PERSPECTIVES
IN HEALTH INFORMATION MANAGEMENT

Paper Categories For Authors For Reviewers Archives About

Input your search...

Vol. 19, Issue 3

# Securing Your Radiology Practice: Evidence-Based Strategies for Radiologists Compiled From 10 Years of Cyberattacks and HIPAA Breaches Involving Medical Imaging

*Gerald M. Bowers, MHA; Mary L. Kleinpeter, MA; and William T. Rials, PhD*

## Abstract

While there is significant literature discussing physical and cybersecurity risks around health information technology in general, the number of publications that specifically address medical imaging is much smaller, and many of these focus on the technical security requirements for the exchange of medical images over public networks rather than practical guidelines for radiologists and technicians. This study examines the US Department of Health and Human Services database of reported breaches involving medical imaging from 2010-2020, identifies the most common contributing factors to those breaches, and offers recommendations for radiology practices to prevent each, based on the National Institute of Standards and Technology (NIST) guidelines as well as measures proposed in the literature on health information technology.

Keywords: cybersecurity, picture archiving and communications system (PACS), digital imaging and communications in medicine (DICOM), Health Insurance Portability and Accountability Act (HIPAA)

## Introduction

In August 2021, the US Department of Health and Human Services sent a warning to health systems that vulnerabilities in medical imaging servers, namely picture archiving and communication systems (PACS), were responsible for over 275 million unsecured images across 130 health systems.[1] This report is the latest example highlighting not only the increasing cybersecurity risks within the healthcare industry—which saw a 55 percent increase in breaches between 2019 and 2020—but also radiology departments in particular.[2] Healthcare data breaches have quickly become the costliest of attacks across all economic sectors, and radiology groups and imaging centers have been increasingly affected in the form of ransomware, denial of service attacks, and lawsuits brought by affected patients.[3]

Interestingly, the vast majority of cyberattacks and breaches could be prevented if basic physical and information security practices were followed, many of which occur at the level of the clinician rather than the information technology or cybersecurity professionals employed by health systems. Despite this, little focus is placed on the role of physicians, technicians, and other healthcare providers in preventing the unauthorized exposure of medical imaging. While large hospital chains and academic medical centers are more likely to have advanced automated protections in place, independent radiologists and imaging centers must do more to involve clinicians in securing complex networks and devices.[4] As this review of breaches involving medical imaging in the US from 2010-2020 shows, basic human error continues to be the most prevalent cause of healthcare breaches and can be prevented through simple, yet often-neglected, measures.

## Methods

Specific instances of breaches or unintentional disclosures of medical images between the years 2010 and 2020 were identified in the US Department of Health and Human Services database of reported breaches[5] using the search terms “radiology,” “imaging,” “PACS,” or “DICOM.” Of 3,366 recorded breaches, 45 cases included these terms, and nine were excluded because no information was available on the type or outcome of the breach. Thirty-six cases involving the theft or illegal disclosure of medical images of 4,835,967 patients were identified and included in this study. These cases were categorized by the type of vulnerability leading to the breach (e.g., lack of physical security, unsecured PACS server, use of unencrypted networks, etc.) and recommendations for radiologists and imaging technicians to prevent similar breaches were proposed based on a careful review of the cybersecurity literature and the National Institute for Standards and Technology (NIST) recommendations for radiology departments.[6]

## Results

Thirty-six breaches from 2010-2020 were organized into nine categories, based on how personal health information (PHI) was accessed, and the number of patients affected (Table 1).

The categories “physical theft of PHI,” “loss of hard copy records,” “loss of unencrypted hard drives,” and “unauthorized access and unintentional disclosure of records” can all be considered failures of physical and information security practices. Together, these categories included 24 breaches from 2010-2020 affecting some 4.68 million patients. Three breaches involved the theft of unencrypted computers left in unsecured offices or taken home by employees and subsequently stolen. Another breach involved a former employee removing electronic protected health information (ePHI) from a practice. Five breaches involved PHI mistakenly mailed to the wrong physicians or patients who requested imaging records, billing statements, or annual reminders for mammograms. One breach involved clerical staff emailing ePHI to their personal email accounts to work at home. Server and software vulnerabilities resulted in three cyberattacks affecting the medical images of 65,516 patients, and two unintentional exposures of images on unsecured servers affected 65,911. One attack involved the business associate of a radiology practice, and two involved the internet-facing servers of radiology practices. Three programming errors affecting servers or billing software led to unauthorized users accessing ePHI. Three phishing attacks and one ransomware attack compromised the data of 7,500 and 10,700 patients, respectively.

