

THOUGHT LEADERSHIP

Don't let legacy PACS become your legacy.

Breaking free from traditional, antiquated imaging systems to rapidly evolve with a changing healthcare landscape.

Healthcare digitized. Then it stood still.

The film-to-digital transformation that began in the 1990s was one of the greatest shifts in healthcare. Walk through a radiology department today and you'll find very few film capture solutions still running — digital acquisition is the norm.

Meaningful Use, government-mandated EHR adoption, and the rise of IoT devices have all driven major gains in the digitization and efficiency of care. These advances changed radiology — and healthcare — forever.

Yet despite all that progress, healthcare still lags behind modern technology. Nowhere is that more evident than in today's legacy PACS solutions. Healthcare's greatest source of digitization can, in some cases, also be its greatest Achilles' heel.

Because healthcare doesn't face the strict requirements imposed on banking or insurance, much of its IT infrastructure is antiquated and vulnerable to cyberattack. This is the nightmare facing every CIO: old systems are expensive to maintain and create huge openings for breaches that can compromise patient data and cost millions in penalties.

Such attacks force infrastructure overhauls that take months — even years — to recover from. Yet many organizations hesitate to modernize, leaving themselves at continual risk.

THE STAKES

Cybersecurity breaches in hospitals rose close to 50% from February through May 2020 versus the prior year.

The threat is real — and most aren't ready.

A recent survey found that 73% of hospitals and physician organizations were not prepared to respond to cyberattacks — and the industry is expected to spend \$134 billion on cybersecurity between 2021 and 2026.

73%

of surveyed organizations not prepared to respond to cyberattacks

\$134B

expected healthcare cybersecurity spend, 2021–2026

40%

of hospital clinical staff receive no cybersecurity training

The proliferation of IoT devices, unpartitioned networks, insufficient access controls, and legacy systems are primary culprits that let cybercriminals compromise protected health information. Gaps in policy and procedure invite employee errors — improper handling and storage of patient files — that make organizations prime targets.

Many IoT devices, beneficial for patient management, lack proper security controls, making them easy to penetrate. Consider every connected device in a single hospital and the challenge of maintaining and updating them all becomes overwhelming.

Telehealth opens another door. As its use surged during the pandemic, IT departments had to ensure employees were trained against the tactics criminals use — and equipped with access controls to help inhibit a breach.

There are many ways cybercrime affects healthcare. The focus of this article is the one that underpins them all: legacy system modernization.

You're asking the wrong question about cost.

In IT, “legacy” means old, outdated, or hard-to-manage technology. Cybercrime is a leading reason to replace it — but cost weaves into every conversation, and most organizations frame it backwards.

Asking how much modernization costs is the wrong approach. The better question is what it costs to maintain your legacy solutions. You may be surprised: a five-year analysis of keeping an old system running can cost more than acquiring new technology.

Daniel Newman at Future of Work notes that large enterprises can spend as much as **80% of their annual budget** maintaining legacy IT systems. No wonder there's little left to upgrade when funds are continually diverted to upkeep.

But is that the right choice? All it takes is one breach, and the cost of not modernizing will far exceed the cost to upgrade — damaging your health system's credibility for years and risking the trust of physicians and patients.

You don't necessarily have to replace everything at once. Some hospitals run over 300 legacy applications behind the scenes even after moving to new EHRs — kept alive for data preservation, compliance, conversion challenges, and historical trending analysis.



Replacing legacy applications with systems based on new and different technologies is one of the IS professional's most significant challenges.

Gartner — IT Glossary, Definition of Legacy Application or System

What to evaluate before you modernize.

Reliance on legacy applications is the Achilles' heel of many organizations — often the very thing inhibiting a digital ROI. A fair analysis of your technology, with prioritized requirements, is the foundation of any modernization strategy.

When evaluating legacy systems

- Ongoing maintenance costs (hardware, software, upkeep)
- Cost of ongoing vendor support contracts
- Workflow improvements — or the cost of poor workflow
- System integration and interoperability
- End-user experience and the loss of customers or staff
- Missed opportunities to expand

Keeping old hardware degrades performance; support gets costly and, if too old, nearly impossible to fix. Newer software offers enhanced workflows, faster processing, AI capabilities, and improved efficiency — often delivering an ROI once paid for.

Questions to ask about your data

- What will you do with it in the future?
- Are you legally required to keep specific data?
- What systems must be migrated, and at what cost?
- What data is critical to benchmark and plan ahead?
- Can the data migrate into a new solution?
- What expertise will you need on staff — and do you have it?
- What does it cost to maintain expertise you no longer need?
- Do market drivers dictate what to update first?
- Do you need mobility or at-home capabilities?

