DEPARTMENT OF VETERANS AFFAIRS

March 4, 2011

The Department of Veterans Affairs appreciates the opportunity to respond to the request for information published in the Federal Register, Volume 75, No. 235 on Wednesday December 8, 2010. This request for information (RFI) asks interested parties to provide information on the effectiveness of federal agencies participation in the development and implementation of standards and conformity assessment activities and programs.

The United States (U.S.) Department of Veterans Affairs (VA) honors our Nation's Veterans by providing quality health care to Veterans and their families. The Veterans Health Administration (VHA) is the largest provider of health care in the U.S. and has been recognized as a leader in its use of health care information technology (IT). Within VHA, the Office of Health Information (OHI) supports Veterans, doctors, nurses, and other health care providers by defining the requirements and direction of VA's electronic health care system known as Veterans Health Information Systems and Technology Architecture (VistA). A critical component of the health IT standards work performed by VHA OHI resources are under the auspices of the Chief Health Informatics Office (CHIO).

CHIO represents VA in voluntary consensus standards bodies and implements the standards developed by those organizations within VA systems in accordance with Office of Management and Budget (OMB) Circular A-119, and the National Technology Transfer and Advancement Act of 1995 (NTTAA). Additional federal mandates, such as Title XIII of the American Recovery and Reinvestment Act (ARRA), subtitle Health Information Technology for Economic and Clinical Health Act (HITECH), which establishes target dates for health care providers to meet requirements for the "Meaningful Use" of electronic health records (EHR), further drive VA's engagement with Standards Developing Organizations (SDOs). There presently exist over two dozen health IT SDOs with which CHIO resources engage, actively participate, or provide a leadership role as appropriate to support VA's mission.

In addition to participating in SDOs to meet the requirements of federal mandates and initiatives as referenced above, VA participates to provide Veterans and their families with increased safety to improve patient experience and to realize cost savings for VA. Health care standards allow consistency of the medical record so that providers can exchange health information and also use the data for clinical decision support. This consistency of the medical record between providers significantly reduces medication errors, duplicate testing, and other dangerous errors by ensuring that all VA clinicians have accurate and up-to-date records. Messaging standards define how this health data is sent from one provider to another so that the data is understood by the EHR system. Standardized messaging saves money by eliminating the custom interfaces and code translations required if each provider or medical device vendor develops idiosyncratic methods of exchange. Additionally, information security standards protect patients' personally identifiable information and medical history as information is stored electronically and shared between providers. These advantages ultimately improve the support and services VA provides to our Nation's Veterans.

SDO participation also decreases the expense to VA of implementing required or beneficial standards. VA standards resources ensure that SDOs consider VA needs as they develop new or improve existing standards. It is more efficient for VA to engage in standards development than to accept the risk of having to implement standards that do not fully meet, or possibly contradict, VA's needs, which would then require VA to expend resources developing workarounds or redundant systems. Similarly, VA's role in SDOs facilitates the improvement of standards required for Meaningful Use certification.

Additionally, VA's effort to promote Unified Modeling Language (UML)-based standards development results in standards that are easier and less costly for developers to implement in solutions. VA has successfully introduced model based standards development in the National Council for Prescription Drug Programs (NCPDP) (see Appendix A) and intends to leverage this success to influence practices within Health Level Seven (HL7) and the Accredited Standards Committee (ASC) X12. VA is also promoting Model Driven Health Tools (MDHT) developed by VA in collaboration with Open Health Tools (OHT), to help SDOs and other federal agencies, such as the Department of Health and Human Services (HHS) Office of the National Coordinator for Health Information Technology (ONC), adopt a model driven approach to standards.

One of VA's earliest and most prominent successes in the standards arena was the creation of the HL7 Electronic Health Record System Functional Model (EHR-S FM) (see Appendix B - C). The model includes a description of EHR functionality that can be used to facilitate communication between clinicians and technology providers to ensure the right information is being made available for the right reason. VA standards resources took internal business owners' requirements to HL7 and led the creation of the EHR-S FM that lists the set of all functions and the conformance criteria that should be present in EHR systems.

Within HL7, VA has also played a significant role in helping to define policy, governance and processes. VA and others identified the need for formalization of processes at HL7 and drove this change through the Process Improvement Committee (PIC). HL7 created this ongoing committee in response to VA's petition to the HL7 Board to transform the SDO into a project focused organization and with improved openness and flexibility. VA resources led the PIC and worked with other HL7 members to define and institute process and governance documents, including the Decision Making Processes (DMP) and the HL7 Roadmap. More recently, VA resources have improved HL7 processes by significantly supporting approaches such as the HL7 Development Framework (HDF) and the HL7's "Service Aware Interoperability Framework (SAIF) and Sound" approach to standards development, which demonstrates how SAIF allows standards to be created and ready for implementation in a single year.

The security of information contained in the EHR and shared with trading partners is an important concern to VA. To this end, VA partners with the Organization for the Advancement of Structured Information Standards (OASIS) to specify health care profiles of existing OASIS standards to achieve the goal of international security and privacy interoperability (see Appendices D - K). VA helped lead the development of critical health profiles, including:

Cross-Enterprise Security and Privacy Authorization (XSPA), Profile of the Security Assertion Markup Language (SAML) for Healthcare, XSPA Profile of the eXtensible Access Control Markup Language (XACML) for Healthcare, and the XSPA Profile of Web Services Trust (WS-Trust) for Healthcare. These profiles ensured that SAML, XACML, and WS-Trust and all existing OASIS standards met access control needs as defined by the U.S. Healthcare Information Technology Standards Panel (HITSP).

VA also participates in Global Standards One (GS1) Healthcare to develop standards to improve patient safety and supply chain efficiencies (see Appendix L). VA is active in Location Identification, Product Identification, and Traceability Adoption workgroups in GS1. Within these workgroups, VA promoted the use of the GS1 Global Location Number (GLN) and GS1 Global Trade Item Number® (GTIN®) to standardize location and product identification throughout the health care supply chain. Adoption of these standards provides traceability of medical supplies that contributes to patient safety as products move from manufacturer to end user.

VA, through its Chief Health Informatics Office (CHIO), has successfully partnered with many private SDOs and collaborated with other federal agencies promoting effective and efficient standards development processes. This resulted in standards that meet VA's and other federal agencies needs, and also benefited the private sector and public good. The above discussion of standards activities along with the attached letters of commendation and press releases citing VA's contribution to the standards community provide a snapshot of VA's involvement and speak to the positive relationships that VA has built with the private standards community.

The Department of Veterans Affairs, Veterans Health Administration, Office of Health Information, Chief Health Informatics Office officials are the points of contact and subject matter experts on health IT standards and we look forward to working with NIST officials in implementing standards and assessments to assure conformity.

Appendix A

March 24, 2010

Linda Fischetti
Chief Health Informatics Officer
Veterans Health Administration
1335 East-West Highway Suite 3100
Silver Spring, MD 20910

Re: Technical Support for Modeling

I would like to commend the Veterans Health Administration and the VHA Chief Health Informatics Office for ongoing participation with the nation’s healthcare standards development organizations and commitment to modeled, interoperable standards. The support and leadership of Dr Nelson Hsing and Frieda Hall of the VHA Chief Health Informatics Office have afforded NCPDP with the technical expertise necessary to move toward model based standards development.

Of special importance is the sharing of the talents and expertise of Galen Mulrooney and Sean Muir. They have been invaluable in assisting NCPDP in planning and building an implementable model framework and migrating to a model driven standards development environment. While the overarching model is still under development, it is anticipated that the first model-based NCPDP standard and implementation guide will move into our ballot process in August of this year. This would not have been a possibility without their assistance.

On behalf of the members, in particular the Maintenance and Control Work Group’s Modeling and Methodology Task Group, and staff of NCPDP, thank you for your commitment to and support of the NCPDP modeling effort.

