DICOM®

Digital Imaging and Communications in Medicine

September 12, 2019

Pia Dangelmayer
Bayerischer Rundfunk
Floriansmühlstraße 60
80939 München

Dear Pia Dangelmayer:

DICOM is taking the opportunity you offered to provide its thoughts on your analysis regarding the security of medical image data managed by others. Much has already been achieved to make medical data more secure. Still, additional effort is helpful to educate more broadly those charged with applying the proper measures for keeping data secure.

Dr. Pianykh's study implies that some sites with DICOM-capable systems may need to better address security issues, for example, by using established DICOM Secure Communications Profiles and Audit logs, as documented in the Integrating the Healthcare Enterprise (IHE) ATNA profile (https://wiki.ihe.net/index.php/Audit_Trail_and_Node_Authentication).

Your assertion that there are "millions of sensitive datasets on patients" at risk, if based solely on Dr. Pianykh's research, is not valid. Unless he did follow-up research, his published paper does not confirm that those systems have any sensitive data on them. Further, it does not make any assertions about the numbers of datasets or that those systems would release any sensitive data if requested. He simply identified systems that would respond to a DICOM Association Negotiation request by accepting such a request (~700) or by rejecting it (~2000), and he apparently did not attempt to discover what was on those systems. Entries in the Shodan database (https://www.shodan.io/) indicate a variety of types of DICOM-capable systems (e.g., viewers) responding to connections, not just PACS servers. For instance, recent interest in artificial intelligence processing of medical images has resulted in contests where research data (very large numbers of medical images which have been scrubbed of patient identifying information) is posted on public servers for contestants use in developing and testing their algorithms. Without close inspection, these DICOM images might appear to be private patient data.

This is not to suggest that situations don't exist where patient data could be exposed, or that hospitals and other medical imaging facilities have no further room for improvement. Rather, this situation is complex, and inferences based on numerical estimates should be made with great caution.

DICOM response to specific questions

1. Do you know of the problem that millions of datasets of patients are openly accessible on the internet?

No. We are aware there are about 700 to 800 systems that will respond to an ordinary connection request for DICOM services over the open internet. We know this includes test systems provided by vendors, educational systems for use by students, archives of educational material, veterinary hospital systems, and materials testing labs (DICOM is used for more than human medicine). We have not seen evidence that millions of datasets are openly accessible on the internet.

Due to concerns regarding the legality of exploring confidential databases, we do not know how one would go about arriving at an estimate of their own.

2. According to the minutes, Mr. Lawrence Tarbox was tasked to reach out to Mr. Pianykh and invite him to join WG-14. Did he ever extend that invitation and/or reach out? What was the result?

Dr. Tarbox was directed to the peer-reviewed journal article outlining Dr. Pianykh's research. The article sufficiently answered the questions that WG-14 had concerning the study.

3. According to the minutes, in November 2016, WG-14 was discussing whether "DICOM is perceived as a security risk (how serious is this, how true?)". After becoming aware of the study and Mr. Tarbox tasked with reaching out, the answer to this question seems to be yes, especially given that the publication of a follow-up research was being discussed in March 2017. Are we correct in assuming that WG-14 concludes that the findings of Mr. Pianykh are serious in nature and/or proof that DICOM indeed is to be judged as a security risk?

The statement in the minutes refers to perceptions which seem to exist in the market, as reflected in some media articles. The DICOM Standard Committee was most interested in how strongly and widely held these perceptions were and whether there might be some truth to them.

DICOM WG-14 concluded that the DICOM Standard did not inherently pose a security risk. The Secure Connection capability (specified in DICOM for almost two decades) is very secure. Proper security, however, requires more than just technical measures. It requires the implementation of institutional plans and policies to address various aspects of security (for example: infrastructure, device configuration, procedures, policies, training, auditing and oversight).

Papers like Dr. Pianykh's are useful to motivate healthcare providers and vendors to deploy the features that are available in DICOM. Security officers at hospitals prioritize their efforts based on the threats they observe and/or become aware of. Therefore, the work of Dr. Pianykh, Shodan and others is helpful in heightening security officers' awareness.

4. To the best of our knowledge, the DICOM standard committee didn't put out alerts or send out warnings to customers, and/or vendors, cloud infrastructure providers and hospitals that use these protocols and PACS-servers. Is that correct? If yes: Why didn't the DICOM standard committee put out warnings and/or alerts? If no: Can you send us copies of the warnings and/or alerts you put out?

WG-14 did not initiate a CVE report (an alert) because there did not seem to be any gap or abuse of the DICOM Standard specification involved. Security mechanisms are documented and there are legitimate needs for both open and secure connections.

It is not within the DICOM charter to examine all vendor products that implement all or some part of the DICOM Standard, or to evaluate customer installation, configuration, and use of those vendor products.

That said, the DICOM Standard Committee publicly published Part 15 (which is focused on the security-related mechanisms of the protocol) and notified the DICOM community (which includes vendors, users, governmental representatives and other interested parties) in 1999, and has publicly republished the standard many times since then.

5. Is security a traditional item in the scope of DICOM?

Yes, in terms of specifying security mechanisms in the DICOM Standard and making that information available to the DICOM community. The DICOM Standard Committee has considered security issues since its inception, ultimately leading to the formation of Working Group 14 on Security in the 1990s.

