Medical Imaging Information Security in 2020

Professor John Magnussen and Samuel Baartz

28 October 2019

Executive Summary:

Digital technologies have touched every part of our lives and - to varying degrees - increased the attack surface and the risk of compromise to individual's sensitive personal data.

Information security of medical imaging in Australia has been severely compromised by a combination of Government inaction and professional convenience.

Legislative or at least regulatory changes are required to secure the vast and rapidly growing stores of medical images and related metadata stored around Australia.

Overview:

Like every area of our lives that has been digitised, in medical imaging too, we are facing tough choices that pit convenience and expediency against security and privacy. Over the last 15-20 years, medical imaging has transitioned from an arcane analog realm into the digital domain. Security was once achieved through inconvenience – printed sheets of film stored in bags to be found spread throughout hospital wards, radiology compactus' and abandoned under patients' beds.

A combination of events led to a rapid transition to digital image acquisition, storage, transmission and viewing. Security and cross-site accessibility aside, it has been an amazingly successful transition, leading to the almost complete demise of printed images and more recently to the rapid waning of portable digital media for image transport and storage.

Medical imaging has followed a path remarkably similar to that of the LP record – first to digital format that the holder of the media owned (CDs), then digital downloads (iTunes) and now on-demand listening (streaming services such as Spotify).

Like the music industry, the regulatory environment has been left far behind. Unlike the music industry, in the medical imaging industry digital rights management and security has been all but forgotten. (See *Table 1* for a comparison)

Several keys issues underlie the failure of medical imaging industry to provide a secure, accessible and compatible archive to the Australian public, each with severe consequences for the privacy of patient data. These shortcomings include no universal patient ID's, lack of centralised image storage, competing medical imaging providers, Medicare not valuing the images, lack of indexation of Medicare benefits. (See *Table 2* for further information)

Table 1: Comparative security measures between the music and medical imaging industries

	Streaming Music	**Medical Imaging**
Copy protection	Very strong	None
Digital licencing	Very strong	None
Access control	Very strong	Often none
User ID management	Very strong	Often none
Media validation	Very strong	None
Encryption	Very strong	None
Digital signatures	Very strong	None
Version control	Very strong	None
System interoperability	Very high	Very limited
Backup	Very good	Often very limited

Table 2: Shortcomings of the medical imaging industry and their consequences

Issue	Consequence
Lack of universal ID for patients[1]	Proliferation of local IDs which are inherently incompatible and often duplicated, making report and image matching difficult at best. Reducing quality of care and increasing the attack surface.
Lack of a central archive or central index for images	Proliferation of local image and report storage repositories, many with different access methods, logins and limited compatibility. This means that end-users (referrers such as GPs or specialists) require multiple different platforms, access points and logins, further increasing the attack surface.
Multiple, competing medical imaging providers	No price or market incentive to retain images or to share access to them with others, reducing quality of care and increasing costs for practitioners.
After report generation, Medicare places no value on images	No legislative or regulatory incentive to regulate, control or adequately secure access to images.
Lack of indexation of Medicare benefits	Reduced operating margins have meant that older image transmission and storage mechanisms (CD, USB, Film) are uneconomical and are being abandoned.

Medical imaging data is inherently insecure

The IHE DICOM 3 'standard', which enabled the modern transformation of medical imaging departments and the creation of large archives (PACS) which now often span multiple states and contain hundreds of millions of cases, was never designed with image security in mind.

There is no digital signature and no transport encryption. There is no confirmation of completion of transmission – of data integrity and completeness. Communication between machines (sources and sinks for data) are not validated, allowing for easy insertion of false data or unregulated querying of databases.

As recent experience has shown[2] [3] [4] exposing these security naïve networks to the outside world is not only commonplace, but also possibly disastrous, even without any hacking being required.

---

[1] The individual healthcare identifier (IHI) program was meant to provide a universal ID for patients (and providers), however its design and implementation, together with its lack of transparency and poor access, means that it has become yet another identifier that is rarely, if ever, used in Medical Imaging in the private sector.

[2] Gillum, J., Kao, J., Larson, J., "Millions of Americans' Medical Images and Data Are Available on the Internet. Anyone Can Take a Peek", ProPublica, September 17, 2019.

[3] Saarinen, J., "Millions of Australians' sensitive medical images, data left openly accessible", IT News, September 20, 2019.

[4] Gregory, A., "NHS Patients' medical images open to all on web", The Times, September 29, 2019.

Why protect medical imaging data?