System modernization is much like enterprise imaging — a continuous journey, not a one-time event. It evolves with your business strategy and needs.

Six factors that drive software modernization.

Focus on the business aspect of modernization, not just the technology. Consider IT alone and the impact won't deliver the results you hoped for.



Finances

There's a cost to modernization — and to maintaining legacy. Evaluate the true cost of old systems against the long-term gains of the new.



Security

Platforms on older operating systems or databases are at risk. Weigh the danger of keeping vulnerable solutions versus software built to withstand intrusion.



Integration

Does your legacy solution integrate to the enterprise and exchange information — or inhibit it? Is data proprietary, or stored in its native format?



Agility

Older solutions aren't as nimble. If you need a competitive edge, new workflows, or mobile support for cases like POCUS, flexible software is a strong reason to modernize.



Growth

Old systems make growth harder — difficult to adapt to modern standards, new web and mobile capabilities, or the cloud. Look for an adaptable framework built to expand.



The long view

Even the newest systems become legacy someday. Choose vendors whose development efforts target platforms that adapt easily to tomorrow's technology.

Is that old system really more secure?

Some things improve with age — good wine, heirloom jewelry, vintage automobiles. Technology is not one of them.

Older legacy systems are less secure than modern solutions. They can be the gateway that lets malware or ransomware compromise your health system — older operating systems, missing security patches, and aging hardware all become weak points. Microsoft and Apple ship patches weekly, sometimes daily, in a constant battle to stay ahead of attackers. Updating ancient code raises a harder question: who knows what else must change, and at what effort?

And consider the truly old system that may be “secure” only because it's offline: what good is data no one can reach across the enterprise? Does the cost to maintain it justify locking it away?

THE BETTER PATH

Migrate the data to a modern system and shut the old one down. You eliminate worries about data security, hardware failure, and system failure — the data stays intact for the whole organization to access and use — and you remove one more cost headache.

ADDING UP THE COSTS

Replacing 300+ legacy systems at once can be cost-prohibitive — data migration, conversion, reworked workflows, and implementation all add up. But a phased approach lets you modernize the enterprise while keeping costs reasonable.

The true costs of legacy systems — as Userlane's Tracey Ruff outlines: lack of performance and speed; lack of mobile capability; poor customer experience; negative employee impact and morale; damage to your brand; lack of scalability and lost revenue; and security threats, where antiquated PACS have given hackers a gateway that cost hospitals far more than replacement ever would.

Define your legacy by eliminating legacy systems.

As a leader in healthcare IT, you own the vision for where your organization goes. Defining the strategy — and the plan to navigate the journey — sets the stage for the cultural change your team must accomplish.

Writing in The New York Times, cybersecurity policy professor Dr. Josephine Wolff of Tufts identified why health systems fail at cybersecurity: inadequate resources; a lack of clear, effective guidelines; the large number of people and systems that need network access; and reliance on specialized equipment that must be compatible with more secure software — a slow, expensive process.

You have an opportunity to define your legacy by eliminating legacy systems and protecting patient data every day. Criminals will keep finding new ways in; you must set the culture and the path for modernization, and provide the training your teams need to stay vigilant.

What “PACS modernization” really means

Define your business needs before buying technology. PACS are a special breed — with few exceptions, every solution on the market has been in development since the technology first became viable, and most still rely on old foundational code. One PACS had millions of lines of code; adding features constantly broke it and took an army of developers to fix.

At its core, you face two options: departmental imaging you expand to the enterprise, or enterprise imaging you drive into the department. Without proper EHR integration, you limit what clinicians see of the complete patient record — raising study costs, patient risk from repeat studies, and constraints on care pathways.

Not all enterprise solutions are equal.

Healthcare has evolved, and so has imaging. Radiology images are no longer confined to the radiology department — they're used at the bedside and in consultation with experts across the country. Enterprise workflows differ fundamentally from departmental ones.

Traditional legacy PACS allow updates at the study level; modern enterprise solutions allow updates at the image level. When it's time to migrate or send data, synchronization at every level — including the images themselves — prevents errors and enables cleaner indexing.

Many call this a deconstructed PACS model; we prefer to think of it as a **restructured** PACS. Best-of-breed solutions that plug into a core enterprise platform offer the greatest flexibility, expandability, and long-term adoptability across workflow, features, and cost.

Simply updating to your PACS vendor's "enterprise solution" may not meet your needs. With the VNA as a critical part of any enterprise solution, those derived from a legacy PACS archive — as most VNAs are — may be built on the same legacy technology, limiting your future capabilities.