Sincerely,

Lee Ann C. Stember

Lee Ann C. Stember
President
National Council for Prescription Drug Programs (NCPDP)
9240 E. Raintree Drive
Scottsdale, AZ 85260
(480) 477-1000 x 108

Lynne Gilbertson

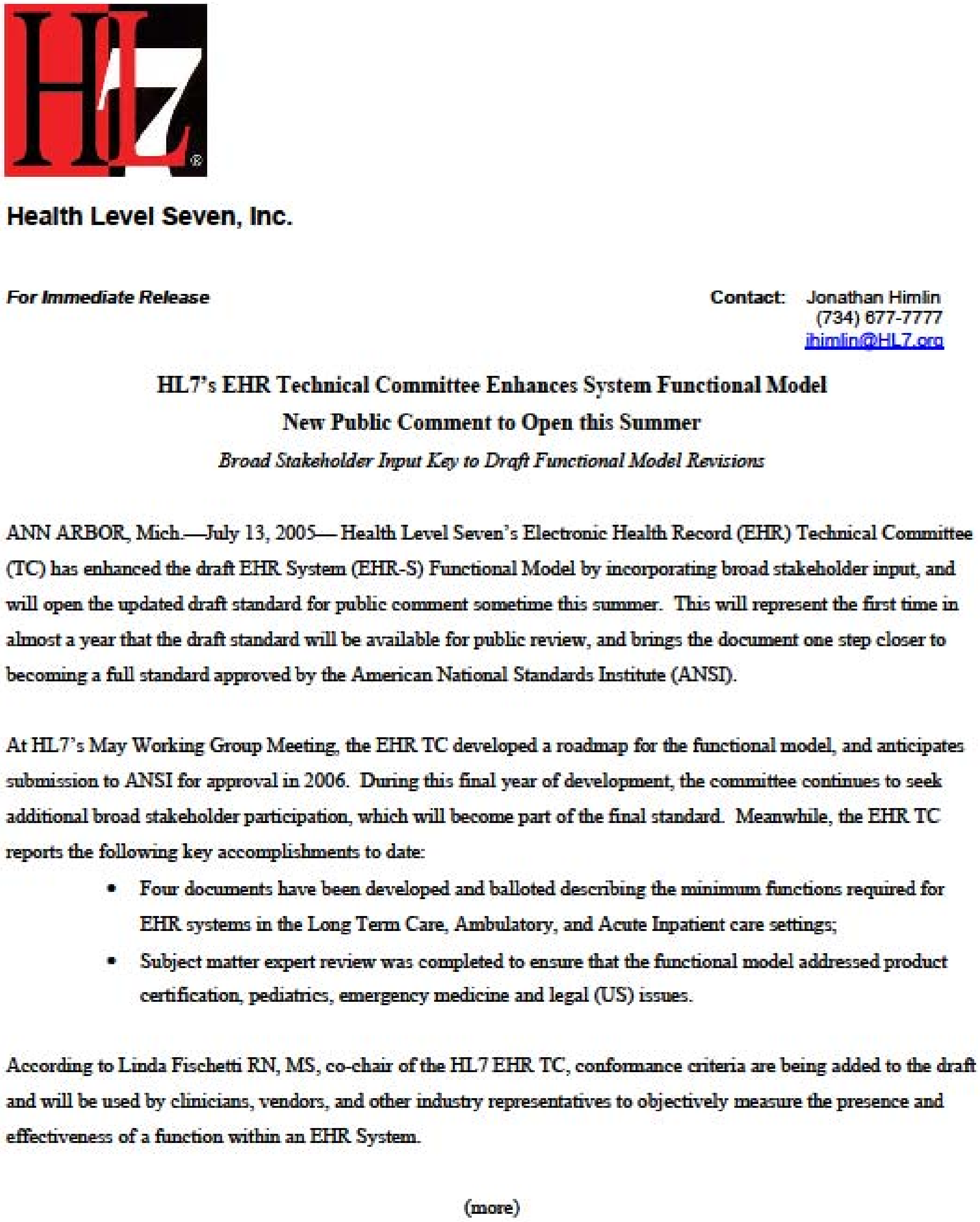
Lynne Gilbertson
VP, Standards Development
National Council for Prescription Drug Programs (NCPDP)

cc:
Tim Cromwell
Veterans Health Administration
Director Standards and Interoperability
Salt Lake City VA Regional Office
550 Foothill Drive Suite 400
Salt Lake City, UT 84113

Galen Mulrooney
Sean Muir

NCPDP Standardization Co-Chairs
NCPDP Board of Trustees

Appendix B **(double right click below to view pages 1 – 4 of PDF)**



Health Level Seven, Inc.

For Immediate Release

Contact: Jonathan Himlin
(734) 677-7777
jhimlin@HL7.org

HL7's EHR Technical Committee Enhances System Functional Model

New Public Comment to Open this Summer

Broad Stakeholder Input Key to Draft Functional Model Revisions

ANN ARBOR, Mich.—July 13, 2005— Health Level Seven's Electronic Health Record (EHR) Technical Committee (TC) has enhanced the draft EHR System (EHR-S) Functional Model by incorporating broad stakeholder input, and will open the updated draft standard for public comment sometime this summer. This will represent the first time in almost a year that the draft standard will be available for public review, and brings the document one step closer to becoming a full standard approved by the American National Standards Institute (ANSI).

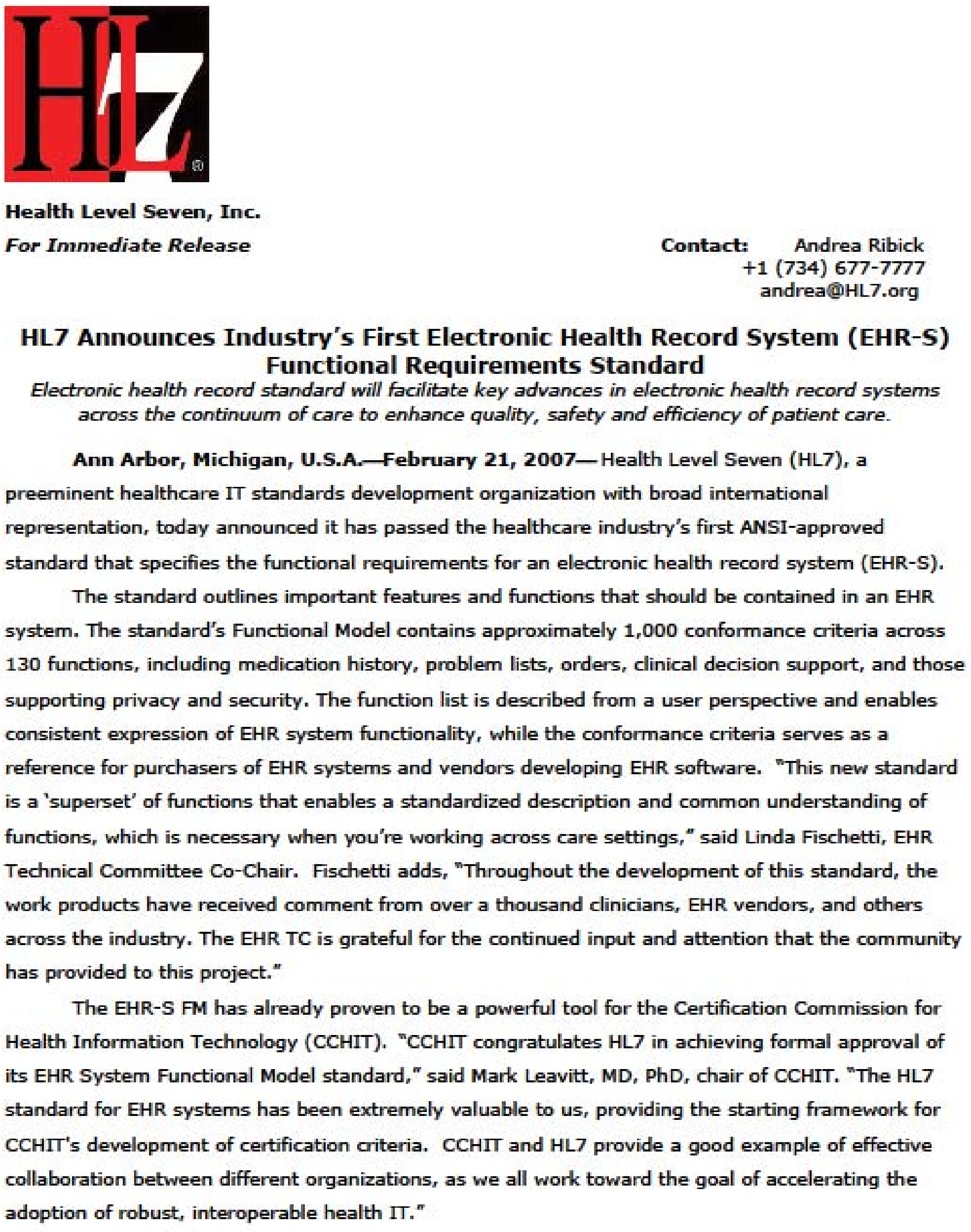
At HL7's May Working Group Meeting, the EHR TC developed a roadmap for the functional model, and anticipates submission to ANSI for approval in 2006. During this final year of development, the committee continues to seek additional broad stakeholder participation, which will become part of the final standard. Meanwhile, the EHR TC reports the following key accomplishments to date:

