CMS Meaningful Use NPRM defines structured data as "data that have a specified data type and response categories within an electronic record or file." This definition is vague. In order for Meaningful Use to be accomplished, many of these criteria require improved granularity. HIMSS also requests that the Final Rule fully harmonize with the CMS Meaningful Use Final Rule.
- HIMSS membership is concerned that many of the certification criteria and standards listed in the IFR pose significant challenges to end users and vendors of inclusive best of breed and modular systems. Based on these criteria, HIMSS is concerned that it would be much more difficult than anticipated to certify a modular EHR.
- HIMSS supports a push towards administrative simplification industry wide using the Council on Operating Rules for Eligibility (CORE) process. HIMSS notes that effective administrative simplification results can be realized when all stakeholders support the CORE rules, which includes payors, clearing houses, software system vendors as well as providers. CORE Phase II is currently being implemented in the industry and we look forward to maturation of eligibility verification based on CORE Phase II by 2014.
- HIMSS members feel that ONC analysis regarding Small Business Impact and the need for a Regulatory Impact Analysis is incorrect regarding Small Business Impact and the overall cost of getting a product certified. According to ONC, most if not all ambulatory EHR vendors would exceed the Small Business size standard ($25 million in annual receipts or smaller) due to the required amount of upfront capital needed to develop and market HIT in the marketplace. According to CCHIT membership data, over 75% of the ambulatory EHR marketplace falls under the Small Business label with less than $25 million in annual revenue.

- Regarding the cost of getting a product prepared for certification, ONC analysis suggests preparing for certification will cost between $50,000 and $150,000 to prepare an average CCHIT certified ambulatory EHR product for HHS certification testing, and it will cost between $75,000 and $200,000 to prepare an average CCHIT certified inpatient EHR for HHS. HIMSS members contend that the costs will be much higher than ONC estimates for preparing a product for certification, and significantly higher for modular systems.
- HIMSS wants to continue to support ONC efforts to monitor the latest industry developments in the field of security.

HIMSS Comments on IFR Definitions:

HIMSS appreciates the opportunity to comment on the definition section of the Interim Final Rule. HIMSS feels that there is questionable clarity between Complete EHR & EHR Module which when combined is the definition of Certified EHR Technology. HIMSS recommends that the following edits be incorporated into the IFR definitions.

1) Definition of Standard: HIMSS has no comments.

2) Definition of Implementation Specification: HIMSS has no comments.

3) Definition of Certification Criteria: HIMSS has no comments.

4) Definition of Qualified EHR: HIMSS has no comments.

5) Definition of EHR Module

HIMSS recommends expanding EHR Module definition to read:

EHR Module is any service that can meet certification criteria using harmonization specifications that will achieve interoperability.

6) Definition of Complete EHR

HIMSS recommends expanding Complete EHR definition to read as:

The term Complete EHR is used to mean EHR technology which is defined as health information that is assembled and maintained in standardized electronic formats and supports EHR systems and infrastructures.

7) Definition of Certified EHR Technology

HIMSS members are concerned that three modular components could each meet a certain number of certification criteria for Stage 1 which in total could meet all the requirements. This does not mean that they would be readily interoperable.

Our members have not observed language in the Certification Criteria in Table 1 of the document that mandates testing and certification of the interoperability between modules. While they may be implied or assumed based on the stated outcomes for functionality for Stage 1, it is not explicitly stated. Clinicians and institutions contemplating the purchase of a modular EHR, where each module is certified, would have an expectation of interoperability. While the IFR does

clearly indicate an expectation that at some point in the future the modules will be 'plug and play' that is still a fair way off and will require considerable work in more clearly defining, agreeing on, and implementing consistency in the framework, standards implementation guides, variables and options for the interchange of health information. HIMSS recommends an additional step for modular certification that requires testing in conjunction with complementing modules. This would complicate the process and considerably increase the cost. While the IFR clearly places the responsibility for interoperability of modules with the purchasers, perhaps there should be some guidance on how that would be done and what would be acceptable.

8) Definition of Disclosure

HIMSS also recommends adding a definition for capability and suggests the following definition: *An implementable business service that specifies interoperable information exchanges to ensure compatibility and reduce redundancy.*

HIMSS Comments on Certification Criteria

HIMSS appreciates the opportunity to comment on the initial Certification Criteria for EHR Technology. HIMSS supports ONC's goal of promoting implementation of interoperable systems to improve the quality of healthcare and HIMSS supports the overall objectives of the required certification criteria. HIMSS membership is concerned that several key items in the required certification criteria are not clearly-defined, and short timelines present huge challenges.

It is critical HIT stakeholders have consistency in terminology related to terms. Stakeholders need significant advance time for the industry to deliver and test products and have clearly understandable language to do that raises the risk of failure and makes it less likely that we can deliver a timely quality outcome. To give an example, "structured data" and "structured reporting" are part of the certification criteria, but the terms are not clearly defined. CMS Meaningful Use NPRM defines structured data as "data that have a specified data type and response categories within an electronic record or file." This definition is vague. In order for Meaningful Use to be accomplished, many of these criteria need improved granularity. HIMSS has developed comments and recommendations on each of the Certification Criteria listed in Table 1 of the Interim Final Rule. These comments and recommendations can be reviewed in Appendix 1 (attached).

Office of the National Coordinator Requests for Comments regarding Certification Standards

The Office of the National Coordinator requests public comment on a single standard for electronic exchange of patient summary information for Stage II. HIMSS appreciates the opportunity to comment on this request. HIMSS endorses the adoption of one patient record summary standard to support Meaningful Use (MU) in Stage II and beyond and the use of CCD or CCR for Stage I as a glide path to a single standard. This means that the selection of the single standard needs to occur within a 6 month time window so that vendors and providers have the lead time to factor changes into their product and implementation plans.

