SOFTWARECPR®
CRISIS PREVENTION AND RECOVERY, LLC

Standards Navigator

Standards Navigator Monthly Report

11-November-2016

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

Standards and regulatory activity overview

A lot of standards and regulatory activity is expected in 2016. Here are some of the areas to watch. Changes to status since the last report are in red text.

- IEC 82304-1 *Health Software: General requirements for safety* will be completed during the first half of 2016. It is intended that this standard be harmonized in the EU, but it is not clear when this may happen.

  Status: The FDIS was approved. The standard will be published after final editing. This is expected around the end of the year.

- A first committee draft of the second edition of IEC 62304 will be circulated for review in the first half of 2016. The second edition will expand the scope of the standard to health software.

  Status: Comments have been received on the first CD. The project team met and has resolved about 80% of the comments. A second committee draft is planned for March 2017 after resolution of the remaining comments.

- New standards for health software covering all parts of the life cycle will be proposed in 2016.

  Status: The proposal for a new standard, *ISO 81001-1 Health software and health IT systems safety, effectiveness and security – Part 1: Foundational principles, concepts, and terms,* has been approved by ISO and IEC. Work on the standard began in early October. The standard is planned to be published in 2020.

- AAMI will move its work on HIT quality management systems and HIT risk management forward. The goal is to complete these by the end of 2016.

  Status: A decision was made to have this work be a 4-part standard. Part one will be on fundamentals, part two on risk management, part three on quality management and part four on usability. Working drafts of the four parts have been created. The next meeting of the AAMI HIT committee to review a draft of the standards will be in January. The current plan calls for publishing to begin in 2017.

- A revision of IEC 80001-1 will begin in 2016.

  Status: The proposal for extending the scope of the 80001 series and for revising 80001-1 has been approved by ISO and IEC. Work began in October on the second edition of IEC 80001-1 with a revised title and scope, *IEC 80001-1 Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software – Part 1: Application of risk management*. The expected date of publication is January, 2020.

- The revision to ISO 13485 will be published in the first half of 2016.

  Status: The 2016 edition of ISO 13485 has been published by ISO.

- CEN has circulated a final draft of an European Standard for application of ISO 9001 by Healthcare Delivery Organizations.

- ISO 14971 is currently under review. It is likely that a revision (amendment or new edition) will be started in 2016.

  Status: The review of 14971 has been completed with mixed results. A meeting of the working group was held in June to discuss whether a revision is necessary. The working group did not come to consensus on revising 14971. A meeting of the working group during the first week of October recommended that a revision be done with a limited scope. The final decision on whether to revise will be made at the ISO TC 210 meeting in November.

  The recommendation of the Joint Working Group was approved at the ISO TC 210 meeting in early November. ISO 14971 and ISO/TR 24971 will be revised. ISO 14971 will be revised with the following plan:

with the following plan:

1) maintain the concepts of and the approach to risk management,

2) clarify the normative requirements, particularly concerning the following topics:

- production and post-production information,
- clinical benefits and risk-benefit analysis,

3) move guidance in the informative annexes to ISO/TR 24971, *Medical devices -- Guidance on the application of ISO 14971*,

4) keep the annex with the rationale in ISO 14971, *Medical devices -- Application of risk management to medical devices,*

5) with no change in scope

6) with a 36 month track (expected publication would be in 2019),

In addition, the JWG was instructed to consider the following items in the revision of ISO 14971:

to consider the following items regarding the

revision of 14971:

1) include references to ISO/TR 24971 and IEC/TR 80002-1, *Medical device software -- Part 1: Guidance on the application of ISO 14971 to medical device software*;

2) Clarify the relationship with 62366-1, *Medical devices -- Part 1: Application of usability engineering to medical devices,*

3) Consider to harmonize the vocabulary with ISO 31000, *Risk management -- Principles and guidelines ,* where appropriate,

4) Address data privacy and security.

ISO/TR 24971 will be revised with the following plan:

1) update the guidance ISO/TR 24971,

2) merge and update guidance from informative annexes of ISO 14971,

3) with no change in scope

4) with a 36 month track (expected publication would be in 2019)

- A second amendment to IEC 60601-1 will be started in the second half of 2016. This amendment is scheduled to be completed in 2019. A fourth edition of 60601-1 will be started following the completion of the amendment and will be scheduled for completion in 2024. Discussions about the structure of the fourth edition will likely begin in 2017 and decisions made before work is started on the fourth edition.

  Status: An approved list of issues to be addressed in the second amendment was finalized at a meeting of SC 62A in October. No changes to the Programmable Electronical Medical Subsystem (PEMS) were included in the approved list of issues.

- Draft texts of the EU Medical Device Regulation and the IVD regulation have been released. These still need legal editing and translation before being published in the Official Journal. Publication is expected around the end of the year.

- The first deliverables from UL/AAMI 2800 on medical device interoperability should be completed in 2016.

  Status: The committee met in June and hopes to have a draft of the first parts available for review soon.

- AAMI TIR 57 on medical device cybersecurity risk management will be published in 2016.

  Status: The TIR has been recognized by the FDA before it was even been made available for purchase by AAMI. The TIR is now available for purchase from AAMI.

- The AAMI Device Security working group intends to begin work on guidance for postmarket cybersecurity activities and plans at its next meeting in December.

