SOFTWARECPR®
CRISIS PREVENTION AND RECOVERY, LLC

Standards Navigator

Standards Navigator Monthly Report

25-September-2013

SoftwareCPR Standards Navigator provides information and tools related to standards that play a significant role in health software and software intensive medical devices. In addition to information on existing standards, SoftwareCPR Standards Navigator keeps you up to date on new standards activity and gives you expert insight into future changes to existing standards.

http://www.softwarecpr.com/topicsframepage.htm

August and September 2013 Standards Navigator Overview

Medical device software

- The IEC 62304 FAQ that was developed by EU notified bodies has been translated to Chinese. This is an indication of the continuing effort by industry to get China to utilize current international standards.

Health IT and mobile health regulation

- FDA published the final guidance entitled " Mobile Medical Applications" dated 25-Sep-2013. This guidance explains FDA's current policies regarding regulation of Mobile Medical Applications. It provides criteria and examples of Mobile Medical Apps that are considered Medical Devices; for these it explains which are subject to FDA regulation and which will not require compliance with the medical device regulations. It also explains criteria for which Mobile Applications, platforms, and services (e.g., distribution) are not considered regulated Medical Devices. This guidance is quite specific and definitive in many respects and for certain intended uses (e.g., medicine reminder systems, personal health coaching and others). The guidance can be downloaded at http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf.
- The Australia TGA also published a Q&A to provide guidance on regulation of medical software and mobile medical ‘apps’. The guidance affirms that software that meets the definition of a medical device in section 41BD of the Therapeutic Goods Act 1989 is a medical device. The TGA already regulates medical device software used for therapeutic purposes under the medical devices regulatory framework. The guidance states that the regulations make no distinction between different forms of software. Mobile apps are considered within the medical devices regulatory framework. The guidance states that all medical device software products must meet the Essential Principles for safety and performance. While the guidance provides some general examples of what mobile apps would not come within the definition of a medical device, it is not nearly as specific as the FDA guidance. It also does not exempt any mobile apps that meet the medical device definition from compliance with medical device regulations. The guidance statement can be found at http://www.tga.gov.au/industry/devices-software-mobile-apps.htm.
- The FDA Safety and Innovation Act (FDASIA) workgroup completed its work and made its recommendations in September. The recommendations include: HIT should not be regulated except in cases where there is risk to the patient, a patient-safety risk framework should be used to allow application of regulatory oversight by risk, vendors should be required to list products which represent at least some risk, better post-market surveillance of HIT is needed, steps should be taken to discourage practices that limit the free flow of information. The full draft recommendations report can be found at http://www.healthit.gov/facas/calendar/2013/09/04/hit-policy-committee. In addition, 39 comments were received in response to a request made by the three agencies involved (FDA, ONC and FCC). These comments can be found in Docket HHS-OS-2013-0003 at http://www.regulations.gov/#!docketBrowser;rpp=50;po=0;dct=PS;D=HHS-OS-2013-0003. The agencies have until January to complete the report.
- The IEC 62A Secretariat has recommended that revision of IEC 80001-1 be considered in 2014.

Usability

- The amendments to ISO 62366 and IEC 60601-1-6 were approved unanimously. The amendment to 62366 introduces requirements for legacy products that were created prior to the adoption of ISO 62366 and the amendment to 60601-1-6 clarifies the elements of the usability engineering process that are required for compliance with the IEC 60601 series.

Interoperability

- A new non-profit organization, The Center for Medical Interoperability has been created to improve patient safety and lower costs of health care. Created and with initial funding from the Gary and Mary West Foundation, membership in the new organization will be limited to hospitals and health systems. More information is in the press release at http://www.westhealth.org/news/new-center-for-medical-interoperability.
- No content has been drafted yet for the proposed AAMI/UL 2800 series of standards. The next meeting of the working group will be in December at the AAMI standards week.

Security

- The AAMI medical device security working group has refined the draft of a new work item proposal for a TIR on device security principles and practices, and has begun work on the draft TIR. The draft of the TIR is expected to be available for review at the AAMI standards week in early December.

Medical Devices

- An amendment of IEC 60601-1-10 on Requirements for the development of physiologic closed-loop controllers has been approved. This amendment updates the references to other parts of 60601 and removes the normative reference to IEC 62304 since 60601-1 now has a normative reference to 62304.