The Office of the National Coordinator requested public comment whether HL7 Quality Reporting Document Architecture (QRDA) Implementation Guide based on HL7 CDA Release 2 is a mature enough standard to be used for Complete EHRs and EHR Modules during meaningful use Stage 1. HIMSS welcomes the opportunity to comment on the maturity of HL7 QRDA. HIMSS membership feels that the HL7 QRDA standard is **not** mature enough to be utilized in Stage 1and as presently constituted would need to be more flexible and granular.

ONC requests public comment on the health IT industry's experience using CAQH CORE Phase 1 with adopted HIPAA transaction standards. HIMSS welcomes the opportunity to comment. EHRs do not issue a claim nor do they check eligibility unless it is in an associated module integrated with a Patient Accounting (PA) system. We do need the EHR to have the capability to capture and pass data with regard to visit/episode diagnoses (DX) to support billing functionality in the PA system. Many offices use payor eligibility systems which are not integrated with EHRs. In some instances, ambulatory practices and hospitals access an insurer's stand-alone system to verify patient eligibility.

Specific to the CAQH / Council on Operating Rules for Eligibility (CORE) process, HIMSS supports a push towards administrative simplification industry wide using CORE. HIMSS notes that effective administrative simplification results can be realized when all stakeholders support the CORE rules, which includes clearinghouses and payors, as well as the software system vendors as well as providers. CORE rules are currently able to support and facilitate administrative simplification as outlined in the MU requirements. CORE Phase II is currently being implemented in the industry and we look forward to maturation of eligibility verification based on CORE Phase II by 2014.

The development of national standards should be required that will allow various Information System (IS) products to exchange data i.e. eligibility to allow communication to the EHR Payors, Pharmacy, Patient Portals and Clearinghouses. In ambulatory practice systems and pharmacies many retail pharmacies must purchase a vendor module to allow for the integration of prescribing information. For example, the Virginia Women's Center, HIMSS 2009 Davies Award recipient for Ambulatory Care must purchase modules to allow for the exchange of the information. This is an extra module for the pharmacy and EHR module which result in additional labor and capital costs to the provider.

The exchange of data for Ambulatory Eligible Providers' via clearinghouse should be practice-based instead of a per transaction approach, which is cost prohibitive to many practices as they will not be able to complete certain functions (i.e. hire additional assistance.) In addition, practices may make the economic decision to combine transactions, such as the anticipated approach for reaching the 30% Medicaid threshold.

In addition, HIMSS requests clarification on the language that describes the intent to exchange information with other systems i.e. eligibility, e-prescribing. Does the government mean insurance or for benefit verification and authorization of eligible benefits?

Finally, on the pharmacy side, it would be helpful to the Eligible Provider (EP) to receive notification of prescriptions being received and any changes that pharmacists need to make via the system that move information. The goal of e-prescribing is not only to reduce administrative costs but to ensure the patients receive the medications prescribed to support the appropriate treatment.

ONC requests public comment regarding industry readiness if they were to adopt certification criteria requiring the use of additional vocabularies and code sets in parallel with meaningful use Stage 2. HIMSS welcomes the opportunity to comment. HIMSS recognizes the value of the code set, but is concerned about timelines. Vendors require significant time to allow for changes in the databases to be compliant with certification criteria. Any changes would require a window of 12 months in order to prevent errors.

The HIMSS provider community would like to note that most EHR systems have a local description/local interpretation from the vocabulary. Any standard for human-readable data that would be adopted should also ensure that the human readable data is also easy to understand for patients.

HIMSS Comments on Implementation Specifications

ONC is seeking public comment on whether there are in fact implementation specifications that are industry-tested and would not present a significant burden if they were adopted. We believe that certain exchange purposes, such as electronic prescribing and laboratory test results, already have available some of the most mature implementation specifications. We will consider adopting implementation specifications, for any or all adopted standards provided that there is convincing evidence submitted in public comment of the specifications' maturity and widespread usage. HIMSS welcomes the opportunity to comment on ONC's request on implementation specifications.

HIMSS is concerned that there is lack of a clear roadmap in the IFR. ONC took pains to note that it was not recommending adoption of implementation specifications, except in a few cases established by other federal regulations, such as HIPAA ASC X12N transactions and NCPDP guides. ONC explained that based on recommendations of the HIT Standards Committee, it considered implementation specifications, such as those produced by Healthcare Information Technology Standards Panel (HITSP), the Integrating the Healthcare Enterprise (IHE) Initiatives, and others to be too immature and not widely adopted. This requirement sets up the interesting dynamic of how, in a regulated industry focused on qualifying for meaningful use incentives, new specifications become adopted. Since much of the interoperability criteria need not be demonstrated in meaningful use during Stage 1, there is time for the HIT Standards Committee to adopt implementation guides for 2013. The guidance provided about Stage 2, except for moving toward requiring controlled vocabularies and structured documents, offers no direction for implementers. Today we have two transport standards, SOAP and REST, as well as content standards including HL7 CDA/CCD, ASTM CCR, HL7 Version 2.x messages and no implementation guides as to when and how to assemble these and then apply security without significant point to point negotiation and configuration. The HIT Standards Committee has adopted the 'simple is better' approach and is applying it to a very complex domain. We have an incomplete roadmap to interoperability at this point. While some may look to the NHIN projects,

these having increasingly focused on the HITSP specifications, which have harmonized standards and integration profiles over the last four years. We want to emphasize that merely selecting standards does not lead to interoperable implementations. True interoperability requires consensus based deliberations of a broad base of stakeholders and subject matter experts who then develop clear documentation of implementation guidance for the selected standards, with subsequent conformance testing of the implementations. The implementation guides produced by HITSP, IHE and others are being successfully adopted and implemented by HIEs regionally, nationally and globally. HIMSS recommends that the next version of the IFR and the related roadmap be informed by this additional information**.**

Privacy and Security Standards

HIMSS welcomes the opportunity to comment on the ONC IFR privacy and security standards. As you know, HIMSS has leveraged the subject matter expertise of our Privacy and Security Steering Committee to guide implementation of strategic initiatives that promote the privacy and security of secure electronic health information exchange.

