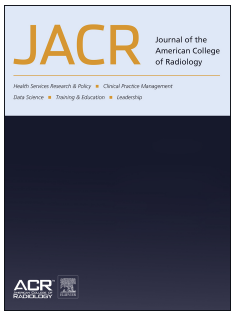
# Journal Pre-proof




JACR Cybersecurity Expert Panels: Cybersecurity Imperatives in Radiology Practices

Sanaz Vahdati, MD, Shawn Clark, MHA, MS, MFA, Gal Gnainsky, MBA, Devang Gor, MD, MBA, Chris Joerg, MS, Po-Hao Chen, MD, MBA

PII: S1546-1440(25)00258-3

DOI: https://doi.org/10.1016/j.jacr.2025.04.031

Reference: JACR 6856

To appear in: *Journal of the American College of Radiology*

Received Date: 11 April 2025

Accepted Date: 18 April 2025

Please cite this article as: Vahdati S, Clark S, Gnainsky G, Gor D, Joerg C, Chen P-H, JACR Cybersecurity Expert Panels: Cybersecurity Imperatives in Radiology Practices, *Journal of the American College of Radiology* (2025), doi: https://doi.org/10.1016/j.jacr.2025.04.031.

# JACR Cybersecurity Expert Panels: Cybersecurity Imperatives in Radiology Practices

Sanaz Vahdati[1], MD

Shawn Clark[2], MHA, MS, MFA

Gal Gnainsky[3], MBA

Devang Gor[4], MD, MBA

Chris Joerg[5], MS

Po-Hao Chen[6], MD, MBA

[1] Department of Radiology, Mayo Clinic, Rochester, MN, USA

[2] Cybersecurity Technology Protection, Cleveland Clinic, Cleveland, OH, USA

[3] Philips, Amsterdam, NL

[4] Department of Radiology, Lehigh Valley Health Network, Allentown, PA, USA

[5] Radiology Partners, Los Angeles, CA, USA

[6] Imaging Department, Diagnostics Institute, Cleveland Clinic, Cleveland, OH, USA

## Corresponding Author:

Po-Hao "Howard" Chen, MD, MBA

Cleveland Clinic

9500 Euclid Ave, JJ3

Cleveland, OH 44195

chenp2@ccf.org

## ICMJE statement:

Substantial contributions to the conception or design of the work: all authors.

Drafting of the manuscript: all authors.

Revising the manuscript critically for important intellectual content: all authors.

## Leadership roles:

All authors report being employed at non-profit institutions.

Dr. Vahdati is a postdoctoral research fellow at the Mayo Clinic Artificial Intelligence Lab and a Society of Imaging Informatics (SIIM) Security subcommittee member.
Mr. Clark is the Manager of Cybersecurity Technology Protection at Cleveland Clinic.
Mr. Gal Gnainsky is the Chief Security Officer at Philips.
Dr. Gor is Chair of the Department of Radiology, Lehigh Valley Health Network, and Associate Professor of Radiology at USF Morsani School of Medicine.
Mr. Joerg is the Chief Information Security Officer at Radiology Partners.
Dr. Chen is Vice Chair of Artificial Intelligence of radiology, pathology, and laboratory medicine for Diagnostics Institute, an associate professor at Lerner College of Medicine at Case Western Reserve University, and a musculoskeletal radiologist at Cleveland Clinic.

## Conflict of interest disclosures:

All authors report no disclosures relevant to this manuscript.

# JACR Cybersecurity Expert Panels: Cybersecurity Imperatives in Radiology Practices


## Abstract:

Today's radiology systems rely heavily on interconnected electronic systems in order to deliver high-quality patient care. Security risks that interfere with access or jeopardize the integrity of any networked component can negatively impact patient care. Radiology practice is a susceptible target for cybersecurity incidents, and achieving optimal cybersecurity in this era of artificial intelligence requires strong collaboration between radiology practice and vendors. In this JACR Cybersecurity Expert Panel article, four cybersecurity experts across clinical radiology practice and industry share comments and deliver insights on critical steps required to be taken from both radiology practice and vendors' perspectives toward secure device procurement and mitigating vulnerability to cyberattacks.