Software Engineering

- A minor revision of ISO/IEC TR 90003 Application of ISO 9001 to Software has been initiated. This revision is intended to just make changes necessary to reference the newer versions of ISO 9001 and ISO/IEC 12207. This International Technical Report provides guidance for organizations in the application of ISO 9001:2008 to the acquisition, supply, development, operation and maintenance of computer software.
- A new committee draft of the revision of ISO/IEC 15288 System Engineering Life Cycle Processes has been circulated for comment. The processes in this International Standard form a comprehensive set from which an organization can construct system life cycle models appropriate to its products and services. An organization, depending on its purpose, can select and apply an appropriate subset to fulfill that purpose.
- A committee draft for vote of ISO/IEC 15026-3 Systems and software assurance – Part 3: Systems Integrity Levels has been circulated. This part of ISO/IEC 15026 specifies the concept of integrity levels with corresponding integrity level requirements that are required to be met in order to show the achievement of the integrity level. It places requirements on and recommends methods for defining and using integrity levels and their integrity level requirements. It covers systems, software products, and their elements, as well as relevant external dependences.
- A committee draft for ISO/IEC 42030 Architecture Evaluation has been circulated for comment. This International Standard provides the core ontology for architecture evaluations. The provisions of this International Standard serve to prescribe the structure, properties and products of architecture evaluations. This International Standard also specifies provisions that prescribe desired properties of architecture evaluation methods in order to usefully support architecture evaluations. By providing the ontology for specifying evaluation methods, this International Standard provides the basis on which to compare architecture evaluation methods and select the most suitable methods for use during architecture evaluations.
- A new work item draft for ISO/IEC TR 20000-7 Service Management – Part 7: Guidance on the application of ISO/IEC 20000-1 to the cloud has been circulated. ISO/IEC 20000-1 specifies a service management system (SMS) as the means to achieve the integrated management of the service management policies, objectives, plans, processes, process interfaces, documentation and resources. The guidance in this part of ISO/IEC 20000 can be of interest to organizations that are involved in the provision or management of customer and supporting services that include cloud services. It can also be of interest to organizations that are faced with major changes to their existing services and support arrangements as part of a move to cloud services.

Activity – July 2013

NEW STANDARDS, REPORTS & REGULATIONS

	Topic	Use / Users	Description
ISO/IEC TR 90003 CD	Software	Manufacturers	Committee draft for comment on revision of guidance for application of ISO 9001 for software. ***The draft technical report can be found on the SoftwareCPR Standards Navigator web page.***
ISO/IEC 15288 CD	Systems engineering	Manufacturers	ISO/IEC 15288 System Engineering Life Cycle Processes committee draft for comment. This is a draft of a new edition. ***The draft standard can be found on the SoftwareCPR Standards Navigator web page.***
ISO/IEC 15026-3 CDV	Software	Manufacturers	ISO/IEC 15026-3 Systems and software assurance – Part 3: Systems Integrity Levels committee draft for vote. ***The draft standard can be found on the SoftwareCPR Standards Navigator web page.***
ISO/IEC 42030 CD	Systems	Manufacturers	ISO/IEC 42030 Architecture Evaluation has been circulated for comment. This International Standard provides the core ontology for architecture evaluations. ***The draft standard can be found on the SoftwareCPR Standards Navigator web page.***
ISO/IEC TR 20000-7 NP	Networks	Hospitals	ISO/IEC TR 20000-7 Service Management – Part 7: Guidance on the application of ISO/IEC 20000-1 to the cloud. A new work item draft has been circulated in support of the NP ballot and for comment. ***The draft standard can be found on the SoftwareCPR Standards Navigator web page.***

STANDARDS & GUIDANCE DRAFTS STILL IN REVIEW

IEC 62304 Amendment 1 CD	Medical device software	Manufacturers	Revision of IEC 62304 has been divided into two parts, an amendment and a second edition. The amendment includes a revision to how software safety classification is determined and new requirements for legacy software that was developed prior to 62304, as well as a few other new requirements and clarification of existing requirements. A committee draft of the amendment has been circulated for comment. The second edition of 62304 will extend the scope to health software. Work on the second edition will begin later this year. ***The draft amendment can be found on the SoftwareCPR Standards Navigator web page.***
ISO 80001-2-6 DTR	Medical devices on networks	Hospitals and manufacturers	Draft for vote on guidance for responsibility agreements between hospitals and manufacturers. ***The draft technical report can be found on the SoftwareCPR Standards Navigator web page.***
ISO 17522 DTR	Mobile Devices	Manufacturers	This technical report describes the status and requirements of health applications and services on smart devices platforms and suggests the reference architecture for these. ***The draft technical report can be found on the SoftwareCPR Standards Navigator web page.***
ISO 33001 DIS	Process assessment	Manufacturers	ISO IEC 33001 DIS Information technology — Process assessment — Concepts and terminology This International Standard provides a glossary of terms related to the performance of process assessment, together with an overall introduction to the concepts and standards framework for process assessment. The Standard identifies the principal components supporting the performance of process assessment, describes the results of process assessment, and gives an overview of the ways in which the results of assessment can be applied. ***The draft standard can be found on the SoftwareCPR Standards Navigator web page.***
ISO 33002 DIS	Process assessment	Manufacturers	ISO IEC 33002 DIS Information Technology — Process Assessment — Requirements for performing process assessment