HIMSS is concerned that the goal of the privacy and security standards in the IFR are not clear. In order to ensure interoperability, both sender and receiver may need to follow a specific standard. The goal of this IFR must be to support secure interoperability. HIMSS also recommends that language be added to the IFR specifying required end point system-to-system authentication, which ensures that the EHR is talking to a trusted system.

HIMSS also requests clarification regarding how the privacy and security requirements apply to modular systems. Does this requirement apply to each EHR module? Do internal transactions between modular units require encryption (e.g., ATD transactions)? Modularity causes difficulty with security and privacy. Security and privacy can only be evaluated when the complete system is brought together. Modules may have no inherent security controls as those may be part of the platform and integration components (e.g., CCOW, Web-service, Browser plug-in). Modules may rely on the implemented environment to provide security functions, may produce audit logs but leverage platform for secure access and communications. Is it possible that – for modules that are undergoing certification – the vendor could declare *how the module should be implemented* such that it meets security/privacy objectives?

HIMSS has specific comments related to each of the security requirements related to each of the individual criteria which can be found in Appendix 2 of this letter.

Regulatory Impact Analysis

The Office of the National Coordinator has requested comments on their estimation of the economic impact of the rule. Per the ONC cost estimates and research, many CCHIT ambulatory and inpatient certification criteria require the same capabilities as the interim final rule will require for certification. Accordingly CCHIT certified EHRs will incur minimal costs to prepare for certification and CCHIT certified EHRs are similar to the ONC definition of a "complete EHR." ONC estimates that it will cost between $50,000 and $150,000 to prepare an average CCHIT certified ambulatory EHR product for HHS certification testing, and it will cost between $75,000 and $200,000 to prepare an average CCHIT certified inpatient EHR for HHS

certification testing. HIMSS welcomes the opportunity to comment on ONC's cost analysis. Feedback from HIMSS members indicates an investment of over 2,500 hours of staff time is devoted to preparing EHRs for certification. HIMSS members also indicate that a much more significant investment of both time and resources is required to prepare modular systems for certification. HIMSS is concerned ONC's cost estimate is low and will work with ONC to provide additional information for consideration.

The Office of the National Coordinator has requested comments on their analysis that most if not all current and potential EHR vendors would exceed the Small Business size standard ($25 million in annual receipts or smaller) due to the required amount of upfront capital needed to develop and market HIT in the marketplace. HIMSS welcomes the opportunity to comment on this analysis. Citing this data with permission from CCHIT, the below data was presented in a CCHIT Town Hall at HIMSS09, April 5, 2009. As presented in the CCHIT Town Hall slides, http://www.slideshare.net/cchit/cchit-town-hall-himss-09 , CCHIT had gathered data on (slide 18) the annual revenue and practices sizes served among the ambulatory vendors applying for certification as follows:

- 7% annual revenue > $100 Million
- 9% annual revenue between $21-$100 Million
- 13% annual revenue between $11-$20 Million
- 25% annual revenue < $1 Million
- 37% annual revenue between $1-$10 Million

The approximate % of practice sizes served by the vendors applying showing number of physicians in the practice
74% - 1 Physician in the Practice
85% - 2-5 Physicians in the Practice
85% - 6-15 Physicians in the Practice
70% - 16-50 Physicians in the Practice
50% - >50 Physicians in the Practice

Additionally, CCHIT also reported in the April 2009 Town Hall that there was a sharp increase in the number of applications for Certification. Prior to ARRA being signed, CCHIT averaged five applications per month for certification, and in the three weeks following ARRA being signed, 43 vendors applied for certification. Clearly there was a stimulus effect on certifications around ARRA signing.

Conclusion

The American Recovery and Reinvestment Act created many challenges and opportunities for the federal government and the healthcare community. We appreciate your effort to engage healthcare stakeholders in reviewing the guidance document, and look forward to future dialogue with HHS on this important issue. Our staff points of contact are Mr. Thomas M. Leary, Sr. Director for Federal Affairs.

Sincerely,

Barry P. Chaiken, MD, FHIMSS
Chair, HIMSS Board of Directors
CMO, DocsNetwork, Ltd.
CMO, Imprivata, Inc.

H. Stephen Lieber, CAE
President/CEO
HIMSS

392
393 **Appendix 1: HIMSS Comments on Certification Criteria Table 1**
394

Proposed Meaningful Use Stage 1 Objectives	Certification Criteria to support Stage 1 for Eligible Providers	Certification Criteria to support Stage 1 for Hospitals	HIMSS Comments
Use CPOE.	Enable a user to electronically retrieve, and manage at a minimum, the following order types: 1) Medications 2) Laboratory 3) Radiology/Imaging 4) Provider Referrals	Enable a user to electronically retrieve, and manage at a minimum, the following order types: 1) Medications 2) Laboratory 3) Radiology/Imaging 4) Blood Bank 5) Physical Therapy 6) Occupational Therapy 7) Respiratory Therapy 8) Rehabilitation Therapy 9) Dialysis 10) Provider Consults 11) Discharge and Transfers 12) Dietary	HIMSS believes this requirement is ambiguous. HIMSS requests clarification stating if the intention is to create orders or track results. CPOE will generate orders, but a certified CPOE must have the capability to capture data other than code including details, dose, route, and time of order. HIMSS requests clarification on the term "manage." In the context of the IFR, is the intent that the users package the order to send out to another system or manage the order internally? HIMSS members have suggested using the Joint Commission Verification Requirements Definition of "Manage." HIMSS recommends expanding the scope beyond hospital inpatient only. The IFR should allow hospitals the option to select the venue of care Members of HIMSS Ambulatory community also are concerned regarding radiology and laboratory requirements placed on CPOE. Many ambulatory care providers utilize an external service (an example would be Quest Diagnostics for laboratory diagnostics). HIMSS seeks clarification stating if ambulatory care EHRs would not be certified if the system owner uses an outside system.
Implement drug-drug,	1. Automatically and electronically	1. Automatically and electronically	HIMSS is concerned that the requirement for drug checking seems