Without going into great detail, there are numerous reasons why medical imaging data is worth taking the time to protect, and include:

1. Individual privacy and a breach of confidentiality[5]
2. Loss of data integrity impacting health outcomes
3. Data availability attack impacting health outcomes
4. Loss of confidence in the medical imaging profession
5. Blackmail of high-profile targets[6] and political manipulation
6. Commercial exploitation[7]
7. Ransomware attacks[8]

A system vulnerable to exploits

Large archives containing millions of patient encounters are now common, as are conglomerates or practice groups, spanning cities and sometimes states. Single points of entry or exploits can lead to large data breaches in which networks are connected to large numbers of 'imaging modalities', of varying age and security.

Many of these modalities (x-ray machines, ultrasound units, CT or MRI scanners, etc.) are built on older operating systems, poorly patched or updated and with many units 10-15 years old, often unsupported and forgotten.

This leaves them vulnerable to many forms of hacking, particularly as Medical Imaging practice networks are usually poorly segmented if at all - client accessible machines often access the same subnets as the modalities, including WiFi, providing easy access for compromised computers.

As was shown with Stuxnet, state actors can design attacks with particular end-points in mind, and insertion of attack vectors into a medical imaging network would be trivial at this point.

This provides a large risk of 'loss of confidence', for individuals, for companies, including listed entities (with an inherent large share price risk).

Protection is required from key exploits:

1. Data insertion - putting bogus studies into PACS to pollute them or to target individuals
2. Intentionally corrupting existing data, either by internal actors intentional or otherwise, or external actors, ‘hacking’ the RIS (radiology information system)
3. Denial of service – ‘breaking’ or shutting down imaging modalities across networks.

---

[5] Borys, S., “Inside a massive cyber hack that risks compromising leaders across the globe”, ABC News, October 2, 2019.
[6] Kolata, G., “You Got a Brain Scan at the Hospital. Someday a Computer May Use It to Identify You”, New York Times, October 23, 2019.
[7] Vast datasets are required for machine learning, which is set to transform medical imaging
[8] Hendry, J., “Victorian Hospitals go offline after ransomware attack”, IT News, October 1, 2019.

What is required from here?

The easy parts of the equation include:

1. Assist Specialist Colleges to create Security Guidelines
2. Use the best of ASD to develop 'best practice' for
    a. User engagement
    b. Network segmentation
    c. Access control and monitoring
    d. Audit procedures
    e. Critical system backups
    f. Stopping network threat propagations - moving from one network to the next once they are 'inside'
3. Provide tools for auditing access, both legitimate and illegitimate
4. Have a mechanism to report breaches which is not wholly punitive
5. Engage with the medical fraternity in general about their roles and responsibilities. Data security is necessary, even if a cost to your business.

The harder part requires a change of approach by Government.

Without a single, unique and accessible ID and a central, secure archive or index, there is no way to globally increase security without locally increasing inconvenience, which is no longer tolerated. Retrieval times of days for images (in the times of films in bags) are long gone and load times of minutes for CDs are not tolerated or affordable.

The current IHI system[9] allows for multiple 'unique' IDs per patient, does not replace any other ID and is not easily accessible by either the patient or the medical providers (no positive ID with the number(s) exist). As such, the IHI cannot be used by medical imaging providers to identify a patient and are unlikely to be adopted in any meaningful way.

Even if a universal ID did exist, without a central archive or at the very least index, access and security of medical images will remain a hodgepodge of confusingly incompatible and variously inaccessible systems with generally poor or non-existent security.

Conclusion

Like all areas of our lives, medical imaging is being transformed by the proliferation of digital technologies. While attempts have been made to secure and organise this industry, today there are profound structural issues. These structural issues, if exploited, could result in the widespread breach of sensitive health data and lead to significant cases of fraud, brand damage and legal disputes. Urgent reform is necessary and must be pursued in a unified fashion by both industry and Government.

[9] Australian Government Department of Human Services, "Individual Healthcare Identifiers", Australian Government Department of Human Services.

Professor John Magnussen (MBBS, PhD, FRANZCR, FRSM) is a Diagnostic and Interventional Radiologist and the Professor of Radiology at Macquarie University, Sydney. He is on the eHealth Committee of the Royal Australian and New Zealand College of Radiologists and has been involved in the design and build of multiple radiology practices including PACS and RIS, AI research with Fujitsu and GE as well as speaking on technology in Radiology.

Samuel Baartz (M.A. International Security Studies) has been working the private sector for a cybersecurity company for the past three years. Presenting this in his capacity as a researcher, Samuel has completed a Master's Degree in International Security Studies with a focus on emerging technologies and their impact on intelligence collection.