			This International Standard defines the minimum set of requirements for performing an assessment that will ensure assessment results are objective, consistent, repeatable and representative of the assessed processes. The requirements help to ensure that the assessment output is self-consistent and to provide evidence to substantiate the ratings and to verify compliance with the requirements. ***The draft standard can be found on the SoftwareCPR Standards Navigator web page.***
ISO 33003 DIS	Process assessment	Manufacturers	ISO IEC 33003 DIS Information technology — Process assessment — Requirements for process measurement frameworks This International Standard provides requirements for process measurement frameworks that support and enable the assessment of process quality characteristics, from conceptualization to empirical validation. ***The draft standard can be found on the SoftwareCPR Standards Navigator web page.***
ISO 33004 DIS	Process assessment	Manufacturers	ISO IEC 33004 DIS Information technology — Process assessment — Requirements for process reference, process assessment and maturity models This International Standard provides requirements for the construction and verification of process reference models, process assessment models and maturity models. ***The draft standard can be found on the SoftwareCPR Standards Navigator web page.***
ISO 33020 DIS	Process assessment	Manufacturers	ISO IEC 33020 DIS Information technology — Process assessment — Process measurement framework for assessment of process capability This International Standard defines a process measurement framework conformant to the requirements defined in ISO/IEC 33003 for the process quality characteristic of process capability. The process measurement framework in this international standard conforms to the requirements of ISO 33003 and is applicable to any domain. ***The draft standard can be found on the SoftwareCPR Standards Navigator web page.***

REFERENCES

	Topic	Use / Users	Description
IMDRF draft document on Standalone Medical Device Software: Key Definitions	Medical device software	Manufacturers	The International Medical Device Regulators Forum believes that existing regulations do not readily address the unique public health risks posed by standalone software nor assure an appropriate balance between patient/consumer protection and promoting public health by facilitating innovation. The IMDRF has undertaken an effort to facilitate international regulatory convergence towards a smart, balanced regulatory approach that provides an optimal level of patient safety while fostering innovation and provides patient and providers with continued access to advanced health care technology that is safe. This draft document is the first of several documents intended to achieve these objectives. It identifies and defines key terms needed for regulation of standalone medical device software.
FDA draft premarket cybersecurity guidance	Security	Manufacturers	Recommendations for security controls to assure medical device cybersecurity and documentation to submit in a premarket review to demonstrate effective cybersecurity management. Recommends identifying cybersecurity risks and providing a traceability matrix that links cybersecurity controls to cybersecurity risks that were identified. Also recommends documentation to demonstrate that the device will be provided to purchasers free of malware and a plan for providing updates and patches to provide up-to-date protection. This is a draft for comment. Comments should be submitted before September 13.
FDA Safety communication on cybersecurity	Security	Manufacturers and hospitals	FDA has become aware of cybersecurity vulnerabilities and incidents that could directly impact medical devices or hospital network operations. This safety communication recommends that medical device manufacturers take steps to limit opportunities for unauthorized access to medical devices and hospitals take steps to evaluate network security and protect the hospital systems. The FDA also recommends prompt reporting of events that have impacted the performance of a medical device or hospital network.
ICS-CERT Alert	Security	Manufacturers, hospitals	ICS-CERT is issuing this alert to provide early notice of a report of a hard-coded password vulnerability affecting roughly 300 medical devices across approximately 40 vendors. According to their report, the