The categories of breaches were also examined by the year they were reported to the US Department of Health and Human Services, and no discernible trends in the frequency of varies categories was noted (Figure 1). There were an average of 3.2 breaches per year between 2010 and 2020.

## Discussion

### Basic Physical and Information Security Measures

The types of breaches identified in this report match the conclusions of previous authors: namely, that data breaches of PHI in the US most often involve accessing electronic media from laptop computers or portable electronic devices, which are typically obtained through theft.[7] Many of the measures to prevent breaches of this nature will seem obvious but will still require effort for an effective implementation. These include the use of strong passwords, multifactor authentication, encryption of devices, and physical security measures like securing laptop computers not in use, the use of logbooks for issuing laptops and portal electronic devices, and ensuring network access is suspended and ID badges deactivated for former employees.

Wunsch and colleagues also recommend healthcare workers "learn their environments" to best guard against theft and unauthorized access of information.[8] Users in the radiology department should know where servers are located and where portable laptops and other devices are stored. Access to this equipment should be physically secure and available to a limited number of people.

Additionally, any exposed network plugs should be physically secured so that they cannot be pulled out and plugged into a different device. Networking equipment such as switches and routers should only be in secured rooms with limited access, and switches should be configured so that only pre-approved devices and computers are permitted to connect. Furthermore, unused network ports should be switched off until they are needed. Wireless networks should be operated in a secure configuration, which needs to be reviewed and updated at regular intervals.[9] Any wireless "guest" devices like personal cellphones or computers should be segmented and not allowed to interface with the primary healthcare network.

### Server and Software Vulnerabilities

In 2020, the US Cybersecurity and Infrastructure Security Agency (CISA) identified security loopholes in the software of over 100 types of devices, including radiography, computed tomography (CT), magnetic resonance imaging (MRI), ultrasound (US), mammography, positron emission tomography (PET), fluoroscopy, and others.[10] Of these loopholes, unsecured servers represent one of the greatest security risks to radiology departments. Studies conducted using internet scanning tools have identified thousands of unprotected servers in the United States. In radiology departments, the unprotected servers are most commonly PACS, containing medical imaging studies and other sensitive ePHI.[11,12] In most instances, these vulnerabilities never result in breaches, but they present an enormous risk to radiology departments and can be prevented with the implementation of simple IT security measures.

Many software loopholes and vulnerabilities can be mitigated by using basic cyber hygiene, such as limiting the use of administrative privileges. It is not uncommon for end users to have administrative privileges allowed on their user accounts for convenience and flexibility. However, the United States Center for Internet Security (CIS) has reported that the misuse of administrative privileges is a "primary method" for attackers.[13]

An essential step that radiologists and technicians can take to mitigate these risks is to ensure their IT department utilizes what is known as a continuous vulnerability and patch management system that regularly updates operating systems, applications, and firmware to adhere to medical device advisory released by CISA. Any legacy systems that can no longer be updated should be replaced.[14] Other examples of vulnerabilities identified by CISA include older versions of DICOM servers, which transmit messages in unprotected, clear-text format that can be exploited if an attacker has access to the network[15] and methods of hiding malware within DICOM files.[16] DICOM servers that are connected to the internet should be protected by a firewall and require a VPN connection and password to be accessed via the internet.[17]

## Targeted Phishing and Malware Attacks

The most probable and oftentimes most damaging attack directed at health systems is ransomware, which is a form of malware that encrypts files on the infected computer and its shared networks and then displays a message demanding the payment of a ransom. A particularly concerning subset of ransomware is known as killware. Killware is a type of malware that causes substantial physical harm or death.[18] When ransomware incapacitates medical equipment or medical records, diagnoses may may be delayed or missed and people's lives and well-being can be put at serious risk. In these scenarios, ransomware may be considered killware. Rials suggests that ransomware attacks will continue to be a top cybersecurity threat, and variants will evolve to become more technically advanced.[19] Most ransomware variants involve human interaction for the malware to be activated and spread throughout the network.[20] A common injection method for ransomware is phishing, a form of social engineering that can be used to gain access to a network and then disrupt health services, steal ePHI, or target individual patients.