drug allergy, drug formulary checks/ Maintain an up-to-date problem list of current and active diagnoses based on ICD-9-CM or SNOMED CT.	generate and indicate (e.g., pop-up message or sound) in real-time, alerts at the point of care for drug-drug and drug-allergy contraindications based on medication list, medication allergy list, age, and CPOE. 2. Enable a user to electronically check if drugs are in a formulary or preferred drug list in accordance with the standard specified in Table 2A row 2. 3. Provide certain users with administrator rights to deactivate, modify, and add rules for drug and drug-allergy checking. 4. Automatically and electronically track, record, and generate reports on the number of alerts responded to by a user. Enable a user to electronically record, modify and retrieve a patients problem list for longitudinal care (i.e. over multiple	generate and indicate (e.g., pop-up message or sound) in real-time, alerts at the point of care for drug-drug and drug-allergy contraindications based on medication list, medication allergy list, age, and CPOE. 2. Enable a user to electronically check if drugs are in a formulary or preferred drug list in accordance with the standard specified in Table 2A row 2. 3. Provide certain users with administrator rights to deactivate, modify, and add rules for drug and drug-allergy checking. 4. Automatically and electronically track, record, and generate reports on the number of alerts responded to by a user. Enable a user to electronically record, modify and retrieve a patients problem list for longitudinal care (i.e. over multiple	potentially problematic, since implementers often run into trouble with low specificity, alert fatigue, etc. when initially implementing these checks/alerts. One can imagine this functionality being widely enabled quickly, and the potential negative outcomes that could result. HIMSS and many other organizations have provided guidance to leverage these best practices to help mitigate this risk. Regarding the electronic tracking and reporting of alerts, HIMSS members request a clear definition or standard of what type of transmission constitutes an “alert” Regarding workflow, HIMSS members would like to state that many problem lists are currently maintained by hospital nursing staffs. Nurses and other staff members would need to be retrained to meet requirement. Finally, HIMSS recommends that hospital requirement#2 should require a hospital formulary rather than electronic prescribing. E-Prescribing isn’t required for hospital setting. Formulary modules of a certified hospital EHR should include a mode of suggesting a generic replacement for the formulary.

	office visits) in accordance with applicable standards specified in table 2A, row 1	office visits) in accordance with applicable standards specified in table 2A, row 1	
Generate and transmit permissible prescriptions electronically (e-RX).	Enable a user to electronically transmit medication orders (prescriptions) for patients in accordance with the standards specified in Table 2A row 3.	None associated with Meaningful Use	HIMSS recommends a notation that E-Prescribing requirements must meet state board of pharmacy requirements.
Maintain active medication list.	Enable a user to electronically record, modify, and retrieve a patient's active medication list as well as medication history for longitudinal care (i.e., over multiple office visits) in accordance with the applicable standard specified in Table 2A row 1.	Enable a user to electronically record, modify, and retrieve a patient's active medication list as well as medication history for longitudinal care (i.e., over multiple office visits) in accordance with the applicable standard specified in Table 2A row 1.	Under the Eligible Hospital criteria, the term "office visits" should be replaced with an alternative term. The acute care environment doesn't lend itself to multiple office visits. HIMSS recommends using the term "hospital visit" in place of "office visits" for the eligible hospital requirement.
Maintain active medication allergy list.	Enable a user to electronically record, modify, and retrieve a patient's active medication allergy list as well as medication allergy history for longitudinal care (i.e., over multiple office visits).	Enable a user to electronically record, modify, and retrieve a patient's active medication allergy list as well as medication allergy history for longitudinal care (i.e., over multiple office visits).	HIMSS recommends that a certified EHR should feature a full allergy list, not just medication allergies. HIMSS also notes that no standards for allergy lists exist for EHR modules.

Record demographics.	Enable a user to electronically record, modify, and retrieve patient demographic data including preferred language, insurance type, gender, race, ethnicity, and date of birth.	Enable a user to electronically record, modify, and retrieve patient demographic data including preferred language, insurance type, gender, race, ethnicity, date of birth, and date and cause of death in the event of mortality.	HIMSS would like to comment that the EHR should not be and never has been used as a repository for cause of death information. HIMSS members again express concern over the impact of these criteria to modular systems. Demographics change between demographics, and standards would be required to support merging demographics.
Record and chart changes in vital signs: • Height • Weight • Blood pressure • Calculate and display: BMI • Plot and display growth charts for children 2–20 years, including BMI. Record smoking status in patients 13 or older. Incorporate clinical lab-test results into EHR as structured data. Generate lists of patients by specific conditions to use for quality	1. Enable a user to electronically record, modify, and retrieve a patient's vital signs including, at minimum, the height, weight, blood pressure, temperature, and pulse. 2. Automatically calculate and display body mass index (BMI) based on a patient's height and weight. 3. Plot and electronically display, upon request, growth charts (height, weight, and BMI) for patients 2-20 years old Enable a user to electronically record, modify, and retrieve the smoking status of a patient to: current	1. Enable a user to electronically record, modify, and retrieve a patient's vital signs including, at a minimum, the height, weight, blood pressure, temperature, and pulse. 2. Automatically calculate and display body mass index (BMI) based on a patient's height and weight. 3. Plot and electronically display, upon request, growth charts (height, weight, and BMI) for patients 2-20 years old Enable a user to electronically record, modify, and retrieve the smoking status of a patient to: current	HIMSS feels that maintaining a growth chart in a hospital setting is not a normal function (unless the acute facility in question is a children's hospital) and should be removed from the eligible hospital criteria. HIMSS seeks clarification. Are all types of eligible providers, including specialists required to keep an entire list of records? HIMSS requests clarification on how to handle unstructured data and display attachments. HIMSS members are concerned that this requirement assumes that all received data must and will have LOINC codes? Not all data have LOINC codes. -