regarding medical devices with hard-coded passwords			vulnerability could be exploited to potentially change critical settings and/or modify device firmware. The alert also identifies baseline mitigations for reducing risks to these and other cybersecurity attacks.
ONC Patient Safety Action & Surveillance Plan	Health IT safety	Health IT manufacturers, hospitals	The final version of the ONC plan that has the objectives to use health IT to make care safer and to continuously improve the safety of health IT.
ONC contract with the Joint Commission to investigate health IT-related safety events	Health IT safety	Hospitals, health IT manufacturers	The purpose of this contract is to ensure that there is an early detection system on health IT-related safety issues, including those associated with EHRs.
ONC guidance on annual surveillance plans by authorized certification bodies	Surveillance of certified EHRs	Authorized EHR certification bodies	Authorized Certification Bodies are expected to conduct surveillance on EHRs that they have certified. This guidance provides the priorities for topics to assess in the surveillance plan. Safety-related capabilities and security capabilities are two of the four areas for priority identified in this guidance.
NIST draft outline of a cybersecurity framework	Security	Hospitals, manufacturers	NIST was directed to prepare a cybersecurity framework for critical infrastructure in Presidential Executive Order 13636. Healthcare was identified as one of the areas with critical infrastructure. This draft for comment is only an outline of the framework. NIST intends the framework to take a risk management approach at a high level, focusing on key functions of cybersecurity management which are broken down into categories

for critical infrastructure			and subcategories. References such as existing standards, guidelines and practices will be provided for each subcategory. A draft of the framework will be released in October.
TEAM-NB position paper on use of ISO 14971:2012	Risk management	Manufacturers	Describes the steps TEAM-NB members plan to verify where relevant if requirements of EN ISO 14971:2012 have been met. This should help manufacturers update their risk management procedures and files to maintain compliance with the Essential Requirements of the directives, when building on the presumption of conformity. ***The position paper can be found on the SoftwareCPR Standards Navigator web page.***
TEAM-NB "Vision on Revision"	Regulation	Regulators, Manufacturers, Notified bodies	This document forms the input of TEAM-NB into the debate on The Revision of European Legislation on Medical Devices. Contributions came from BSI Germany, BSI UK, DEKRA Netherlands, TUV Austria, and TUV Sud. ***The report can be found on the SoftwareCPR Standards Navigator web page.***
Report	Interoperability	Medical device manufacturers, Hospitals, Regulators	AAMI/FDA Interoperability Summit report An AAMI/FDA sponsored summit meeting on medical device interoperability was held in late 2012. This report documents the discussion and identifies themes from the summit. This report can be found at http://www.aami.org/interoperability/Interoperability_Summit_publication.pdf
Report	Wireless	Hospitals, Medical device manufacturers	AAMI Wireless Workshop report A workshop with approximately 80 invited medical wireless experts was held in late 2012. This report documents the discussion and outcomes of this workshop. A follow-up meeting is planned for March 2013. This report can be found at http://www.aami.org/wireless/2012_Wireless_Workshop_publication.pdf

Presentation	Research	Medical device manufacturers	Medical Device Innovation Consortium (MDIC) Presentation from FDA and MDIC FDA and Life Science Alley have been collaborating on establishing a public-private partnership for research into regulatory science. A non-profit organization called the Medical Device Innovation Consortium has been created. This presentation by the FDA and the temporary director of the non-profit describes the need and the plans for this organization. ***This presentation can be found on the Standards Navigator web page.***
Announcement	Interoperability	Medical device manufacturers, Hospitals, Regulators	AAMI/UL collaboration on interoperability standards AAMI and UL have announced that they will collaborate on a series of standards for medical device interoperability. The press release announces the collaboration and its benefits. This announcement can be found at http://www.aami.org/news/2012/091712_press_AAMI_UL_Interoperability.pdf
Report	Security	Medical device manufacturers, Regulators	GAO report on FDA review of certain medical devices The General Accounting Office does investigations for the US Congress. In this report they reviewed how FDA reviewed implanted medical devices that used wireless communications for security vulnerabilities that could cause safety concerns. They looked at two devices that researchers had shown could be controlled by use of off-the-shelf radio devices. In their findings, they criticized FDA for not reviewing security capabilities in these devices, even though they determined that FDA had the authority to do so. This will certainly result in FDA increasing their scrutiny of security for these type of devices. Since a security vulnerability in a device that is wirelessly communicating over a network seems to surely pose a risk as well, it is likely that FDA will also increase security scrutiny of all devices that use wireless communications. Dr. Kevin Fu testified to the National Institute of Standards and Technology Information Security & Privacy Advisory Board that "Conventional malware is rampant in hospitals because of medical devices using unpatched operating systems. There's little recourse for hospitals when a manufacturer refuses to allow OS updates or security patches." A report of the meeting can be found in the MIT Technology Review http://www.technologyreview.com/news/429616/computer-viruses-are-rampant-on-medical-devices-in-hospitals/