- Four documents have been developed and balloted describing the minimum functions required for EHR systems in the Long Term Care, Ambulatory, and Acute Inpatient care settings;
- Subject matter expert review was completed to ensure that the functional model addressed product certification, pediatrics, emergency medicine and legal (US) issues.

According to Linda Fischetti RN, MS, co-chair of the HL7 EHR TC, conformance criteria are being added to the draft and will be used by clinicians, vendors, and other industry representatives to objectively measure the presence and effectiveness of a function within an EHR System.

(more)

Appendix C (double right click below to view pages 1 - 4 of PDF)



Health Level Seven, Inc.

For Immediate Release

Contact: Andrea Ribick
+1 (734) 677-7777
andrea@HL7.org

HL7 Announces Industry's First Electronic Health Record System (EHR-S) Functional Requirements Standard

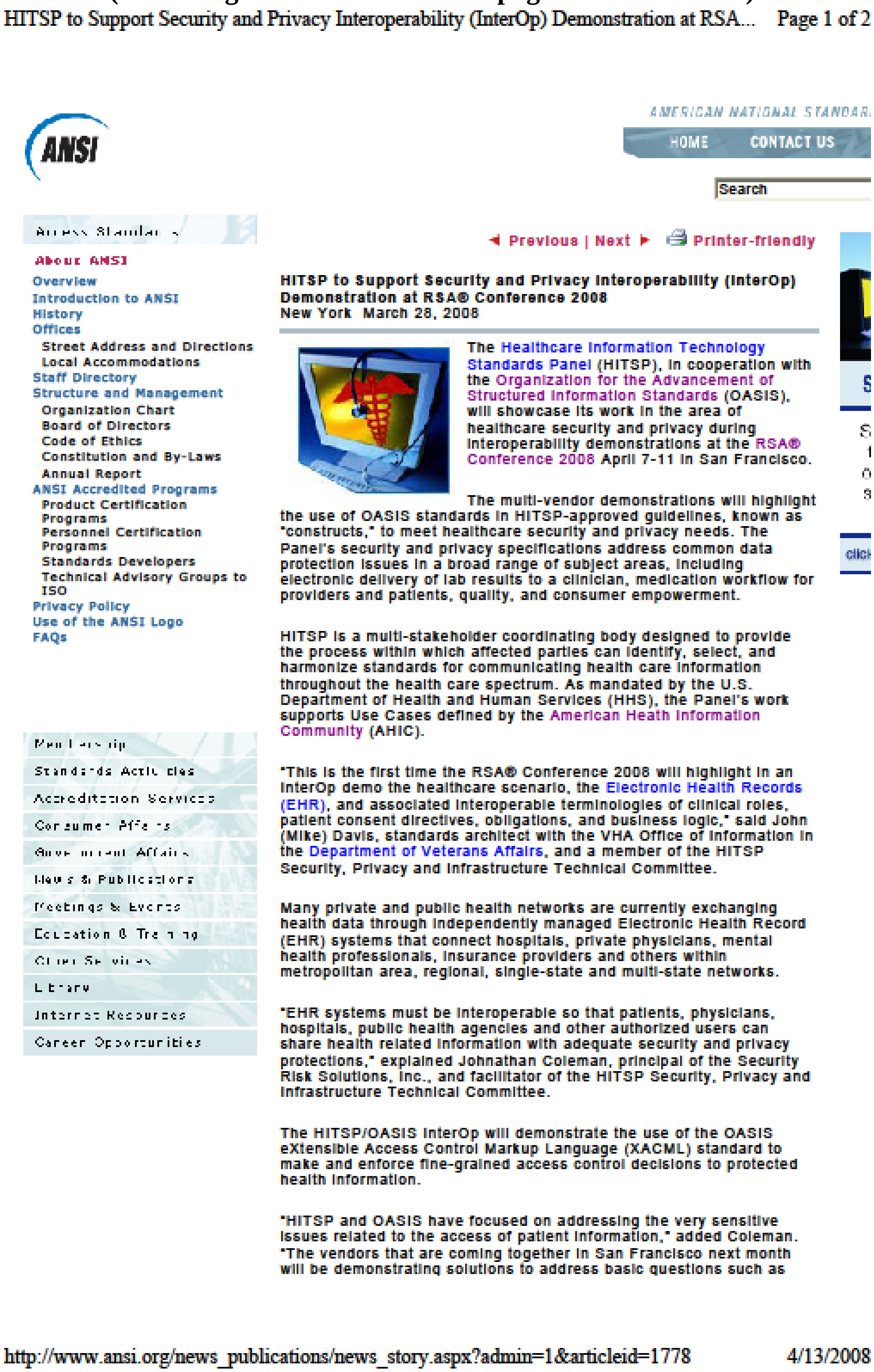
Electronic health record standard will facilitate key advances in electronic health record systems across the continuum of care to enhance quality, safety and efficiency of patient care.

Ann Arbor, Michigan, U.S.A.—February 21, 2007— Health Level Seven (HL7), a preeminent healthcare IT standards development organization with broad international representation, today announced it has passed the healthcare industry's first ANSI-approved standard that specifies the functional requirements for an electronic health record system (EHR-S).

The standard outlines important features and functions that should be contained in an EHR system. The standard's Functional Model contains approximately 1,000 conformance criteria across 130 functions, including medication history, problem lists, orders, clinical decision support, and those supporting privacy and security. The function list is described from a user perspective and enables consistent expression of EHR system functionality, while the conformance criteria serves as a reference for purchasers of EHR systems and vendors developing EHR software. "This new standard is a 'superset' of functions that enables a standardized description and common understanding of functions, which is necessary when you're working across care settings," said Linda Fischetti, EHR Technical Committee Co-Chair. Fischetti adds, "Throughout the development of this standard, the work products have received comment from over a thousand clinicians, EHR vendors, and others across the industry. The EHR TC is grateful for the continued input and attention that the community has provided to this project."

The EHR-S FM has already proven to be a powerful tool for the Certification Commission for Health Information Technology (CCHIT). "CCHIT congratulates HL7 in achieving formal approval of its EHR System Functional Model standard," said Mark Leavitt, MD, PhD, chair of CCHIT. "The HL7 standard for EHR systems has been extremely valuable to us, providing the starting framework for CCHIT's development of certification criteria. CCHIT and HL7 provide a good example of effective collaboration between different organizations, as we all work toward the goal of accelerating the adoption of robust, interoperable health IT."