improvement, reduction of disparities, and outreach. Report quality measures to CMS or the States.	smoker, former smoker, or never smoked. 1. Electronically receive clinical laboratory test results in a structured format and display such results in human readable format. 2. Electronically display in human readable format any clinical laboratory tests that have been received with LOINC® codes. 3. Electronically display all the information for a test report specified at 42 CFR 493.1291(c)(1) through (7).6 4. Enable a user to electronically update a patient's record based upon received laboratory test results. Enable a user to electronically select, sort, retrieve, and output a list of patients and patients' clinical information, based on user-defined demographic data, medication list, and specific	smoker, former smoker, or never smoked. 1. Electronically receive clinical laboratory test results in a structured format and display such results in human readable format. 2. Electronically display in human readable format any clinical laboratory tests that have been received with LOINC® codes. 3. Electronically display all the information for a test report specified at 42 CFR 493.1291(c)(1) through (7).6 4. Enable a user to electronically update a patient's record based upon received laboratory test results. Enable a user to electronically select, sort, retrieve, and output a list of patients and patients' clinical information, based on user-defined demographic data, medication list, and specific	

	conditions 1. Calculate and electronically display quality measure results as specified by CMS or states. 2. Enable a user to electronically submit calculated quality measures in accordance with the standard specified in Table 2A row 5.	conditions 1. Calculate and electronically display quality measure results as specified by CMS or states. 2. Enable a user to electronically submit calculated quality measures in accordance with the standard specified in Table 2A row 5.	
Send reminders to patients per patient preference for preventive or follow up care.	Electronically generate, upon request, a patient reminder list for preventive or follow-up care according to patient preferences based on demographic data, specific conditions, and/or medication list.	No Associated Proposed Meaningful Use Stage 1 Objective.	HIMSS would like to note that the CMS Meaningful Use NPRM requires a specific time frame for sending reminders. HIMSS recommends that this provision include the same specific timeframe.
Implement 5 clinical decision support rules.	1. Implement automated, electronic clinical decision support rules (in addition to drug-drug and drug-allergy contraindication checking) according to specialty or clinical priorities that use demographic data, specific patient diagnoses,	1. Implement automated, electronic clinical decision support rules (in addition to drug-drug and drug-allergy contraindication checking) according to specialty or clinical priorities that use demographic data, specific patient diagnoses,	HIMSS members request clarification on the meaning of "rule." HIMSS members understand "rule" as an interruptive alert. HIMSS notes that there are many ways to address quality measures and support outside of rules. If rules, as defined as an interruptive alert, are utilized in the final rule, AHRQ Recommendations http://himssclinicaldecisionsupportwiki.pbworks.com/AHRQ-eRecommendations-Template:-Feedback-and-Discussion will help support CDS rules. HIMSS welcomes the opportunity to

	conditions, diagnostic test results and/or patient medication list. 2. Automatically and electronically generate and indicate (e.g., pop-up message or sound) in real-time, alerts and care suggestions based upon clinical decision support rules and evidence grade. 3. Automatically and electronically track, record, and generate reports on the number of alerts responded to by a user.	conditions, diagnostic test results and/or patient medication list. 2. Automatically and electronically generate and indicate (e.g., pop-up message or sound) in real-time, alerts and care suggestions based upon clinical decision support rules and evidence grade. 3. Automatically and electronically track, record, and generate reports on the number of alerts responded to by a user.	comment regarding the requirement for automatic drug-drug interaction. Many CDS/CIS implementers find that turning on Drug-Drug Interactions (DDI) alerts, even after selecting the 'high severity' subset of alert triggers, results in significant problems with 'alert overload' from false negative alerting and consequent clinician concerns over inappropriate workflow interruption. Requiring alerts be 'turned on' could result in widespread, negative/unintended consequences via workflow disruptions unless this problem is appropriately addressed. HIMSS notes that drug-drug interaction alerts are sometimes likely more doable than helpful to quality of care and patient safety. HIMSS recommends utilizing a finer set of criteria following implementation guidance from HIMSS on deploying drug-drug interaction alerts effectively (www.himss.org/cdsguide). HIMSS recommends the implementation of decision support rules applied at the appropriate point of care with one example of each of the following: - alerts at point of ordering - at point of medication/immunization administration - alerts when clinically relevant data are received or entered outside of the above processes.
Check insurance eligibility electronically from public and private payers. Submit claims	Enable a user to electronically record and display patients' insurance eligibility, and submit insurance eligibility queries to public or private payers and receive	Enable a user to electronically record and display patients' insurance eligibility, and submit insurance eligibility queries to public or private payers and receive	HIMSS supports a push towards administrative simplification industry wide using the Council on Operating Rules for Eligibility (CORE) process. HIMSS notes that effective administrative simplification results can be realized when all stakeholders support the CORE rules, which includes clearinghouses and payors, as

