

ARCHITECTURE

MUCH MORE
THAN I.T.

HEALTHCARE APPLICATION
PORTFOLIO MANAGEMENT &
DECOMISSINING:
DECREASE COSTS, INCREASE AGILITY

Author:

Justin Campbell

Vice President, Galen Healthcare

For more information visit www.galenhealthcare.com

©2020 Galen Healthcare Solutions. All Rights Reserved.

CONTENTS

- 1. Abstract3
- 2. Key Takeaways.....3
- 3. Downward Cost Pressures Exacerbated by COVID 19 Pandemic4
- 4. Healthcare Mergers & Acquisitions Create Complexity.....5
- 5. Application Portfolio Rationalization to Deliver Cost Reduction.....7
- 6. Legacy Data Management & Retention Strategy.....8
- 7. Inventory, Catalogue & Discovery.....9
- 8. Portfolio Analysis, Valuation & Application Retirement Prioritization.....11
- 9. Execution & Rationalization13
- 10. Application Decommissioning Enabled by Data Archiving14
- 11. What Must Be Archived?14
- 12. Have you Evaluated your Accessibility Needs?15
- 13. Do Not Forget the Metadata.....16
- 14. Cold Storage Approach16
- 15. Ongoing Application Portfolio Optimization.....17
- 16. Conclusion – Action is Needed to Stay Competitive18

ABSTRACT

Healthcare delivery continues to be a dynamic market. Agility, timeliness, and flexibility enable business value. Health systems that have made significant investments to their information technology infrastructure are finding they must upgrade their technology continuously. At the same time, they are experiencing downward cost pressures generated and intensified by COVID-19. Meanwhile, mergers and acquisitions continue to increase year after year sparking more healthcare IT portfolio rationalization and complicating efforts to retain certain data. In this context, application portfolio management and decommissioning is a necessary practice to ensure that IT is properly aligned with emerging initiatives and priorities; addition to portfolio costs must be counter measured to balance cost and value.

KEY TAKEAWAYS



Aged technology is one of the factors that impact the high cost of healthcare. Up to 70% of a health system's IT operating investment is attributed to the applications and infrastructure that support the environment.



Application decommissioning is critical to improving the financial posture of healthcare delivery organizations that has likely been significantly diminished by COVID-19; a simple effort of technology portfolio rationalization can reduce IT spend in any environment as much as 60% CAPEX and 30% OPEX.



Formulation of the risk profile of the application portfolio is linchpin to the initiative and ranks applications based on their functionality, type of information processed, and overall business value. The context of the risk assessment is to define a plan for consolidation, remediation, or elimination of the legacy applications.



Done right, application decommissioning can save your organization a lot of time and money that would have otherwise been spent managing legacy applications. Done wrong, you can face a lot of legal scrutiny and cybersecurity issues.

DOWNWARD COST PRESSURES EXACERBATED BY COVID-19 PANDEMIC

The dynamics of consolidation in healthcare have produced national health systems that span geography and settings of care. These changes have yielded many benefits. But not for all.

Rural hospitals, for example, were already struggling, and now, COVID-19 threatens to bring them to the breaking point. Over the last 10 years, more than 120 rural hospitals have ceased operations, and recent research from the Chartis Center for Rural Health found that more than 450 rural hospitals are vulnerable to closure. Those hospitals have survived by a heavy reliance on moneymakers such as elective surgeries, physical therapy, and lab tests to make their razor-thin margins work. But many of them still operate in the red. "If we're not able to address the short-term cash needs of rural hospitals, we're going to see hundreds of rural hospitals close before this crisis ends," warned Alan Morgan, the head of the National Rural Health Association, which represents 21,000 health care providers and hospitals. "This is not hyperbole."