Appendix D (double right click below to view pages 1 and 2 of PDF)



HITSP to Support Security and Privacy Interoperability (InterOp) Demonstration at RSA... Page 1 of 2

HITSP to Support Security and Privacy Interoperability (InterOp) Demonstration at RSA® Conference 2008
New York March 28, 2008

The Healthcare Information Technology Standards Panel (HITSP), in cooperation with the Organization for the Advancement of Structured Information Standards (OASIS), will showcase its work in the area of healthcare security and privacy during interoperability demonstrations at the RSA® Conference 2008 April 7-11 in San Francisco.

The multi-vendor demonstrations will highlight the use of OASIS standards in HITSP-approved guidelines, known as "constructs," to meet healthcare security and privacy needs. The Panel's security and privacy specifications address common data protection issues in a broad range of subject areas, including electronic delivery of lab results to a clinician, medication workflow for providers and patients, quality, and consumer empowerment.

HITSP is a multi-stakeholder coordinating body designed to provide the process within which affected parties can identify, select, and harmonize standards for communicating health care information throughout the health care spectrum. As mandated by the U.S. Department of Health and Human Services (HHS), the Panel's work supports Use Cases defined by the American Heath Information Community (AHIC).

"This is the first time the RSA® Conference 2008 will highlight in an InterOp demo the healthcare scenario, the Electronic Health Records (EHR), and associated interoperable terminologies of clinical roles, patient consent directives, obligations, and business logic," said John (Mike) Davis, standards architect with the VHA Office of Information in the Department of Veterans Affairs, and a member of the HITSP Security, Privacy and Infrastructure Technical Committee.

Many private and public health networks are currently exchanging health data through independently managed Electronic Health Record (EHR) systems that connect hospitals, private physicians, mental health professionals, insurance providers and others within metropolitan area, regional, single-state and multi-state networks.

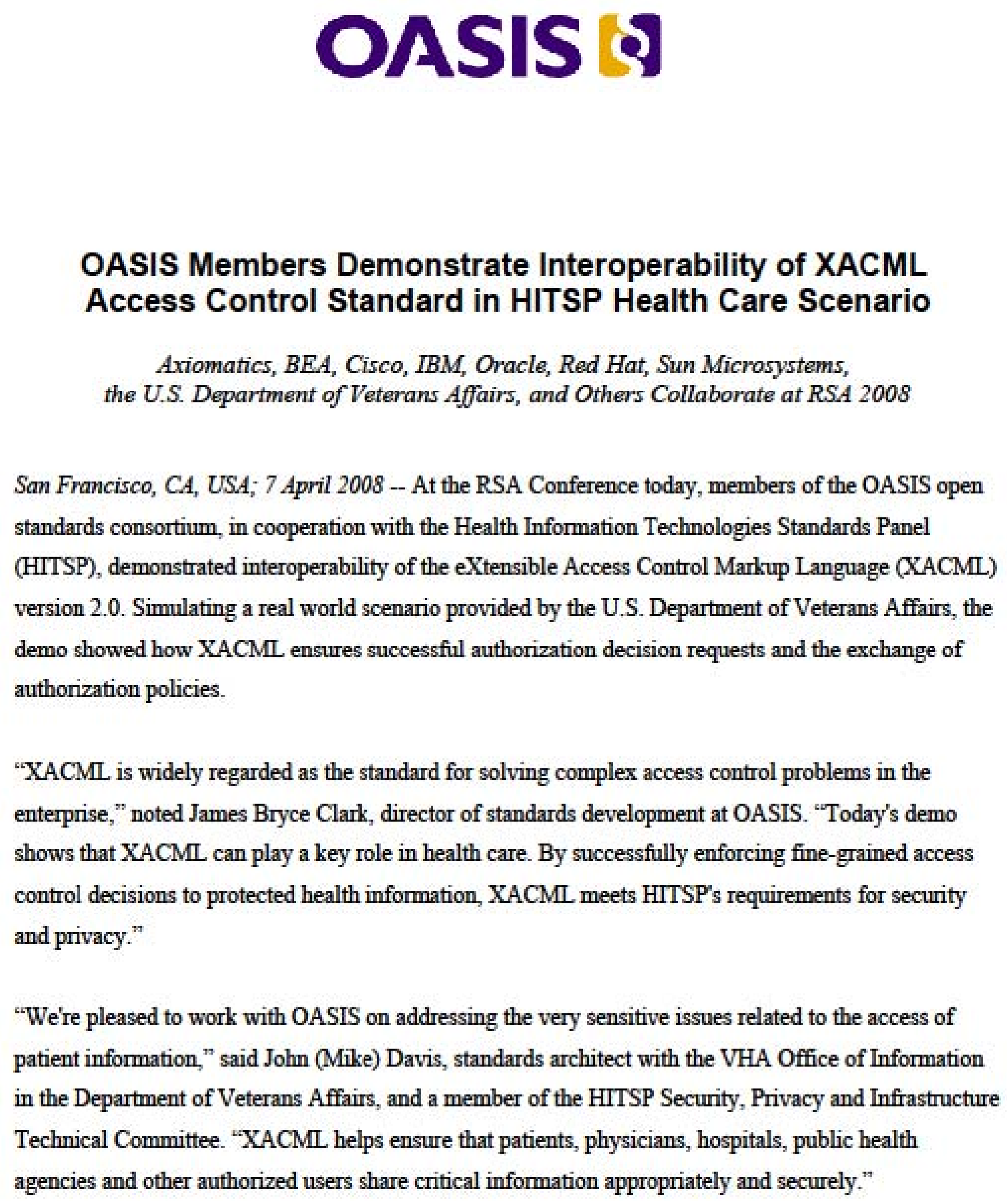
"EHR systems must be interoperable so that patients, physicians, hospitals, public health agencies and other authorized users can share health related information with adequate security and privacy protections," explained Johnathan Coleman, principal of the Security Risk Solutions, Inc., and facilitator of the HITSP Security, Privacy and Infrastructure Technical Committee.

The HITSP/OASIS InterOp will demonstrate the use of the OASIS eXtensible Access Control Markup Language (XACML) standard to make and enforce fine-grained access control decisions to protected health information.

"HITSP and OASIS have focused on addressing the very sensitive issues related to the access of patient information," added Coleman. "The vendors that are coming together in San Francisco next month will be demonstrating solutions to address basic questions such as

http://www.ansi.org/news_publications/news_story.aspx?admin=1&articleid=1778 4/13/2008

Appendix E **(double right click below to view pages 1-3 of PDF)**



OASIS

OASIS Members Demonstrate Interoperability of XACML Access Control Standard in HITSP Health Care Scenario

Axiomatics, BEA, Cisco, IBM, Oracle, Red Hat, Sun Microsystems, the U.S. Department of Veterans Affairs, and Others Collaborate at RSA 2008

San Francisco, CA, USA; 7 April 2008 -- At the RSA Conference today, members of the OASIS open standards consortium, in cooperation with the Health Information Technologies Standards Panel (HITSP), demonstrated interoperability of the eXtensible Access Control Markup Language (XACML) version 2.0. Simulating a real world scenario provided by the U.S. Department of Veterans Affairs, the demo showed how XACML ensures successful authorization decision requests and the exchange of authorization policies.

"XACML is widely regarded as the standard for solving complex access control problems in the enterprise," noted James Bryce Clark, director of standards development at OASIS. "Today's demo shows that XACML can play a key role in health care. By successfully enforcing fine-grained access control decisions to protected health information, XACML meets HITSP's requirements for security and privacy."

"We're pleased to work with OASIS on addressing the very sensitive issues related to the access of patient information," said John (Mike) Davis, standards architect with the VHA Office of Information in the Department of Veterans Affairs, and a member of the HITSP Security, Privacy and Infrastructure Technical Committee. "XACML helps ensure that patients, physicians, hospitals, public health agencies and other authorized users share critical information appropriately and securely."