electronically to public and private payers.	an eligibility response in accordance with the applicable standards specified in Table 2A row 4. Enable a user to electronically submit claims to public or private payers in accordance with the applicable standards specified in Table 2A row 4.	an eligibility response in accordance with the applicable standards specified in Table 2A row 4. Enable a user to electronically submit claims to public or private payers in accordance with the applicable standards specified in Table 2A row 4.	well as the software system vendors as well as providers. CORE rules are currently able to support and facilitate administrative simplification as outlined in the MU requirements. CORE Phase II is currently being implemented in the industry and we look forward to maturation of eligibility verification based on CORE Phase II by 2014.
Provide patients with an electronic copy of their health information upon request. Provide patients with an electronic copy of their discharge instructions and procedures at time of discharge, upon request. Provide patients with timely electronic access to their health information (including lab results, problem list,	Enable a user to create an electronic copy of a patient's clinical information, including, at a minimum, diagnostic test results, problem list, medication list, medication allergy list, immunizations, and procedures in: (1) Human readable format; and (2) accordance with the standards% specified in Table 2A row 1 to provide to a patient on electronic media, or through some other electronic means. Enable a user to provide patients	Enable a user to create an electronic copy of a patient's clinical information, including, at a minimum, diagnostic test results, problem list, medication list, medication allergy list, immunizations, discharge summary, and procedures in: (1) Human readable format; and (2) accordance with the standards% specified in Table 2A row 1 to provide to a patient on electronic media, or through some other electronic means. Enable a user to	The stated requirement indicates that internal problem lists must be mapped to ICD-9 or SNOMED-CT. HIMSS recommends language recognizing the eventual transition to ICD-10 HIMSS requests clarification on several criteria listed under this section: • Please clarify, when does a diagnosis become inactive? • Please clarify, how to operationalize current vs. non-current? • HIMSS requests a definition of "patient's problem list". Please specify, is it a problem list or a diagnosis list? HIMSS recommends that Eligible Hospital criteria should be exactly the same as the Eligible Professional criteria to enable patients to have access to their records. HIMSS would like to recognize and

medication lists, allergies) within 96 hours of the information being available to the eligible professional. Provide clinical summaries for patients for each office visit.	with online access to their clinical information, including, at a minimum, lab test results, problem list, medication list, medication allergy list, immunizations, and procedures. 1. Enable a user to provide clinical summaries to patients (in paper or electronic form) for each office visit that include, at a minimum, diagnostic test results, medication list, medication allergy list, procedures, problem list, and immunizations. 2. If the clinical summary is provided electronically (i.e., not printed), it must be provided in: (1) Human readable format; and (2) accordance with the standards% specified in Table 2A row 1 to provide to a patient on electronic media, or through some other electronic	create an electronic copy of the discharge instructions and procedures for a patient, in human readable format, at the time of discharge to provide to a patient on electronic media, or through some other electronic means.	note the potential burden on nursing in the acute care setting at time of discharge. Nurses would be required to provide clinical summaries and track compliance, slowing workflow. HIMSS members are concerned that "Electronic copy in a human readable format" is too vague. HIMSS recommends the inclusion of a standard readable format in order to ensure compliance.

	means		
Capability to exchange key clinical information among providers of care and patient authorized entities electronically. Provide summary care record for each transition of care and referral.	1. Electronically receive a patient summary record, from other providers and organizations including, at a minimum, diagnostic test results, problem list, medication list, medication allergy list, immunizations, and procedures and upon receipt of a patient summary record formatted in an alternative standard specified in Table 2A row 1, displaying it in human readable format. 2. Enable a user to electronically transmit a patient summary record to other providers and organizations including, at a minimum, diagnostic test results, problem list, medication list, medication allergy list, immunizations, and procedures in accordance with the standards% specified in Table 2A row 1.	1. Electronically receive a patient summary record, from other providers and organizations including, at a minimum, discharge summary, diagnostic test results, problem list, medication list, medication allergy list, immunizations, and procedures and upon receipt of a patient summary record formatted in an alternative standard specified in Table 2A row 1, displaying it in human readable format. 2. Enable a user to electronically transmit a patient summary record, to other providers and organizations including, at a minimum, discharge summary, diagnostic test results, problem list, medication list, medication allergy list, immunizations, and procedures in	HIMSS supports the use of CCD or CCR for Stage I and agrees one patient summary record standard should be adopted to support Meaningful Use (MU) in Stage II and beyond.

		accordance with the standards% specified in Table 2A row 1.	
Perform medication reconciliation at relevant encounters and each transition of care. Capability to submit electronic data to immunization registries and actual submission where required and accepted.	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. Electronically record, retrieve, and transmit immunization information to immunization registries in accordance with the standards specified in Table 2A row 8 or in accordance with the applicable state-designated standard format.	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. Electronically record, retrieve, and transmit immunization information to immunization registries in accordance with the standards specified in Table 2A row 8 or in accordance with the applicable state-designated standard format.	HIMSS requests clarified definitions of medication reconciliation. The medications list can be obtained from many different sources (patient memory, multiple providers, OTC). HIMSS requests clarified definitions of the immunization registry.
Capability to provide electronic submission of reportable lab results (as required by state or local law) to public health agencies and actual		Electronically record, retrieve, and transmit reportable clinical lab results to public health agencies in accordance with the standards% specified in Table 2A row 6.	HIMSS is concerned that Public Health EP's would need to have standards in place and a protocol from private providers. Without public health providers having the capabilities to receive and analyze data, the provision loses possible value.

