Security and Privacy in DICOM

DICOM – Digital Imaging and Communications in Medicine – is *the* international standard for medical imaging. It has been developed since the early nineties and has roots that go back even further. So how does such a mature – or should we say old – standard hold itself in the modern world of IT, with data in the clouds, hackers accessing our (medical) systems, ransomware in hospitals, and the like? The short answer is that DICOM is up to its task, also in the areas of security and privacy, but that the actual security and privacy depends entirely on the implementation of the standard: both in the products as well as in the deployment of these products in the field. (Remember, DICOM is not a software package; rather, it is specifications for information exchange. It is similar to the NEMA specifications for electrical power plugs and sockets. A product development team uses these specifications when creating a product.)

Some history

Starting in 1999, the DICOM Standard has included options for encrypting and protecting data moving over network connections. This was in response to the implementation of HIPAA (Health Insurance Portability and Accountability Act) and not in response to cybersecurity concerns.

In 2001, DICOM extended the use of CMS (Cryptographic Message Syntax) for encrypting DICOM data. It specified how sensitive portions of a DICOM object (PHI-Protected Health Information) can be encrypted within the DICOM object (the digital equivalent of a DICOM image) for safekeeping. Hereby it offers protection of a DICOM object throughout its life, and not just during information interchange. This encryption of *sensitive portions* of a DICOM object is an integral DICOM capability. When the goal is to encrypt the *entire* DICOM object, this is not in the scope of DICOM. It is, however, facilitated by DICOM to be performed by other encryption methods.

Security and privacy mechanisms

Most DICOM objects contain images and associated demographic and medical information about the patient, which need to be kept confidential. Encryption is one way to keep these data confidential. DICOM does not specify the encryption in detail (it refers to other standards for that), but several changes made to the DICOM Standard over the last decade facilitate encryption, including the transfer of encrypted DICOM objects, and reading of encrypted DICOM objects on the receiver's end.

- When sending those objects in an email, DICOM defines how to encrypt the files using CMS encryption methods for email.
- When sending those objects using traditional DICOM transfer mechanism (the DIMSE protocol), DICOM defines how to use an encrypted TLS connection.
- When sending those objects using the new DICOM transfer mechanism (DICOM web services), DICOM defines how to use an encrypted HTTPS connection.

Important to note is that DICOM merely facilitates the use of encryption but does not mandate it. It defines how encryption is to be used in a DICOM context. Whether to employ encryption is a policy choice of the hospital and an implementation choice of the product vendor. If the vendors have chosen not to implement encryption, or even if they do, hospitals can choose to set up a VPN encrypted network and use unencrypted DICOM. This is actually quite common between sites, but may, from a cybersecurity point of view, not be advisable.

Conclusion

The security and privacy capabilities of the DICOM Standard are only a small piece of the total protection of the privacy and protection against intrusion and hijacking of medical data. The CIOs (Chief Information Officers of the hospitals, health care systems and other health care providers) are responsible for protecting the medical data of their customers, i.e. the patients. Ultimately these CIOs have the capability and the responsibility for implementing and maintaining the protective mechanisms within their own systems and the interfaces towards these systems. DICOM is ready to facilitate this.

Authors; DICOM Co-Chairs Jeroen Medema- Philips, Robert Horn-AGFA, Lawrence Tarbox-Univ. of Arkansas for Medical Sciences