Appendix F

This is a printer friendly version
To print this article open the file menu and choose Print.

Back

Article published April 10, 2008

Demo shows promise for using XACML with EMRs

By: *Joseph Conn / HITS staff writer*

A consortium of information technology vendors and the Veterans Health Administration of the Veterans Affairs Department demonstrated this week at a San Francisco trade show the use of extensible access-control markup language, known as XACML, to provide granular levels of control over access to a patient's personal healthcare information in an electronic medical-record system.

The demonstration was part of the annual RSA Conference, a meeting of computer security experts. The conference, which opened Monday and closes Friday, draws its name from the initials of the last names of three developers of an algorithm widely used in encryption.

In addition to the VA, participants in the XACML demonstration were Axiomatics, BEA Systems, IBM Corp., Oracle Corp., Red Hat, Securent and Sun Microsystems. All seven firms are members of the Organization for the Advancement of Structured Information Standards, or OASIS, a not-for-profit consortium that drives the development and adoption of open standards for computerized communication.

The vendors were demonstrating the use of XACML to implement an access-control transaction package known as TP20 developed by the Healthcare Information Technology Standards Panel.

Participants in the demonstration who could speak on the record were unavailable at deadline.

According to a member of the demonstration team who asked not to be identified, the demonstration proved that XACML could be used for role-based constraints—allowing certain physicians to see a patient record, but not others—as well as providing patients with a high degree of "granular" control over access to their records—allowing some parts of their records to be shared, but not others. The exhibit also demonstrated the use of XACML to convey requests and provide access authorizations in the event of an emergency when patient permission is unattainable, the source said.

"In healthcare, patient safety trumps security, so in the HITSP use case, we have to be able to demonstrate a 'break the glass' mechanism," the source said.

In a news release, James Clark, director of standards development at OASIS said XACML is widely regarded as the standard for solving complex access-control problems. The demonstration at the RSA conference “shows that XACML can play a key role in healthcare. By successfully enforcing fine-grained, access-control decisions to protected health information, XACML meets HITSP’s requirements for security and privacy.”

John Davis, standards architect with the VHA’s Office of Information and a member of the HITSP technical committee on security, privacy and infrastructure, said in the same release that XACML “helps ensure that patients, physicians, hospitals, public health agencies and other authorized users share critical information appropriately and securely.”

What do you think? Write us with your comments at hitsdaily@crain.com. Please include your name, title and hometown.

Appendix G

From: Michelle Maas Deane [mailto:mmaasdeane@ANSI.ORG]
Sent: Friday, April 11, 2008 3:33 PM
To: HITSP@MAILLIST.ANSI.ORG
Subject: 04/11/08 - HITSP Update from John D. Halamka, MD

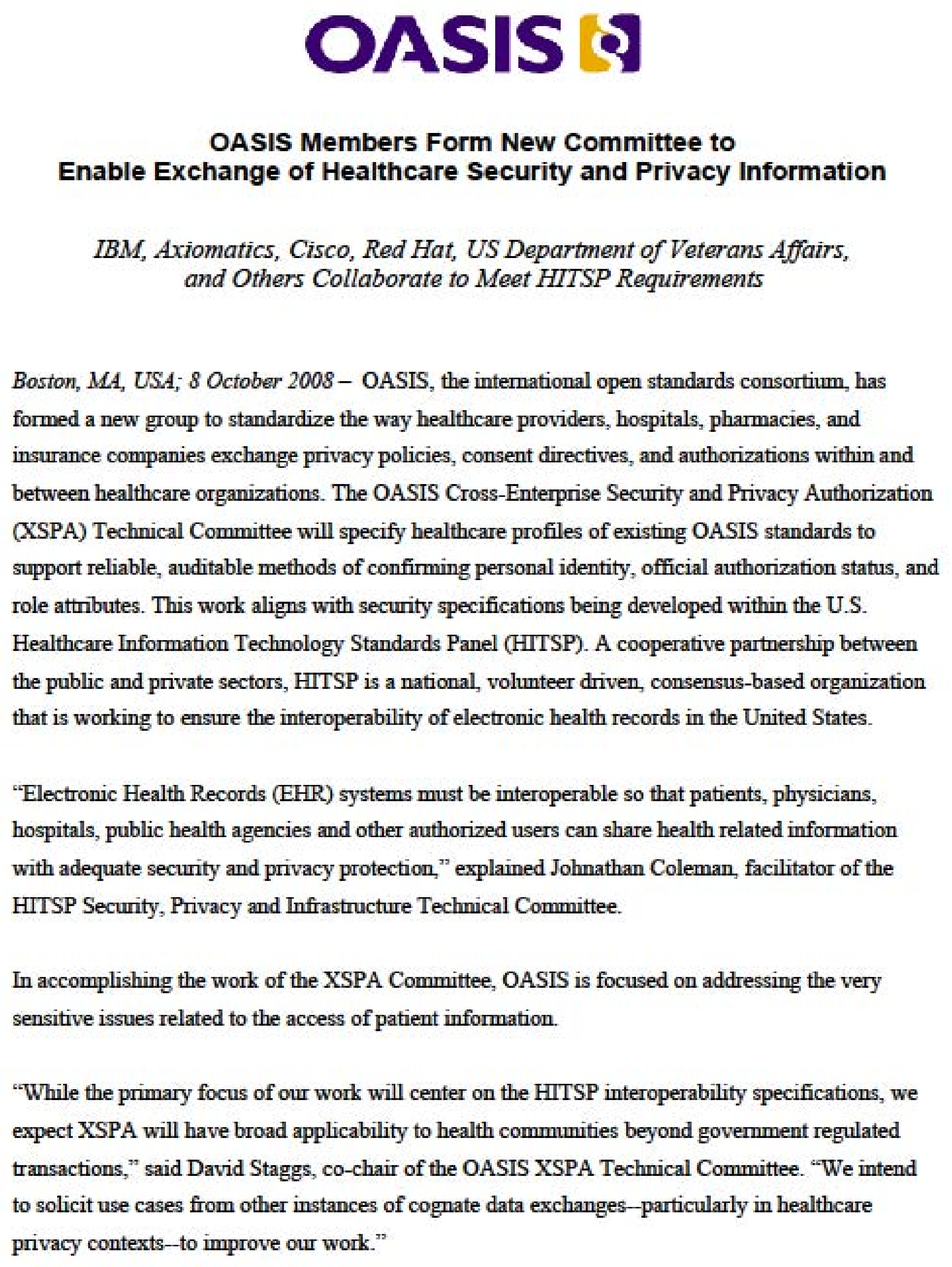
Folks:

1. The following documents that were recently Panel approved have been published and are now available on hitsp.org:
   - HITSP/IS02 - Biosurveillance Interoperability Specification and associated constructs (updated to reference Security and Privacy constructs)
   - HITSP/IS07 - Medication Management Interoperability Specification and associated constructs
   - HITSP/T31 - Document Reliable Interchange

   They will be submitted to AHIC at the June meeting.

2. The OASIS-HITSP Interoperability demonstration took place during the RSA Conference this week. The InterOp demonstrated the use of the OASIS eXtensible Access Control Markup Language (XACML) standard to make and enforce fine-grained access control decisions to protected health information. The RSA Conference attracts around 17000 people and this is the first time it has highlighted in an InterOp demo the healthcare scenario, the Electronic Health Records (EHR) and associated interoperable terminologies of clinical roles, patient consent directives, obligations, and business logic. Congratulations to Mike Davis and the Security, Privacy and Infrastructure TC for a job well done.