submission where it can be received.			
Capability to provide electronic syndromic surveillance data to public health agencies and actual transmission according to applicable law and practice. Protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities.	Electronically record, retrieve, and transmit syndrome-based (e.g., influenza like illness) public health surveillance information to public health agencies in accordance with the standards specified in Table 2A row 7. 1. Assign a unique name and/or number for identifying and tracking user identity and establish controls that permit only authorized users to access electronic health information. 2. Permit authorized users (who are authorized for emergency situations) to access electronic health information during an emergency. 3. Terminate an electronic session after a predetermined time of inactivity. 4. Encrypt and decrypt electronic	Electronically record, retrieve, and transmit syndrome-based (e.g., influenza like illness) public health surveillance information to public health agencies in accordance with the standards specified in Table 2A row 7. 1. Assign a unique name and/or number for identifying and tracking user identity and establish controls that permit only authorized users to access electronic health information. 2. Permit authorized users (who are authorized for emergency situations) to access electronic health information during an emergency. 3. Terminate an electronic session after a predetermined time of inactivity. 4. Encrypt and decrypt electronic	HIMSS is supportive of the population health objectives and measures included in the CMS Proposed Rule. HIMSS believes that the public health reporting requirements strike the correct balance between advancing the use of data for population health improvement and recognizing the limitations that exist with the current health information technology infrastructure. HIMSS recognizes the infrastructure necessary to support the electronic exchange of information with public health departments is still to be developed in many parts of the country. This is particularly true for local health departments, which have varying capacity to send and receive data electronically. This situation is likely to be slow to change given the dire budget situation in which local health departments find themselves. There is a risk that one of the five key goals identified by ONC and CMS for the use of EHR, improving population and public health, will not be achieved without additional investment. HIMSS supports efforts to find funding mechanisms for state and local health EMR implementation.

	health information according to user-defined preferences (e.g., backups, removable media, at log-on/off) in accordance with the standard specified in Table 2B row 1. 5. Encrypt and decrypt electronic health information when exchanged in accordance with the standard specified in Table 2B row 2. 6. Record actions (e.g., deletion) related to electronic health information in accordance with the standard specified in Table 2B row 3 (i.e., audit log), provide alerts based on user-defined events, and electronically display and print all or a specified set of recorded information upon request or at a set period of time. 7. Verify that electronic health information has not been altered in transit and detect the alteration and deletion of	health information according to user-defined preferences (e.g., backups, removable media, at log-on/off) in accordance with the standard specified in Table 2B row 1. 5. Encrypt and decrypt electronic health information when exchanged in accordance with the standard specified in Table 2B row 2. 6. Record actions (e.g., deletion) related to electronic health information in accordance with the standard specified in Table 2B row 3 (i.e., audit log), provide alerts based on user-defined events, and electronically display and print all or a specified set of recorded information upon request or at a set period of time. 7. Verify that electronic health information has not been altered in transit and detect the alteration and deletion of	

	electronic health information and audit logs in accordance with the standard specified in Table 2B row 4. 8. Verify that a person or entity seeking access to electronic health information is the one claimed and is authorized to access such information. 9. Verify that a person or entity seeking access to electronic health information across a network is the one claimed and is authorized to access such information in accordance with the standard specified in Table 2B row 5. 10. Record disclosures made for treatment, payment, and health care operations in accordance with the standard specified in Table 2B row 7	electronic health information and audit logs in accordance with the standard specified in Table 2B row 4. 8. Verify that a person or entity seeking access to electronic health information is the one claimed and is authorized to access such information. 9. Verify that a person or entity seeking access to electronic health information across a network is the one claimed and is authorized to access such information in accordance with the standard specified in Table 2B row 5. 10. Record disclosures made for treatment, payment, and health care operations in accordance with the standard specified in Table 2B row 7	

401 **Appendix 2: HIMSS Comments on Privacy and Security Standards Table 2B**
402

Purpose	Adopted Standard	HIMSS Comments on Privacy and Security Standards
General Encryption and Decryption of Electronic Health Information.	A symmetric 128 bit fixed-block cipher algorithm capable of using a 128, 192, or 256 bit encryption key must be used (*e.g.*, FIPS 197 Advanced Encryption Standard, (AES), Nov 2001)	**COMMENT 1** - This row does not specify an encryption standard, just some bit values. Those bit values are only inherent in AES. Requiring AES is potentially troublesome for the healthcare industry as it is not available with commonly used platforms such as Windows XP, 2000. (It is only available with more recent versions such as Windows VISTA, 7.) Instead we recommend specifying the algorithm set that is defined in FIPS 140-2 Annex A while noting that Annex A is in draft form. (Note – The US Government does not mandate AES, it mandates the FIPS standard above) For example for FISMA, currently Triple DES is in there and is acceptable and is currently available in all platforms **COMMENT 2** – The scope of this requirement is unclear - does this apply to encryption of only data in transmission, or does it apply to data at rest as well? (The standard listed in row 2 of this table is clearly for data exchange.) It may be best to specify the security requirements for data at rest as separate from EHR requirements, as these may be best handled operationally though the risk assessment and mitigation activities required by HIPAA

