DICOM℠ be
Digital Imaging and Communications in Medicine

DICOM Secretariat/MITA

1300 North 17th Street, Suite 900

Arlington, VA 22209, USA

http://www.dicomstandard.org/

dicom@dicomstandard.org

Minutes

MEETING NAME WG-14

MEETING PLACE/DIAL IN GoToMeeting

DATE & TIME Tuesday, February 23, 2021, 9:00 AM - 10:00 AM EDT

PRESIDING OFFICERS Lawrence Tarbox, CHAIR, AAPM/Univ. of Arkansas for Medical Sciences

Rob Horn, CHAIR, Fairhaven Technologies

VOTING MEMBERS PRESENT	AAPM/Univ. of Arkansas for Medical Sciences	Lawrence Tarbox
	Agfa HealthCare Inc.	Bill Jacqmein
	Fairhaven Technologies	Robert Horn
	GE Healthcare	Matthew Hillyer
	JIRA	Akihiro Yomoda
	Medical Image Standards Association of Taiwan	Chung-Yueh Lien

VOTING MEMBERS ABSENT	American College of Radiology	Matt Jordan
	Canon Medical Systems USA, Inc.	Scott Nitsche
	Center for Medical Device Standardization Administration,CFDA	Jia Zheng
	Hologic Inc.	Jeff Garrett
	Konica Minolta Healthcare Americas, Inc.	Michael Laconti
	Laitek Inc.	Douglas Sluis
	OFFIS - Institute for Information Technology	Marco Eichelberg
	PHC co.,Ltd	Katsuya Watanabe
	Philips	Ben Kokx
	PixelMed Publishing	David Clunie
	Siemens Healthcare GmbH	Hans-Martin von Stockhausen
	Stryker Communications	Corey Cochran

OTHERS PRESENT	GE Healthcare	Steven Nichols, Observer
	National Taipei University of Nursing and Health Sciences	Tuz-Yun Ting, Observer
	Philips	Nikhilesh Sonar, Observer
	Philips India	Arul Patchi Prasath S, Observer

DICOM SECRETARIAT Carolyn Hull, MITA

1 CALL TO ORDER AND REVIEW OF ANTI-TRUST RULES AND DICOM PATENT POLICY

The meeting was called to order. Staff reviewed the Guidelines for Conducting DICOM/NEMA Meetings and recorded attendance.

2 WELCOME/ATTENDANCE/INTRODUCTION

The attendance was taken.

3 REVIEW AND APPROVE AGENDA

The agenda was reviewed and approved.

4 REVIEW MINUTES

The minutes of the previous meeting-1/26/21 were approved.

5 Hot issues that have come up since the last WG-14 tcon (all)

Cyber surveillance-healthcare #1 target for 2020 for public attackers. Most breaches are exposing VPNs and did not make updates.

6. **ISO FYI-** ISO group is making updates to these Standards:
   - IEC TR 80001-2-2:2012 ED1 Application of risk management for IT-networks incorporating medical devices - Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls
   - IEC TR 80001-2-8:2016 ED1 Application of risk management for IT-networks incorporating medical devices - Part 2-8: Application guidance - Guidance on standards for establishing the security capabilities identified in IEC TR 80001-2-2

   The project lead is ben.kokx@philips.com. Please contact him directly if interested.

   Their stated target is a formal draft by 2022-10-28 and publish final text by 2023-12-29

7. **SIIM FYI-** It was suggested for members of WG-14 to join a SIIM Security Taskforce meeting to discuss sharing the documents WG-14 is drafting. They do not have a meeting set up yet, but we will coordinate once they do. Lawrence Tarbox and Rob Horn indicated interest.

8. **Short paper (add)-conveying 1 time passwords over DICOM DIMSE- (Rob Horn)-** The group reviewed this. What to do with it? In addition to meeting with the Security Taskforce, Lawrence Tarbox will email Cheryl Carey and see what she thinks about DICOM education via SIIM. One other idea is for new feature, e.g. to go through SIIM.

Action: Rob Horn to polish for user story.

9. **NIST paper on PACS Security-**Review for this month

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-24.pdf

If using Windows and Linux, both have a good IP and applications filtering capability. If think of network as functional blocks, rather than a system.

usenix.org/system/files/login/articles/1156-singer.pdf

https://canary.tools/

Action: Rob to write complementary/companion paper to NIST and using IT people as examples, companion to NIST paper. NIST showed how to do this using x software, here is how to do this on Windows 10.

10. **Certified time stamp CP2098-** (Rob)- came from Michael (?) updated definition of "certified timestamp."