Appendix H **(double right click below to view pages 1-3 of PDF)**



OASIS

OASIS Members Form New Committee to Enable Exchange of Healthcare Security and Privacy Information

IBM, Axiomatics, Cisco, Red Hat, US Department of Veterans Affairs, and Others Collaborate to Meet HITSP Requirements

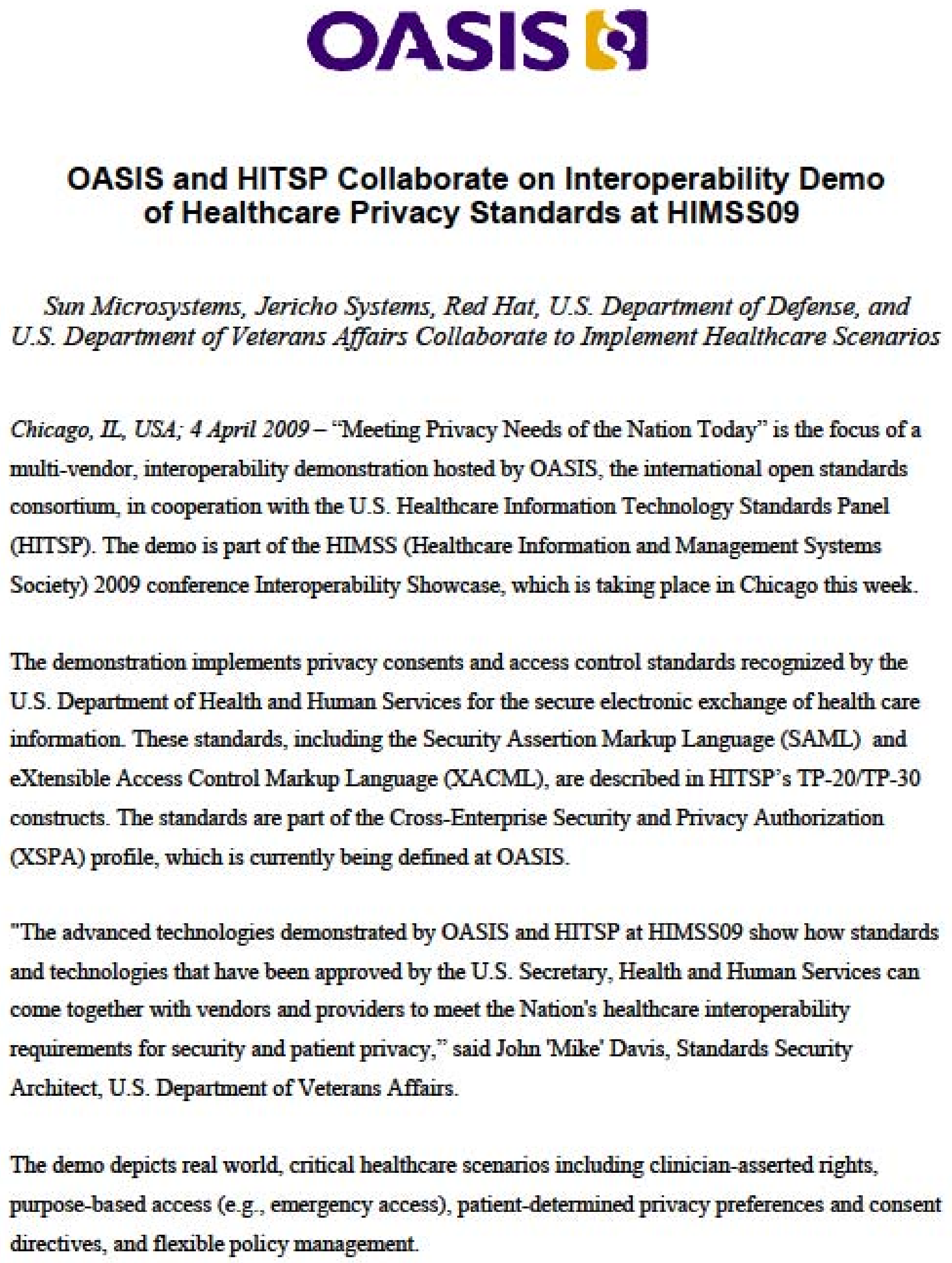
Boston, MA, USA; 8 October 2008 – OASIS, the international open standards consortium, has formed a new group to standardize the way healthcare providers, hospitals, pharmacies, and insurance companies exchange privacy policies, consent directives, and authorizations within and between healthcare organizations. The OASIS Cross-Enterprise Security and Privacy Authorization (XSPA) Technical Committee will specify healthcare profiles of existing OASIS standards to support reliable, auditable methods of confirming personal identity, official authorization status, and role attributes. This work aligns with security specifications being developed within the U.S. Healthcare Information Technology Standards Panel (HITSP). A cooperative partnership between the public and private sectors, HITSP is a national, volunteer driven, consensus-based organization that is working to ensure the interoperability of electronic health records in the United States.

"Electronic Health Records (EHR) systems must be interoperable so that patients, physicians, hospitals, public health agencies and other authorized users can share health related information with adequate security and privacy protection," explained Johnathan Coleman, facilitator of the HITSP Security, Privacy and Infrastructure Technical Committee.

In accomplishing the work of the XSPA Committee, OASIS is focused on addressing the very sensitive issues related to the access of patient information.

"While the primary focus of our work will center on the HITSP interoperability specifications, we expect XSPA will have broad applicability to health communities beyond government regulated transactions," said David Staggs, co-chair of the OASIS XSPA Technical Committee. "We intend to solicit use cases from other instances of cognate data exchanges--particularly in healthcare privacy contexts--to improve our work."

Appendix I **(double right click below to view pages 1 and 2 of PDF)**



OASIS

OASIS and HITSP Collaborate on Interoperability Demo of Healthcare Privacy Standards at HIMSS09

Sun Microsystems, Jericho Systems, Red Hat, U.S. Department of Defense, and U.S. Department of Veterans Affairs Collaborate to Implement Healthcare Scenarios

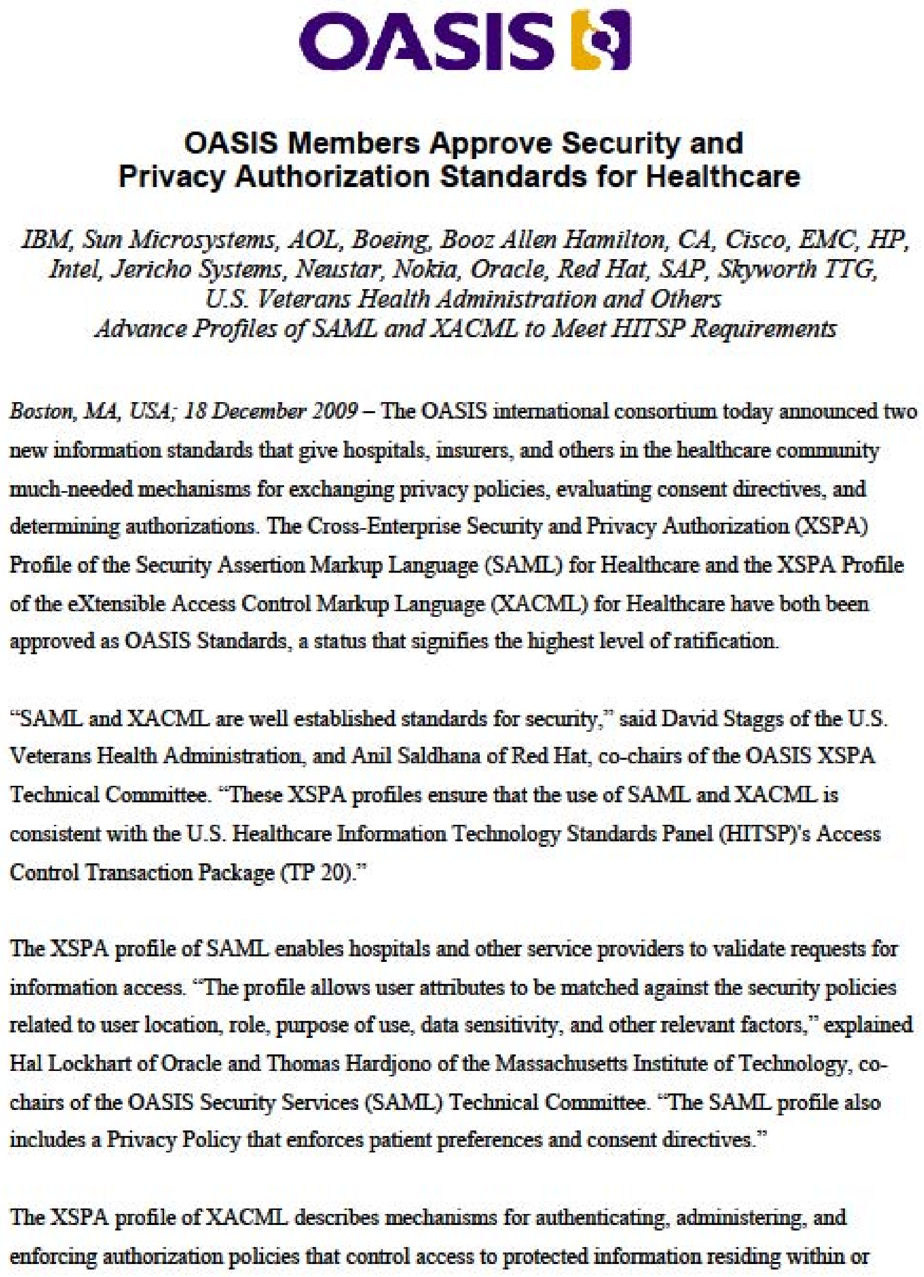
Chicago, IL, USA; 4 April 2009 – "Meeting Privacy Needs of the Nation Today" is the focus of a multi-vendor, interoperability demonstration hosted by OASIS, the international open standards consortium, in cooperation with the U.S. Healthcare Information Technology Standards Panel (HITSP). The demo is part of the HIMSS (Healthcare Information and Management Systems Society) 2009 conference Interoperability Showcase, which is taking place in Chicago this week.

