



CASE STUDY: AMERICAN COLLEGE OF RADIOLOGY

ACR IMPROVES DATA PROTECTION, SAVES TIME AND MONEY WITH INFOLOCK'S MANAGED DLP PROGRAM

CUSTOMER PROFILE



HQ LOCATION

Reston, VA - USA

INDUSTRY

Healthcare

ORGANIZATION SIZE

500 Employees

ORGANIZATION SERVES

40,000 Medical Professionals

INDUSTRY CONSIDERATIONS



\$7.13 million

Average cost of a data breach in the healthcare industry



10.5% increase

The healthcare industry experienced a 10.5% increase in average data breach costs between 2019 and 2020

The American College of Radiology (ACR) is a professional medical society representing some 40,000 medical professionals, including radiologists, radiation oncologists, nuclear medicine physicians, and medical physicists. With core values of leadership, integrity, quality, and innovation, ACR is dedicated to serving patients and society by empowering its members to advance the practice, science and professions of radiological care.

As with other organizations driving change in the healthcare arena, ACR's lifeblood is data. With greater scrutiny being placed on data privacy and security by regulators and individuals, protecting information assets is an essential component of ACR's ability to deliver value to its stakeholders.

THE CHALLENGE

Data Loss Prevention (DLP) is vital in our age of digital communication and cyber-crime. According to an IBM-Ponemon study, DLP is among the key factors in mitigating the cost of data breaches (along with encryption, threat intelligence, and DevSecOps).

The impact is significant - the average cost per data breach in the healthcare industry is \$7.13 million.

And healthcare has the highest data breach costs of any industry. Breaches involving PII cost an average of \$150 per data record and HIPAA violations often result in heavy fines and other penalties.

Implementing and running a DLP program is complex. It needs to flex and adapt to a constantly changing environment. Managing the sheer volume of data—on customers, employees, and operations—is a major challenge. As data accumulates in size and duration, the likelihood of compromise increases.

Like many organizations, ACR manages a significant number of systems containing sensitive information. When the organization explored improving its risk posture with a DLP program, it became clear that it needed to find a partner with specific expertise in this domain that would provide guidance as well as experienced personnel to implement the program.

DECISION TO OUTSOURCE

ACR evaluated whether or not to expand the internal team's headcount or outsource the function to an experienced partner. Outsourcing proved to be a timely and cost-effective solution and provided additional benefits such as providing an objective third-party in sensitive instances.

"With Infolock, we got both a primary and an alternate analyst. And then, no matter how complex an issue might be, we've got depth inside their company."

"We wanted to ensure that sensitive data would only be shared with authorized individuals," said Matt Jordan, ACR's Senior Director of Security and Infrastructure. "And external DLP management addresses certain internal concerns. For example, if an incident investigation revealed an employee's delicate PII, a third party could be trusted to treat it impartially. As the saying goes, once you see something, you can't un-see it." Ultimately, they decided a third-party DLP solution was the best fit for ACR.

WHY INFOLOCK

After comparing numerous DLP solution providers, ACR chose Infolock for several reasons. Infolock has extensive experience implementing and managing successful DLP programs and other data protection solutions. With a focus on strategic governance, not just tactical techniques, Infolock's framework for data risk management was also valued by ACR. Infolock believes a successful DLP program must start with top-down policymaking and enforcement, something that resonated with ACR's belief in the importance of leadership setting high quality standards.

Infolock's grasp of the practical nuances of DLP was attractive to the ACR as well. For example, improper deployment,

configuration, and integration of a DLP program can generate false positives that interrupt key processes. And that can lead to business units demanding that DLP be turned off, defeating its purpose.

"Infolock also understood that cyberattacks targeting technical vulnerabilities weren't the only issue," said Jordan. "Human error and routine system issues account for half of all data breaches, especially through phishing and unintentional data exposure."

Finally, Infolock's approach to project management was a strong positive. For DLP programs, Infolock provides a dedicated analyst who becomes the client's trusted partner. The analyst—Shana Eichelberger in ACR's case—is both a technical expert and a relationship builder.

Infolock backs its primary analyst with a talented bench of DLP support professionals and an established, proven process. "With Infolock, we got both a primary and an alternate analyst," said ACR's Jordan. "And then, no matter how complex an issue might be, we've got depth inside their company."

THE SOLUTION

Infolock's approach to ACR's DLP program included the following key services:

- **DLP program development:** Infolock created administrative and incident-response runbooks to document all DLP processes and procedures, plus customized reports for ACR management.
- **DLP administration:** Infolock's basic blocking and tackling of ACR's DLP program included comprehensive implementation, detailed configuration, and software installation and maintenance.
- **Incident triage:** Infolock set up and fine-tuned workflows to reduce false positives and hold low-priority true positives outside the event escalation process. The goal was to avoid "chasing ghosts" and make the most efficient, cost-effective use of data security resources.
- **Comprehensive reporting:** Infolock provided daily system reports, weekly operational reports, and ad hoc reports. For example, a "Breakdown of 2nd-Level Responses" status report helped ACR understand anomalous activities, process glitches, and optimal staff allocations.

- **Collaborative consulting:** Infolock led weekly team meetings to assess incidents and recommend tuning, held quarterly reviews to identify key milestones for the next period, and presented an annual program plan to measure risk maturity.
- **Real-time responsiveness:** Infolock's dedicated analyst for ACR, Shana, provided instant feedback and nimble solutions whenever challenges arose. ACR did not have to call a support center, log into a portal to open a ticket, or wait for a callback from tech support.

Dan Reardon, ACR's Chief Compliance Officer, emphasized the value of this dedicated resource. "Having Shana immediately available, not having to play phone tag—plus her ability to ask the right questions, understand our needs, and come up with practical solutions—is a big positive for ACR."

THE RESULTS

Outsourcing DLP to Infolock has delivered many benefits to ACR, including:

- **Faster initial assessment of risk conditions:** Infolock's pre-tuned policies and custom workflows enabled ACR to start detecting the risk of data loss quickly.
- **More accurate, efficient incident response:** Infolock's first-tier triage has eliminated many false positives and created a workflow to set aside low-priority incidents for later review. As a result, only high-priority incidents are escalated, optimizing the efforts of second-tier support.
- **Improved incident visibility and mitigation:** Another outcome of Infolock's DLP program has been an increase in the number of incidents identified, reported, and resolved. One of the most effective mitigation techniques is automatic data encryption.
- **Better quality control:** Infolock's DLP system exposed policy violations and outdated processes, enabling ACR to improve procedures, secure sensitive data, and reduce risk.
- **More mature risk posture:** Infolock's managed services freed ACR to focus on high-level analysis and decision-making—a hallmark of risk maturity.
- **Cost savings:** Compared to managing all of the end-to-end DLP activities in house and hiring dedicated staff accordingly, outsourcing DLP to Infolock has represented a substantial cost savings.

"Infolock has become a trusted partner and helps us protect our most sensitive information," added Reardon. "Our collaboration with Infolock on DLP has been a major success for ACR."

"It's hard to run a DLP system. There is a particular expertise that goes beyond simply looking at daily tickets and blindly escalating them. With Infolock, we can be confident that we have a partner who is remaining vigilant and ensuring the system continues to work well."

Matt Jordan

Sr. Director of Security & Infrastructure



LEARN MORE AT [INFOLOCK.COM](https://www.infolock.com)

© 2023 Infolock. All Rights Reserved.