Starting in the late 1990s, WG-14 added security and privacy mechanisms to the DICOM protocol to support such things as secure network connections, digital signatures, encrypted email and media, encryption of files and parts of files, de-identification, audit trails, device authentication, and user identity-based access.

WG-14, the DICOM Standard Committee, and more recently WG-29 (Education, Communication, and Outreach) make a point of educating the DICOM community of the mechanisms available in the DICOM Standard. DICOM Security mechanisms are included in DICOM conference presentations on a regular basis and periodically in presentations at annual meetings of organizations such as the Radiological Society of North America (RSNA), Society for Imaging Informatics in Medicine, and American Association of Physicists in Medicine (AAPM). The DICOM website highlights security in the "Using DICOM" section (https://www.dicomstandard.org/using/security/). Members of WG-14, working as part of the Medical Imaging & Technology Alliance (MITA), prepared a series of security related whitepapers in a collaboration between MITA, COCIR, and the Japan Medical Imaging and Radiological Systems Industries Association (JIRA) from 2001-2007. (https://www.medicalimaging.org/policy-and-positions/joint-security-and-privacy-committee-2/).

Properly securing an institution that might use the DICOM Standard goes well beyond the charter of DICOM and by extension, the responsibilities of its committee members. National Institute of Standards and Technology (NIST) and National Security Agency (NSA) documents make clear that a technical interchange standard by itself cannot assure security. It can provide the means to facilitate the secure exchange of information, but ultimately security is dependent on the environment in which the standard is used. If users do not deploy, activate and maintain secure communications protocols, or do not protect keys on which those protocols are based, there can be no guarantee of security.

6. If not, who is responsible for keeping PACS-servers safe and secure?

The actual implementation, deployment, purchase, maintenance and configuration of systems that implement the DICOM Standard are the responsibility of the product vendors and their customers. Further, it is the responsibility of the vendors to provide and maintain software implementations.

Some guidance on how a number of security topics can be collaboratively addressed is provided on the MITA website (https://www.medicalimaging.org/policy-and-positions/joint-security-and-privacy-committee-2/)

Healthcare providers are regulated by the U.S. Department of Health and Human Services (HHS) and other agencies and are subject to rules such as Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR). Vendors are regulated by the U.S. Food and Drug Administration (FDA) and other agencies and are subject to regulatory cybersecurity directives.

DICOM is a standards development organization. Its responsibility is limited to defining and maintaining the standard so that it can be used effectively by vendors and institutions. The membership includes many manufacturers, medical professional societies, government organizations, and provider organizations.

7. Are there any cases you know of in which malicious actors were able to access this data?

No confirmed breaches due to flaws in the DICOM security protocol have been brought to the attention of the DICOM Standard Committee.

8. WG-14 was dormant for more than ten years. Right after the publication of Mr. Pianykh's study the working group comes back to life. Was the study of Mr. Pianykh the reason to re-establish WG-14? If not: Why was this group dormant for more than ten years and why was it re-established?

WG-14 was extremely active in the late 1990s and early 2000s, publishing seven major supplements to the DICOM Standard covering technical capabilities that could be incorporated into vendor products and used by provider sites to enhance security. These mostly leveraged general IT standards, such as Transport Layer Security (TLS) (the same protocol that secures web transactions). By 2006, the planned objectives of WG-14 were completed and the group's focus turned to maintenance of the specifications. WG-14 continued to report at meetings of the DICOM Standard Committee, keeping abreast of developments and monitoring for potential additional work items. In 2015, independent of Dr. Pianykh's work, WG-14 launched several new work items aimed at improvements to some mechanisms already in the Standard, retiring some mechanisms that were obsolete, and evaluating whether any new mechanisms were needed to support the new DICOMweb™ protocols. Dr. Pianykh's concerns came to our attention while these activities progressed.

Important Points to Consider

1. ***DICOM added a secure connection capability to the standard in 1999, 20 years ago*.**

   Prior to 1999, products assumed they were being run on a secured (e.g. limited access) network.

2. ***DICOM specifies protocols; vendors implement those protocols in their products' features; healthcare providers install and operate those products, utilizing those features*.**

   DICOM is responsible for defining relevant security mechanisms in our protocol. Vendors are responsible for implementing security features in their products. Healthcare providers are responsible for securing their facility and making appropriate use of security features.

3. ***We estimate there are about a million DICOM-capable devices in the world; the vast majority of those have been installed and configured with some degree of security.***

   The Shodan database identifies ~700 systems in the US that have been installed and configured with an open connection on the public internet, which agrees with Dr. Piankyh's experiments. Even though it is a comparatively small number, it may be possible that some of those systems may contain patient records. Those likely represent bad configuration choices on the part of those operating those systems. Some of those 700 systems do not contain patient records and have open connections to support product development, product demonstration, interoperability testing, product evaluations or performance tests, anonymized education or research datasets, and veterinary data~~.~~

If you have any questions, please do not hesitate to email or call.

Kind regards,

Lisa Spellman
DICOM General Secretary
lspellman@dicomstandard.org
Direct line: +1-703-841-3237

cc: Kevin Cosgriff
Jeff Tomitz
Clark Silcox
Tracey Cullen
Patrick Hope
Zack Hornberger
Luiza Kowalczyk