The demonstration implements privacy consents and access control standards recognized by the U.S. Department of Health and Human Services for the secure electronic exchange of health care information. These standards, including the Security Assertion Markup Language (SAML) and eXtensible Access Control Markup Language (XACML), are described in HITSP's TP-20/TP-30 constructs. The standards are part of the Cross-Enterprise Security and Privacy Authorization (XSPA) profile, which is currently being defined at OASIS.

"The advanced technologies demonstrated by OASIS and HITSP at HIMSS09 show how standards and technologies that have been approved by the U.S. Secretary, Health and Human Services can come together with vendors and providers to meet the Nation's healthcare interoperability requirements for security and patient privacy," said John 'Mike' Davis, Standards Security Architect, U.S. Department of Veterans Affairs.

The demo depicts real world, critical healthcare scenarios including clinician-asserted rights, purpose-based access (e.g., emergency access), patient-determined privacy preferences and consent directives, and flexible policy management.

Appendix J **(double right click below to view pages 1-3 of PDF)**



OASIS Members Approve Security and Privacy Authorization Standards for Healthcare

IBM, Sun Microsystems, AOL, Boeing, Booz Allen Hamilton, CA, Cisco, EMC, HP,
Intel, Jericho Systems, Neustar, Nokia, Oracle, Red Hat, SAP, Skyworth TTG,
U.S. Veterans Health Administration and Others
Advance Profiles of SAML and XACML to Meet HITSP Requirements

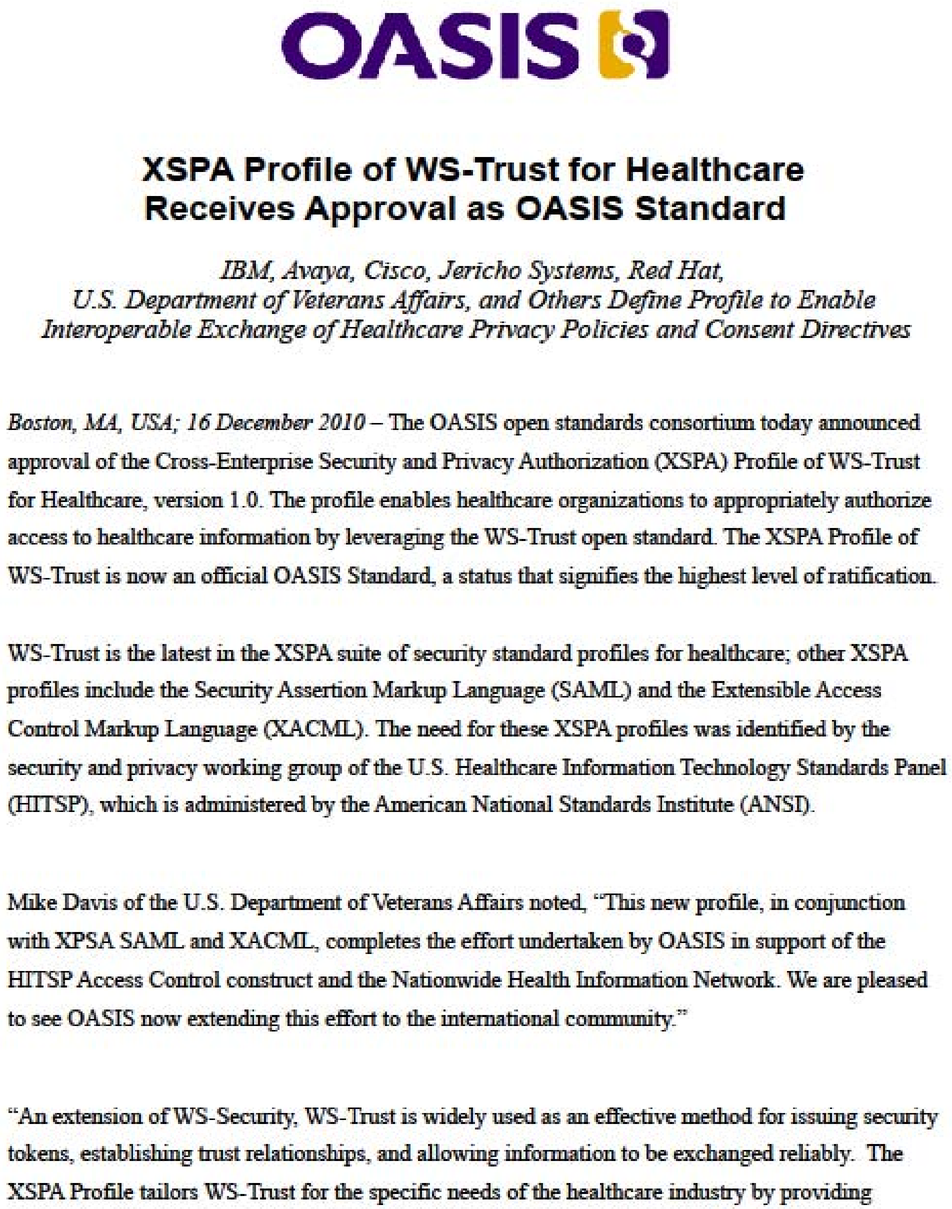
Boston, MA, USA; 18 December 2009 – The OASIS international consortium today announced two new information standards that give hospitals, insurers, and others in the healthcare community much-needed mechanisms for exchanging privacy policies, evaluating consent directives, and determining authorizations. The Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of the Security Assertion Markup Language (SAML) for Healthcare and the XSPA Profile of the eXtensible Access Control Markup Language (XACML) for Healthcare have both been approved as OASIS Standards, a status that signifies the highest level of ratification.

"SAML and XACML are well established standards for security," said David Staggs of the U.S. Veterans Health Administration, and Anil Saldhana of Red Hat, co-chairs of the OASIS XSPA Technical Committee. "These XSPA profiles ensure that the use of SAML and XACML is consistent with the U.S. Healthcare Information Technology Standards Panel (HITSP)'s Access Control Transaction Package (TP 20)."