			The article states that “In September, the Government Accountability Office issued a report warning that computerized medical devices could be vulnerable to hacking, posing a safety threat, and asked the FDA to address the issue. The GAO report focused mostly on the threat to two kinds of wireless implanted devices: implanted defibrillators and insulin pumps. The vulnerability of these devices has received widespread press attention (see "Personal Security" and "Keeping Pacemakers Safe from Hackers"), but no actual attacks on them have been reported. Fu, who is a leader in researching the risks described in the GAO report, said those two classes of device are "a drop in the bucket": thousands of other network-connected devices used for patient care are also vulnerable to infection. "These are life-saving devices. Patients are overwhelmingly safer with them than without them. But cracks are showing," he said. (Fu was *Technology Review's* Innovator of the Year in 2009.)” One of Dr. Fu’s collaborators in research that showed an implanted defibrillator could be hacked was Dr. William Maisel who is now the Deputy Director for Science at CDRH. FDA staff has indicated that they are in the process of revising the FDA Cybersecurity Guidance. This guidance will likely include recommendations for manufacturer’s security programs for devices and additional recommendations for security information to be provided during pre-market review of devices that are intended for use on a network. In addition, the guidance is now expected to provide information on when a security issue is reportable to the FDA and when a security event will result in a recall. Another interesting bit of information in this report was the FDA response that they had hired a consultant (later determined to be McKinsey) to assess how they review software and make suggestions for improvements. This assessment is supposed to be completed by the end of 2012. This report can be found at http://www.gao.gov/products/GAO-12-816

Report	Mobile medical devices	Medical devices manufacturers, Hospitals, Regulators	FCC report on Mobile Medical Devices The FCC created an independent mHealth Task Force, to research the barriers to rapid deployment of mHealth technology and develop recommendations to government and industry to address those barriers. This report documents the task force recommendations for achieving 5 goals: Goal 1: FCC should continue to play a leadership role in advancing mobile health adoption. Goal 2: Federal agencies should increase collaboration to promote innovation, protect patient safety, and avoid regulatory duplication. Goal 3: The FCC should build on existing programs and link programs where possible in order to expand broadband access for healthcare. Goal 4: The FCC should continue efforts to increase capacity, reliability, interoperability and RF safety of mHealth technologies. Goal 5: Industry should support continued investment, innovation, and job creation in the growing mobile health sector. Recommendations include: • greater collaboration with other US Federal agencies • promoting the availability of broadband for healthcare • harmonizing spectrum allocations for healthcare internationally • industry use of standards based technologies for transmitting authenticated messages and encrypted health information ***This report can be found on the Standards Navigator web page***
Report	Health IT	Hospitals, EHR vendors, MD manufacturers	Institute of Medicine report – Health IT and patient safety The Institute of Medicine produced a report on the impact of Health IT on patient safety. The report had a number of recommendations for the Secretary of HHS. ***A presentation on the recommendations and the entire report are available at the SoftwareCPR Standards Navigator web page.***

Regulation	Regulation	Medical device manufacturers, IVD manufacturers	EU draft proposed new Medical Device Regulation and In-Vitro Device Regulation These draft regulations can be found at http://ec.europa.eu/health/medical-devices/files/revision_docs/proposal_2012_542_en.pdf - medical devices http://ec.europa.eu/health/medical-devices/files/revision_docs/proposal_2012_541_en.pdf - In-vitro devices

STANDARDS CURRENTLY UNDER DEVELOPMENT OR REVISION

	Topic	Use / Users	Description
IEC 62304 Amendment 1	Software Life Cycle	Medical Device manufacturers, Regulators	Amendment to the Medical Device Software Life Cycle standard. This standard is harmonized in the EU. The amendment addresses software safety classification and how to be compliant with legacy software. Current status: Comments received on the first CD are being resolved. Next step: Second CD or CDV will be circulated. Expected completion: January 2014
IEC 82304-1	Health Software	Medical device manufacturers, Regulators	New standard on Health Software: General Requirements. This standard is intended to be for standalone software products and to cover the product level requirements such as product validation, labeling, documents to be provided to the user, etc. Current status: Comments received on the first CD are being resolved. Major issues are scope and terminology. Next step: Second CD will be circulated. Expected completion: 2015

IEC 62366-1	Medical devices	Medical device manufacturers, Regulators	The standard on human factors engineering is being revised and divided into two documents. The first is a standard that includes requirements for the process. The second will be a technical report providing information about good practices for implementing the human factors process. This document is the first part. Current status: Comments have been resolved on the first CD and a second CD circulated. Next step: Comments received on the second CD. Expected completion: 2015