Comment that we do not say what to do when a signature is an odd length. Working Group 6 will likely run with this. Will go through Working Group 6, no additional action from WG-14. FYI-update in DCMTK will include certified timestamps report.

    a. **Digital signatures profile to incorporate SHA-2**-Discuss and vote whether to add more profiles. Discuss during next meeting, add to next meeting agenda. (goes under item above). What do we want to add about SHA-2 and SHA-3? Begin here. Start with this topic and others forward next meeting.

11. **CP-2092_update_MAC_algorithms was approved for Voting Packet (i.e. public comment). –** In the working group 6 process, will not modify and will put together a separate work item proposal. Add to next meeting.

12. **Consulting companies pushing DICOM security issues-** Did not discuss.

13. **Follow up from DSC meeting/Bryan Fang from CIMICS conversation: WG-14 to explore ideas to prevent information sent by a modality from being intercepted and tampered with**. Did not discuss.

14. **MITA Update: Collaborative white papers (review Carolyn Hull proposal to add them under the Security page)**Did not discuss, but group approved of adding papers to the website when they are complete.

a. **Whitepapers:** Review options for website.

Development of shelf-ready content-

This project still holds a high priority as it's important for DICOM & MITA to have these resources.

- Concept description:
- Develop a series of short documents – stories – around 700 words that can be posted on DICOM website as FAQ-type info and able to send to have these short pieces at the immediate ready when some issue blows up and media and others request written feedback with an ASAP timeline.
- **Audience**: These are not meant to be technical engineering papers. These are something a product manager or a regulator would read. ~700 words is about the length of an opinion piece, be able to give to media and use in an FAQ.

Topic / Title	**Content to be included**	**Lead**
"Why doesn't DICOM mandate security"	- Possible content: DICOM is not a regulatory body - Not always the best fit solution for a particular organization	Rob
"How can I tell if my system is exposed?"	- We describe how to do it.	Hans v on tcon 2019-12-17
"*How to turn on encryption and why"*	- Different for modalities and PACs	Hans v on tcon 2019-12-17
"How an administrator could use SHODAN to find leaks"	- "You've heard about all of those exposed DICOM ports, you can find out if any of yours are exposed at your institution. Enter info into Shodan & it will tell you the open ports and IP addresses..." - Can be tricky if have dynamic IPs and such, but at least give them guidance	**Can add these to the DICOM website when complete and discuss with SIIM.**
"Hey administrator, have you looked at X / have you considered…?"	- DICOM is not responsible for the deployment. We don't want to come across as defensive, rather, explain what the reader can do	
"What to put in an RFP".	- Ensure content doesn't stray into anti-trust territory. We think we can include content that is general, but helpful.	

	- Maybe just include hyperlinks to sections? Call out the preamble, gives the mindset, intent – this could turn into a nice short piece	
One-Pager Checklist	- Audience: For administrators, including PACS and CISOs. - Include a short, focused list, a one pager/check-list for PACS Admins and only coming from the DICOM side (noting which may be DICOM-only and which may need to be DICOM-MITA jointly developed) - The content and goal are to aim end users at **NSA Manageable Network** paper - Example: The real basics, Step 1: the real danger is connected to your network, many do not realize that they have holes, know your use case - **Status**: The WG started a draft on the call (2019-12-17).	

6 Profile/standardizing a user authentication scheme, re: 2FA.

7 NSA Manageable Network paper

- **Action item**: Add in a section to the same white paper talking about NSA. A new document web security considerations. Then, if people want to do DICOM 2.0, can go further. Add to table. Will be looking for a volunteer.

– This has been discussed on several past calls. The proposal is for WG-14, jointly with MITA, to create a white paper based on NSA Manageable Network Plan. NSA created a high-level project plan. Add details about how to use DICOM and MDS2 to help fill in the gaps. MITA will help to produce and promote.

– Target audience: Hospital CISOs

– Link to draft: Rob Horn started a rough draft, is in Meeting Folder for 15 May 2019 (Note: DICOM does not list link to meeting folders in the Minutes).

– Link to NSA site: https://apps.nsa.gov/iaarchive/search.cfm?criteria=manageable+network+plan

– **Status update:**

8 DATE AND TIME OF NEXT MEETINGS

The next face to face meeting and any teleconferences of the committees can be proposed.

Tuesday, March 23, 2021, 9:00AM ET

Tuesday, April 27, 2021, 9:00AM ET

12. ADJOURN- 10:01AM ET.

Reviewed by Counsel 3/5/21

NEMALINK CODE	09-wg14
SUBMITTED BY	Hull, Carolyn
SUBMITTED ON	2/25/21
LEGAL REVIEW	
UPLOAD LOCATION	Enter upload location.