## Keywords:

Cybersecurity, Ransomware, Procurement

# Introduction:

Increasingly connected and reliant on technology, healthcare has seen a dramatic growth in disruptive cyberattacks. The year 2024 was punctuated by some of the most impactful healthcare cyberattacks, affecting hundreds of millions of patient data, and 2025 has shown no sign of slowing down. Today's radiology departments and private practices must protect modalities, workstations, and server software, all the while responding to growing demands for artificial intelligence, remote work, and cloud [1].

With the looming threat of ransomware, data breaches, and other security-related disruptive changes, there is a rising emphasis on how radiology practices can collaborate with the industry to keep existing systems safe while keeping cybersecurity top-of-mind during the procurement of new hardware and software devices. In this JACR Cybersecurity Expert Panel article, four cybersecurity experts across clinical radiology practice and industry share comments and deliver insights on critical steps required to be taken from both radiology practice and vendors' perspectives toward secure device procurement and mitigating vulnerability to cyberattacks.



**Mr. Shawn Clark, Cybersecurity Technology Protection Manager, Cleveland Clinic**

68% of cybersecurity incidents involve a human element, while more than 40% of incidents involve social engineering [2]. This shouldn't suggest that vendors are less responsible for securing their medical devices. Early and often collaboration between vendors and Radiology practices is essential but must be cost-effective and easy to implement. Moving to an 'opt-out' instead of 'opt-in' security model is an effective way manufacturers can incentivize protecting Patient Health Information (PHI) with minimal impact on the device or the radiology practice. For example, devices storing PHI should have the hard drive encrypted by default. Vendors should be held accountable for maintaining and documenting the ongoing security of their devices, including vulnerability reporting, patching guidance, and software update schedules.

Radiology practices must also do their part to maintain the security of their patients' data. A list of cost-effective opportunities for preventing user error (Human element) includes:

- Training staff to recognize phishing and social engineering attempts
- Limit internet access to appropriate use cases for medical devices
- Disabling unused USB ports on medical and office devices
- Preventing installation of unauthorized applications on medical devices
- Isolate data from user traffic on the network, especially user internet traffic
- Separate business and personal emails

Security professionals who understand the complexities of medical practices should be engaged early in the lifecycle of the device as critical collaborators. As the number of devices and medical records increases, tools such as firewalls and routers are effective at protecting against internet threats and data loss. But asking a radiologist to manage a firewall is like asking a surgeon to assemble a spaceship. They could do it, but it's not the best use of time or talent.

**Mr. Gal Gnainsky, Chief Security Officer, Philips**

For healthcare systems, this means a continuous focus on protecting the "CIA triad " (confidentiality, integrity, and availability) by safeguarding patient data stored on or transmitted between systems, protecting data from malicious alteration or corruption, and ensuring solutions are always available to perform their intended function. Healthcare providers need collaborative relationships with cyber-mature manufacturers like Philips to partner on innovations, to improve care for patients, and to find the right "balance" during procurement processes between maintaining and supporting secure solutions over the long-run.

Suppliers such as Philips have made significant advancements in device and solution security through controlled processes, secure builds, and security technologies designed and integrated into product solutions. These advancements include vastly improved secure development lifecycle (SDLC) capabilities in tooling and security-by-design processes with robust security testing assurance and risk management to reduce risks to the CIA-triad over the lifecycle of products. While the security foundation of products is highly advanced today, two significant challenges are commonly observed across the medical solutions ecosystem: (1) the means to attain clarity in formal agreements that ensure the execution of shared roles and responsibilities between

healthcare providers and manufacturers. (2) a focus on enabling clear ownership and execution assurance of key risk management and lifecycle management processes to monitor and address developing security risks in the operating environment.

Meeting these challenges means concluding device procurement processes with a solid mutual agreement and handshake. In addition, clear expectations must be established in the shared roles to operate systems intended for clinical use, including end-user training, monitoring, maintenance, physical security, and ownership of essential risk management and product lifecycle management processes, and then doing so *together* with all playing their part.