Radiology is in transition. Vendors who build flexible architectures and modern solutions are better prepared to adapt to the new workflows being created today and tomorrow.



Building best-of-breed solutions that plug into a core enterprise platform offers the greatest degree of flexibility, expandability, and long-term adoptability in terms of workflow, features, and costs.

Doug Rufer — BSBA, RT(R), Mach7 Technologies

It's time to modernize.

No one wants to be known for buying solutions that appease a few users today but leave you with little flexibility, inflated costs, and proprietary capabilities that are hard to escape. Choose a flexible, expandable, modern platform built on top industry standards — one that saves money and improves patient care.

Mach7's Enterprise Imaging Solution ensures your platform adapts as your needs change. Its viewing and platform solutions provide numerous security and privacy features:

01 Secure information transfer

SSL support, LDAP, HTTPS, TLS, and encryption protect data in motion.

02 Active-active clustered architecture

Data is shared across redundant application nodes. If one node fails, the remaining active nodes pick up the load and reassign transactions automatically.

03 Full logging and audit

Complete transaction logging and audits of all study processing, stored in the platform's SQL Server database with retention policies set at the organization level.

Deployed on customer-provided physical or virtual Microsoft Windows Server systems, Mach7 works with whatever antivirus and security features your IT department deems appropriate. We consider our solutions among the most IT-friendly available, and are always open to addressing your security concerns.

LET'S TALK

Leave a legacy worth remembering.

Making the leap to a more open, flexible enterprise imaging platform saves time and money — and the workflow improvements lead to better patient outcomes and happier physicians. That's a legacy you, and your organization, will be glad to leave.

TALK TO US

+1.802.861.7745 · mach7t.com · marketing@mach7t.com

FROM PIXEL TO POINT OF CARE.

CR21-018

References

Third-party figures and claims cited in this paper, with their original sources.

1. Hackett, Mallory. "Number of Cybersecurity Attacks Increase during COVID-19 Crisis." Healthcare Finance News, HIMSS Media, 4 June 2020, www.healthcarefinancenews.com/news/number-cybersecurity-attacks-increase-during-covid-19-crisis.
2. Help Net Security November 16. "Healthcare Organizations Are Sitting Ducks for Attacks and Breaches." Help Net Security, Help Net Security, 16 Nov. 2020, www.helpnetsecurity.com/2020/11/16/healthcare-attacks-breaches/.
3. Help Net Security April 25. "Legacy Infrastructures and Unmanaged Devices Top Security Risks in the Healthcare Industry." Help Net Security, Help Net Security, 25 Apr. 2019, www.helpnetsecurity.com/2019/04/25/healthcare-industry-security-risks/.
4. Newman, Daniel. "Is It Time to Update Your Legacy Systems?" Future of Work, BroadSuite Media Group, 18 Sept. 2017, fowmedia.com/time-update-legacy-systems/.
5. Matheson, Stephen. Retiring Legacy Applications: It's Not All About Cost, Health IT Outcomes, 10 May 2017, www.healthitoutcomes.com/doc/retiring-legacy-applications-it-s-not-all-about-cost-0001.
6. Gartner, Inc. "Definition of Legacy Application Or System - Gartner Information Technology Glossary." Gartner Glossary, Gartner, 2020, www.gartner.com/en/information-technology/glossary/legacy-application-or-system.
7. Singh, Jyot. "Legacy System Modernization: Your 101 Guide to a Successful Migration." RTS Labs, RTS Labs, 15 Sept. 2019, rtslabs.com/legacy-system-modernization-your-101-guide/.
8. Singh, Jyot. "Legacy System Modernization: Your 101 Guide to a Successful Migration." RTS Labs, RTS Labs, 15 Sept. 2019, rtslabs.com/legacy-system-modernization-your-101-guide/.
9. Kelker, Prashnant. "How to Deal with Legacy Systems, the Achilles' Heel of Digital Transformation." CIO, CIO, 29 Mar. 2018, www.cio.com/article/3267464/how-to-deal-with-legacy-systems-the-achilles-heel-of-digital-transformation.html.
10. Ruff, Tracey. "When Legacy Becomes Loss: The True Costs of Legacy Systems." Userlane Blog, 14 May 2020, blog.userlane.com/enterprise-legacy-systems/.
11. Drees, Jackie. "Viewpoint: Why Hospital Cybersecurity Strategies Fail." Becker's Hospital Review, Becker's Healthcare, 20 Oct. 2020, www.beckershospitalreview.com/cybersecurity/viewpoint-why-hospital-cybersecurity-strategies-fail.html.