Another route for the delivery of malware and for data theft is via portable storage media such as universal serial bus (USB) memory sticks. Sittig and colleagues recommend that "at the local device level, organizations should consider disabling USB ports to prevent malicious software delivery."[21]

If feasible, healthcare institutions should use application whitelisting on servers, desktops, and laptops so ransomware and other unauthorized executables cannot be run. This requires organizations to develop a "whitelist" of specified programs that are allowed to run. This should be relatively simple in the PACS context where only a limited number of applications will be used (e.g., on a diagnostic workstation), whereas this might be a rather complex task on general-purpose office PCs.[22] Anti-malware software should be regularly updated on all endpoints throughout the network.

While backups do not prevent cyber incidents from occurring, they do aid in incident response. Unfortunately, cyber incidents have become a ubiquitous facet of life, and some attacks will inevitably succeed, making strong incident response, including backups, necessary.[23] Strong cybersecurity plans should be focused on fast and efficient response to cyber incidents as well as prevention methods. Accessing secure and air-gapped backups is one of the first steps when responding to cyber incidents. Sittig et al. also recommends that backups "should be made frequently (i.e., at least daily, and a continuous or real-time backup is ideal)."[24] Organizations should use the 3-2-1 backup rule: Maintain at least three copies of your data, keep two copies in separate locations, and store at least one copy off-site.

Detection-based tools can give protection to a certain extent but are becoming less effective because advanced threats are not easily detectable in the first place and hundreds to thousands of new advanced malwares are being developed every day by cyber criminals, making it simply impractical and impossible to detect them.[25]

One of the fist steps in improving your cybersecurity posture is to perform a cyber risk assessment to discover any vulnerabilities. Once the weaknesses are identified, tools like gap analysis can be used in order to create remediation plans for any identified risks. When discussing cybersecurity, gap analysis refers to the process of reviewing an organization's existing security controls and determining whether these need to be strengthened, or if new controls need to be added, in order for the company to attain its preferred level of security.[26] Therefore, organizations should continually work toward addressing items in the cyber gap analysis to improve overall cybersecurity posture.

A summary of the most pertinent recommendations according to the categories of breaches discussed is included in Table 2.

## Limitations

There were several limitations of the present study. Most notably, the US Department of Health and Human Services database provided very narrow descriptions on the circumstances leading to each breach, which presented a challenge in making detailed recommendations to mitigate specific server or software vulnerabilities that radiology practices may be facing. Additionally, while each breach discussed in the report was independently identified after being located using search terms, the reliance on common keywords associated with imaging like "PACS" or "DICOM" likely resulted in breaches that were missed during the review of the database.

## Conclusion

From 2010-2020, the US Department of Health and Human Services reported the loss of 4,833,667 patient records involving medical imaging. As examined in this study, many of these losses of PHI and ePHI occurred because of human error on the clinician level. Even the most advanced security solutions can be bypassed when the end users of software and devices or hard copy records fail to take adequate precautions to protect them.

However, such losses can be prevented if radiologists and imaging technicians take simple yet frequently overlooked steps to improve their cyber hygiene. These include preventing physical loss of PHI by restricting access to devices, servers, networking equipment, and physical files. Likewise, server and software vulnerabilities can be prevented by regularly updating software and replacing legacy systems. Clinicians can also prevent phishing and malware attacks by disabling USB ports at the device level, utilizing application whitelisting, regularly updating anti-malware software, and by backing up data. Taken together, such steps can prevent devastating losses of PHI, severe business disruptions, and costly lawsuits from patients.

Funding/COI: None

Acknowledgements: None

## Notes

1. United States Department of Health and Human Services, "HHS Cybersecurity Program, Ransomware Trends 2021." https://www.hhs.gov/sites/default/files/ransomware-trends-2021.pdf. Accessed Nov. 15, 2021.

2. Bitglass, "Bitglass 2021 healthcare breach report: over 26 million people affected in healthcare breaches last year." https://www.bitglass.com/press-releases/2021-healthcare-breach-report. Accessed Nov. 15, 2021.

3. IBM, "2021 Cost of a Data Breach Report." 2021. https://www.ibm.com/security/data-breach. Accessed Nov. 17, 2021.

4. Gillum J, Kao J, and Larson J. "Millions of Americans' medical images and data are available on the internet. Anyone can take a peek." Pro Republica report, 2019. https://www.propublica.org/article/millions-of-americans-medical-images-and-data-are-available-on-the-internet. Accessed Nov. 16, 2021.