- Many documents, both standards and regulations, on security and privacy will be in process during 2016.

  NIST has announced that it will be revising SP 800-53, the most complete compilation of security controls.

  UL has begun publishing a series of standards on security, UL 2900.

  A group in Germany active in medical device standards has expressed an intention to propose an international standard for medical device security risk management.

  The new General Data Privacy Regulation has been approved in the EU.

  The second edition of *ISO 27799 Health informatics -- Information security management in health using ISO/IEC 27002* has been submitted for publication. The published standard should be available before the end of 2016.

  A new standard has been released by the Diabetes Technology Society - Standard for Wireless Diabetes Device Security (DTSec).

  A new directive on network and information security has been published by the EU.

  Discussions at recent international standards meetings make it clear that medical device cybersecurity standards will be started next year. The exact form of these standards is not yet determined, but will probably be decided in the first half of 2017. Standards addressed to manufacturers may include development process, development risk management and post-market process.

  Japan will issue a guidance document on cybersecurity for medical devices.

  NIST has released a new security guidance document, NIST SP 800-160 Systems Security Engineering.

October 2016 Standards Navigator New Documents

Most standards committees have meetings during the late September – mid November timeframe. During this period few new drafts are released as groups prepare for the meetings. During October only a few new draft documents were released for the topics included in this report.

Medical device software

- No new documents this month

Medical Devices

- No new documents this month

Health IT and mobile health applications

- No new documents this month.

Medical device and Health Security

- NIST has released a new security guidance, SP 800-160 Systems Security Engineering. This is a general security guidance, not specific for healthcare. This publication defines *systems security engineering* as a specialty discipline of systems engineering. It provides considerations for the security-oriented activities and tasks that produce security-oriented outcomes as part of every systems engineering process *activity* with focus given to the appropriate level of fidelity and rigor in analyses to achieve assurance and trustworthiness objectives.

  The NIST guidance is available at https://doi.org/10.6028/NIST.SP.800-160.

- Japan is developing a guidance document on cybersecurity for medical devices.

  A presentation on the Japan effort is available on the SoftwareCPR Standards Navigator web page.

Software Engineering and Information Technology

- A final draft for approval (FDIS) of *ISO/IEC/IEEE 24765: Systems and software engineering — Vocabulary, 2nd edition* has been circulated. This International Standard was prepared to collect and standardize terminology. Its purpose is to identify terms currently in use in the field and standard definitions for these terms. It is intended to serve as a useful reference for those in the Information Technology field. It provides definitions that are rigorous, uncomplicated, and understandable.

  The draft standard is available on the SoftwareCPR Standards Navigator web page.

- A final draft for approval (FDIS) of *ISO/IEC/IEEE FDIS 24748-5 Systems and software engineering — Life cycle management — Part 5: Software development planning* has been circulated. Part 5 of ISO/IEC/IEEE 24748 focuses on the processes required for successful planning and management of the project's software development effort and for development of the software development plan (SDP) as a vehicle for representing a project's application of software life cycle processes. This International Standard provides a common framework for planning and controlling the technical processes and activities to produce and sustain software products. The complete life cycle is covered by this International Standard, from idea conception to the retirement of a software product.

  The draft standard is available on the SoftwareCPR Standards Navigator web page.

STANDARDS & GUIDANCE DRAFTS STILL IN REVIEW

These draft documents were issued in a previous month and are still being reviewed. They can be found on the SoftwareCPR Standards Navigator until their review period completes.

	Topic	Use / Users	Description
ISO/IEC 12207 DIS	Software Engineering	Manufacturers	ISO/IEC 12207 establishes a common framework for software life cycle processes, with well-defined terminology, that can be referenced by the software industry. It contains processes, activities, and tasks that are to be applied during the acquisition, supply, development, operation, maintenance or disposal of software systems, products, and services.
ISO 33053 NP	Quality management	Manufacturers	This technical specification defines a process reference model (PRM) for the domain of quality management. The scope of the quality management domain is determined by the requirements in ISO 9001:2015. The model specifies a process architecture for this domain, and comprises a set of processes, with each described in terms of process purpose and outcomes. This is a new proposal for vote.
ISO_26513_	Software Engineering	Manufacturers	This International Standard provides the minimum requirements for testing and reviewing user documentation, including both printed and online documents used in work and other environments by the users of software which includes application software, systems software, and software that controls machinery or hardware devices. It applies to printed user manuals, online help, user assistance for mobile devices, tutorials, websites, and user reference documentation. This is a draft for vote.
ISO_19770-1 DIS	Information Technology	Manufacturers	This international standard specifies the requirements for the establishment, implementation, maintenance and improvement of a management system for IT asset management, referred to as an “IT asset management system”. This is a draft for vote.

STANDARDS & GUIDANCE DRAFTS STILL IN REVIEW

These draft documents were issued in a previous month and are still being reviewed. They can be found on the SoftwareCPR Standards Navigator until their review period completes.

	Topic	Use / Users	Description
ISO_19770-4 DIS	Information Technology	Manufacturers	This part of ISO/IEC 19770 provides an International Standard for resource utilization measurement (RUM). A RUM is a standardized structure containing usage information about the resources that are related to the use of an IT asset. This is a draft for vote.