		COMMENT 3 - The IFR does not specify end point system-to-system authentication – must ensure that the EHR is talking to a trusted system. **COMMENT 4** - The goal is unclear – to ensure interoperability both sender and receiver may need to follow a specific standard. The goal of this IFR must be to support secure interoperability. HIMSS would like to note to HHS/ONC that many challenges remain in interoperability of vendor encryption and key management solutions across networks and while OASIS has developed a "Key Management Integration Protocol" standard, ("KMIP) that standard is under review as a "new work item" in multiple venues and requires testing and validation among a set of multiple public/private stakeholders. **COMMENT 5** - There appears to be some confusion of functional, interoperability and operational requirements. For example, an enterprise can implement encryption operationally. That is, servers can have encryption that would suffice for data at rest but not involve the EHR. Since this IFR is setting requirements for an EHR, it is not clear if ONC considered alternate scenarios for data encryption. We also need to determine the most appropriate way of implementing requirements other than at the EHR (e.g operational requirements can be fully met in ways that are independent of the EHR used.) Also, security objectives can be met in

		ways other than encryption. For example, there is a question as to whether encryption of data at rest is needed when data is stored in a physically secure data center Enterprises should enable encryption on portable/external devices, for example, Laptops, USBs, etc. for export and import. Encryption can be applied to these devices that are separate from the EHR. **COMMENT 6** – It is unclear how this requirement applies to modular systems. Does this requirement apply to each EHR module? Do internal transactions between modular units require encryption (e.g., ATD transactions)? What about other application such CCOW that are agnostic to the underlying security and encryption? Modularity causes difficulty with security and privacy. Security and privacy can only be evaluated when the complete system is brought together. Modules may have no inherent security controls as those may be part of the platform and integration components (e.g., CCOW, Web-service, Browser plug-in). Modules may rely on the implemented environment to provide security functions, may produce audit logs but leverage platform for secure access and communications. Is it possible that for modules that are undergoing certification that the vendor could declare *how the module should be implemented* such that it meets security/privacy objectives?
Encryption and Decryption of Electronic Health	An encrypted and integrity protected link must be implemented (*e.g.*, TLS, IPv6,	**COMMENT 1** – It is clear that this row is specific to exchange – is this for *just* health information exchange across

Information for Exchange.	IPv4 with IPsec).∂	organizational boundaries or should it be applied to all networked communications inside an organization (e.g., ADT feeds, orders and observations, etc.)? From the IHE perspective, ATNA defines the use of TLS, mutually authenticated using AES encryption and SHA 1 hash. This was chosen to ensure interoperability. We need to balance highly secure with interoperable. If we are trying to drive interoperability, then the IFR needs to be specific to ensure interoperability. Specify the EHR communications across organizational boundaries that Transport Layer Security with authentication of both endpoints and encryption be at least 3DES with AES available at later stages. The IFR normative text does not require any form of authentication. We believe there is a clear need for enterprise authentication in 2011.
Record Actions Related to Electronic Health Information (i.e., audit log).	The date, time, patient identification (name or number), and user identification (name or number) must be recorded when electronic health information is created, modified, deleted, or printed. An indication of which action(s) occurred must also be recorded (*e.g.,* modification).∂	**COMMENT 1** – Here, Table 2B is different than normative section – there is an addition requirement for alerts for security incidents. In the table, they have added in the last sent "an indication…." This is non-trivial to implement and should not be in 2011. Recommend delete from table. **COMMENT 2 -** The list of auditable events is *very* comprehensive. It may be best to constrain to those that are related to information exchange across organizational boundaries. Recommend that this applies to events that are related to HIE transactions.
Verification that	A secure hashing algorithm must	**COMMENT 1** – Here again , Table 2B

Electronic Health Information has not been Altered in Transit.	be used to verify that electronic health information has not been altered in transit. The secure hash algorithm used must be SHA–1 or higher (*e.g.,* Federal Information Processing Standards (FIPS) Publication (PUB) Secure Hash Standard (SHS) FIPS PUB 180–3).∂	is different than normative section There is text in the normative section presents expectations about what SHA 1 can do (for example, send alerts or integrity failures). SHA 1 is an algorithm that calculates a value and returns a result. Some separate application would have to note detection of a matching failure and send an alert.
Cross-Enterprise Authentication.	Use of a cross-enterprise secure transaction that contains sufficient identity information such that the receiver can make access control decisions and produce detailed and accurate security audit trails (*e.g.,* IHE Cross Enterprise User Assertion (XUA) with SAML identity assertions).∂	**COMMENT 1** – There is not sufficient infrastructure to support this requirement today. It is impossible for most organizations to support SAML 2.0 for 2011. Only a few may have Active Directory in place. Active Directory modifications were just released last month. We suggest that for 2011, we require only mutual authentication of endpoints of a network communication to assure that systems only talk to authorized systems that have proven operationally that they can enforce necessary access controls and audit logs. **COMMENT 2** – The example in the informative section (Table 2B) (XUA) is for application-based *user* authentication. This requirement should be for truly system-system authentication for 2011 (e.g., TLS) Authentication is not in the normative section. Recommend adding or otherwise making consistent with informative section (Table 2B). **COMMENT 3** – Please clarify if "receiver" is only external or also includes internal.
Record Treatment,	The date, time, patient	**COMMENT 1** – This row causes

Payment, and Health Care Operations Disclosures.	identification (name or number), user identification (name or number), and a description of the disclosure must be recorded.∂	confusion and scoping issues with respect to forthcoming Accounting of Disclosures regulation. Perhaps wait for or defer to this forthcoming regulation. **COMMENT 2** – This requirement does not seem to recognize that creating an Accounting of Disclosures is not a real-time event, but may require post processing of 4-5 audit events. However, it is written here as real-time implementation that is to be "recorded." **COMMENT 3** – Security logs contain identifiers and not descriptive values (e.g., user name) They are real-time audit logs that are focused on recording all security events without regard to if the event is used in an Accounting of Disclosures. Linkages of data and inferences to disclosures are made in post-processing. Imbedding descriptive items in the security log would make the audit log itself PHI. Recommend clearly separating the requirements of the EHR/security audit log from the operational requirement to create an Accounting of Disclosures for a patient.
MISCELLANEOUS		HIMSS notes that Privacy requirements were not included in this IFR. We also note that the topic of consent management is under discussion in the HIT Policy and HIT Standards Committees and this may be a future requirement. If this is the case, then the development of Privacy requirements should be road mapped.

403