5. HHS Cybersecurity Program, Ransomware Trends 2021.

6. NIST Special Publication 1800-24, "Securing Picture Archiving and Communication System (PACS) - Cybersecurity for the Healthcare Sector," DRAFT, September 2019. https://www.nccoe.nist.gov/projects/use-cases/health-it/pacs. Accessed Nov. 15, 2021.

7. Liu V, Musen M, and Chou T, "Data breaches of protected health information in the United States." *J Am Med Assoc.* 2015;313(14):1471–1473.

8. Wunsch R and Moriarty A. "Solutions for Cybersecurity Threats Facing Radiology Practices." *J Am Coll Radiol*. 2021;18(11):1566–1568.

9. Eichelberg M, Kleber K, and Kämmerer M. "Cybersecurity Challenges for PACS and Medical Imaging." *Acad Radiol*. 2020;27(8):1126–1139.

10. Cybersecurity & Infrastructure Security Agency. ICS Medical Advisories. 2020.

11. Gillum J, Kao J, and Larson J. 2019.

12. Beek C. "McAfee researchers find poor security exposes medical data to cybercriminals. 2018. https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-researchers-find-poor-%20security-exposes-medical-data-to-cybercriminals. Accessed Nov. 16, 2021.

13. Tenable Documentation, "CIS Control4: Controlled Use of Administrative Privileges," 2021, https://docs.tenable.com/tenablesc/CIS-CAS/Content/Controls/Basic/Control-4/Control-4.htm.  Accessed Nov. 16, 2021.

14. Rials, W. "Top Cybersecurity Trends for 2021 and Beyond." *Homel Secur Aff*. 2021;1(3)

15. HHS Cybersecurity Program, Ransomware Trends 2021.

16. Ortiz P. "HIPAA-protected malware? Exploiting DICOM flaw to embed malware in CT/MRI imagery." Cylera Labs website. 2019. https://researchcylera.wpcomstaging.com/2019/04/16/pe-dicom-medical-malware/. Accessed Nov. 15, 2021.

17. Gillum J, Kao J, and Larson J. 2019.

18. Higgins M, "What is killware — and should you be worried?" 2021. https://nordvpn.com/blog/what-is-killware/. Accessed May 28, 2022.

19. Rials, W. 2021.

20. HHS Cybersecurity Program, Ransomware Trends 2021.

21. Sittig D and Singh H. "A Socio-Technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks." *Appl Clin Inform*. 2016;7(2):624-32.

22. NTT Security, 2017 Global Threat Intelligence Report (GTIR), 2017. https://www.nttsecurity.com/de-de/gtir-2017. Accessed Nov. 15, 2021.

23. Truong T. "'It's a matter of time:' Cyberattacks increasingly becoming the norm, 2019. https://www.wwltv.com/article/news/its-a-matter-of-time-cyberattacks-increasingly-becoming-the-norm/289-68473bea-0973-48e1-85d1-a13d741ffda5. Accessed May 28, 2022.

24. Sittig D and Singh H. 2016.

25. Zaw N and Soh K. "DICOM: A Ticking Cybersecurity Time-Bomb in the Healthcare Industry." *Healthcare Innovation*. 2017. http://www.athenadynamics.com/event/dicom-unknown-vulnerability-cyber-attacks-global-healthcare-industry. Accessed Nov. 15, 2021.

26. US Dept. Of Health and Human Services Office for Civil Rights. "Risk Analyses vs. Gap Analyses – What is the difference?" 2018. https://www.hhs.gov/sites/default/files/cybersecurity-newsletter-april-2018.pdf. Accessed May 29, 2022.

## Author Biographies

*Gerald M. Bowers is a medical student at Tulane University School of Medicine.*

*Mary L. Kleinpeter is a law student at Tulane University Law School.*

*William T. Rials is the associate director and professor of practice at the Tulane University School of Professional Advancement.*

*Perspectives in Health Information Management* is the quarterly peer-reviewed research journal of AHIMA.

© Copyright AHIMA 2022.
All Rights Reserved

AHIMA®

AHIMA®
FOUNDATION

STAY CONNECTED

- TWITTER
- FACEBOOK
- LINKEDIN
- RSS