**Mr. Chris Joerg, Chief Information Security Officer, Radiology Partners**

Radiology practices face a growing cybersecurity threat from ransomware and data breaches, demanding a proactive approach to safeguard patient data and maintain operational integrity. Collaboration with the industry is crucial to address this challenge effectively.
To protect existing data, systems and software practices should prioritize cybersecurity measures including, but not limited to:

- Modern endpoint protection
- 24/7 security monitoring and response services
- Regular security assessments and patching
- Robust access controls and data segmentation
- Immutable data backups
- Tested incident response plans
- User awareness training
- Collaboration with vendors for security updates and support

Cybersecurity is paramount when procuring new technology or vendor services; organizations should require vendors to demonstrate robust security measures and adherence to standards such as the Health Insurance Portability and Accountability Act (HIPAA), the National Institute of Standards and Technology (NIST), the Health Information Trust Alliance (HITRUST), and System and Organization Controls (SOC) while evaluating practices including data encryption,

access controls, and incident response plans, and selecting products with integrated security features and regular updates.

Additionally, key collaboration opportunities include forging partnerships with industry peers, technology providers, and cybersecurity experts to share threat intelligence, best practices, and incident response strategies, as well as engaging in initiatives that disseminate information on emerging threats and vulnerabilities [3][4].

My practice developed a new offering called Rad Clinical Continuity of Care. This paid service, when implemented, ensures that secure image-based care remains intact, even during an active cyber breach, thereby mitigating clinical, operational, and financial impacts.

**Dr. Devang Gor, Chair, Department of Radiology, Lehigh Valley Health Network**

The financial fallout and loss of reputation from a cyber-attack can drive radiology groups to bankruptcy. The balancing act between maintaining security and rapidly adopting innovation requires a multi-pronged collaboration with hospital administrators, vendors, IT and cybersecurity experts.

To secure existing systems, organizations conduct comprehensive risk assessments. On a recurring, frequent timeline, evaluate current infrastructure using frameworks like the NIST cybersecurity framework. Unpatched software or outdated operating systems are common in older equipment and are prime targets for ransomware; these vulnerabilities should be identified and corrected, Secure and maintain redundant backups, preferably off-site and encrypted. Periodically test the restoration process, engage vendors for frequent software and hardware updates, provide support for end-of-life devices. Engage staff through frequent education, training, susceptibility testing, educate about Phishing, which is the leading cause of breaches. Conduct cyber drills, prepare response plans, and engage media relations experts early in case of a breach. Enforce disciplinary action for repeated lack of engagement by any segment of the community.

Establishment of a strict security assessment protocol is required for all new software and hardware procurement. Organizations must mandate vendors to meet or exceed industry standards and

benchmarks for cyber-security, evaluate risks appropriately while deploying cloud-based systems and multi-vendor AI algorithms, perform robust testing prior to deployment and negotiate contracts that guarantee security updates throughout the equipment lifecycle.

A larger security budget should be justified to highlight the consequence of PHI leakage and devastating loss of revenue following a breach. Institutions must invest in robust cybersecurity insurance, work with regulators and groups like health ISAC to adopt proactive measures on the ransomware trends and advocate through professional societies such as the American College of Radiology to drive standardized encryption and industry-wide security improvements from vendors.

## Conclusion:

Radiology practice is a susceptible target for cybersecurity incidents. Achieving optimal cybersecurity in this era of AI requires strong collaboration between radiology practice and vendors, and the future of secure radiology practice lies in shared accountability [5].

Highlighted strategies provided for cybersecurity through procurement of devices in the radiology setting include security-by-design processes, regular vulnerability assessment, encryption, cost-effective user error prevention, and tested incident response plans. These strategies demonstrate promising outcomes for the secure procurement of devices in the radiology practice. Furthermore, engagement of vendors in regular updates, training of end users, ongoing awareness of emerging threats, and product lifecycle management processes are crucial to safeguard PHI in this rapidly evolving field.

# References:

[1] Shah C, Nachand D, Wald C, Chen P-H. Keeping Patient Data Secure in the Age of Radiology Artificial Intelligence: Cybersecurity Considerations and Future Directions. J Am Coll Radiol 2023;20:828–35.

[2] https://www.verizon.com/business/resources/T1ae/infographics/2024-dbir-public-sector-snapshot.pdf

[3] https://gkc.himss.org/resources-cybersecurity-and-privacy.

[4] https://www.nist.gov/cyberframework.

[5] Nguyen XV, Petscavage-Thomas JM, Straus CM, Ikuta I. Cybersecurity in radiology: Cautionary Tales, Proactive Prevention, and What to do When You Get Hacked. Curr Probl Diagn Radiol 2025;54:245–50.