The XSPA profile of SAML enables hospitals and other service providers to validate requests for information access. "The profile allows user attributes to be matched against the security policies related to user location, role, purpose of use, data sensitivity, and other relevant factors," explained Hal Lockhart of Oracle and Thomas Hardjono of the Massachusetts Institute of Technology, co-chairs of the OASIS Security Services (SAML) Technical Committee. "The SAML profile also includes a Privacy Policy that enforces patient preferences and consent directives."

The XSPA profile of XACML describes mechanisms for authenticating, administering, and enforcing authorization policies that control access to protected information residing within or

Appendix K (double right click below to view pages 1-3 of PDF)



OASIS

XSPA Profile of WS-Trust for Healthcare Receives Approval as OASIS Standard

IBM, Avaya, Cisco, Jericho Systems, Red Hat,
U.S. Department of Veterans Affairs, and Others Define Profile to Enable
Interoperable Exchange of Healthcare Privacy Policies and Consent Directives

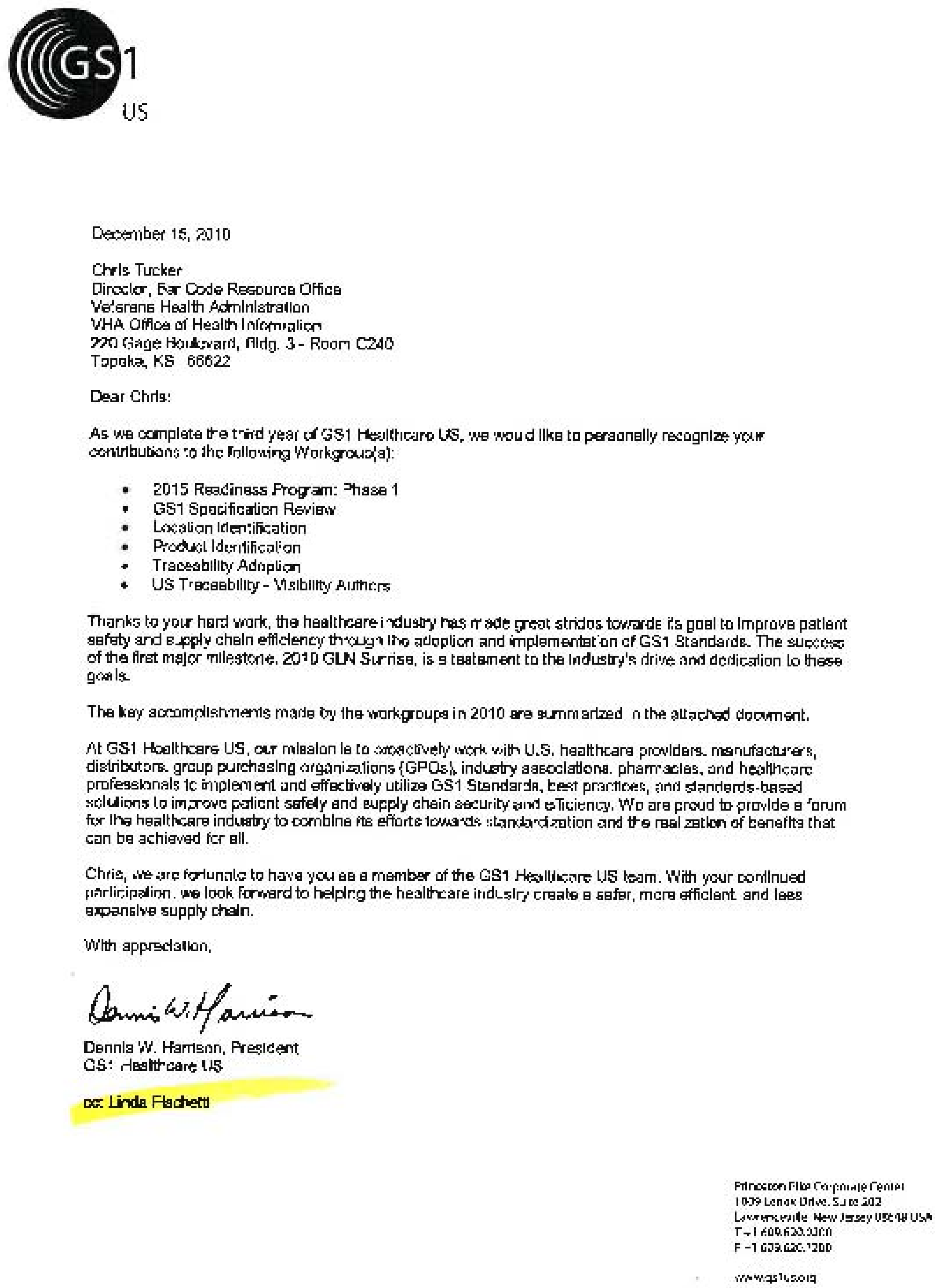
Boston, MA, USA; 16 December 2010 – The OASIS open standards consortium today announced approval of the Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of WS-Trust for Healthcare, version 1.0. The profile enables healthcare organizations to appropriately authorize access to healthcare information by leveraging the WS-Trust open standard. The XSPA Profile of WS-Trust is now an official OASIS Standard, a status that signifies the highest level of ratification.

WS-Trust is the latest in the XSPA suite of security standard profiles for healthcare; other XSPA profiles include the Security Assertion Markup Language (SAML) and the Extensible Access Control Markup Language (XACML). The need for these XSPA profiles was identified by the security and privacy working group of the U.S. Healthcare Information Technology Standards Panel (HITSP), which is administered by the American National Standards Institute (ANSI).

Mike Davis of the U.S. Department of Veterans Affairs noted, “This new profile, in conjunction with XPSA SAML and XACML, completes the effort undertaken by OASIS in support of the HITSP Access Control construct and the Nationwide Health Information Network. We are pleased to see OASIS now extending this effort to the international community.”

“An extension of WS-Security, WS-Trust is widely used as an effective method for issuing security tokens, establishing trust relationships, and allowing information to be exchanged reliably. The XSPA Profile tailors WS-Trust for the specific needs of the healthcare industry by providing

Appendix L (double right click below to view page 1of PDF)



GS1 US

December 15, 2010

Chris Tucker
Director, Bar Code Resource Office
Veterans Health Administration
VHA Office of Health Information
220 Gage Boulevard, Bldg. 3 - Room C240
Topeka, KS 66622

Dear Chris:

As we complete the third year of GS1 Healthcare US, we would like to personally recognize your contributions to the following Workgroup(s):

- 2015 Readiness Program: Phase 1
- GS1 Specification Review
- Location Identification
- Product Identification
- Traceability Adoption
- US Traceability - Visibility Authors

Thanks to your hard work, the healthcare industry has made great strides towards its goal to improve patient safety and supply chain efficiency through the adoption and implementation of GS1 Standards. The success of the first major milestone, 2010 GLN Sunrise, is a testament to the industry's drive and dedication to these goals.

The key accomplishments made by the workgroups in 2010 are summarized in the attached document.

At GS1 Healthcare US, our mission is to proactively work with U.S. healthcare providers, manufacturers, distributors, group purchasing organizations (GPOs), industry associations, pharmacies, and healthcare professionals to implement and effectively utilize GS1 Standards, best practices, and standards-based solutions to improve patient safety and supply chain security and efficiency. We are proud to provide a forum for the healthcare industry to combine its efforts towards standardization and the realization of benefits that can be achieved for all.

Chris, we are fortunate to have you as a member of the GS1 Healthcare US team. With your continued participation, we look forward to helping the healthcare industry create a safer, more efficient and less expensive supply chain.

With appreciation,

Dennis W. Harrison

Dennis W. Harrison, President
GS1 Healthcare US

cc: Linda Fischetti

Princeton Pike Corporate Center
1009 Lenox Drive, Suite 202
Lawrenceville, New Jersey 08648 USA
T +1 609.620.0200
F +1 609.620.1200

www.gs1us.org