During this pandemic, many healthcare delivery organizations have converted to large-scale COVID-19 screening, testing, and treatment. That has led to a sharp decrease in surgery / procedure volumes and significant portions of imaging and related historical services. For many healthcare delivery organizations, the anticipated 20%-40% drop in revenue cannot be absorbed when operating margins (2%-6%) and cash reserves are so thin. In sum, the added financial hit from the coronavirus outbreak could be the final straw for many rural hospitals and independent primary care practices.

To make matters even more taxing, many healthcare delivery organizations hastily adopted new infrastructure and telehealth technology to accommodate a remote workforce and e-Visits. This has caused further erosion of the bottom line.

HEALTHCARE MERGERS & ACQUISITIONS

CREATE COMPLEXITY

Even before the COVID-19 pandemic, the healthcare industry in the United States had been adapting to and weathering tidal waves of change that capsized and sank many of its oldest, bulkiest vessels. As healthcare costs continue to rise faster than inflation rates, as value-based models reward better outcomes and less spending, as care becomes more integrated from hospitals to home-based services, as the cost of drug development is spread throughout the distribution supply chain, and as technology expands to present new solutions and render recent improvements obsolete even before they are completely applied, staying afloat remains a continuous challenge.

It is no surprise, therefore, that every kind of healthcare enterprise has accepted partnerships, mergers, and acquisitions merely to survive. According to *Fortune*, deal-making in the healthcare sector reached \$583 billion in 2019, up 26% from the previous year. All this retrofitting has had to occur while continuing to increase access to care, reduce costs, improve care quality, and maintain staff satisfaction.

At the same time, however, most healthcare delivery organizations do not fully integrate operations and assets each time they make an addition to their information technology application portfolios. They assume that if their legacy systems are working, there is no need to fix them. And that can create problems: most IT applications serve well as temporary solutions, but they may not align perfectly with M&A strategies that were formulated for enterprise-level, business, and organizational objectives.

Instead, as soon as a merger or acquisition occurs, it is essential that a proactive application rationalization program be executed. Whether seller or buyer, healthcare organizations must first focus on simplifying their portfolios and the systems and personnel who support them. Unless they attend to this, they are liable to spend more, sacrifice efficiencies, and neglect the most important matters – legal and regulatory issues, systems and process integration, and business continuity.

Most US health systems maintain an IT portfolio that supports redundant functions across the enterprise. In a consolidation environment where M&A activity is increasing, this can result in costs of \$70,000-\$100,000 per bed to integrate disparate clinical and business systems. A simple effort of technology portfolio rationalization can reduce IT spend in any environment as much as 60% CAPEX and 30% OPEX.

APPLICATION PORTFOLIO RATIONALIZATION TO DELIVER COST REDUCTION

With the continuing development of healthcare information technology applications, complicated by the presence of COVID-19, it is of vital importance for healthcare IT leaders to prioritize application portfolio rationalization as a strategic initiative. At many healthcare delivery organizations, the application portfolio exerts significant drag on overall operational effectiveness while the inflexibility of legacy applications makes it difficult to provide the IT functionality demanded by rapid shifts in business needs. An effective application portfolio management initiative is essential for effectively rationalizing the IT landscape, cutting costs, scaling up to support growth, and boosting agility.

As important as it is to monitor pure costs, you should also keep in mind the risks of a burgeoning application portfolio:

- Application failure
- Application obsolescence
- Data access restrictions
- Compliance breach

To reduce operational spend and complexity, the application portfolio can be rationalized through a set of application cost, count, and risk reduction activities:

- **Reduce costs:** Eliminate licensing, development, support, and infrastructure costs of legacy applications.
- **Retire technical debt:** Migrate from on-prem platforms to take a cloud-first approach, and remove support software versions, legacy architecture patterns, & legacy hardware.
- **Eliminate functional redundancy:** Remove fragmentation, functional overlap, and superfluous integration.
- **Reduce risk:** Focus on and act to enhance high availability, security, scalability, and compliance.

The last bullet (above) is of the greatest importance when deploying data governance to achieve application portfolio rationalization. Applications on aging technology that have outlived support are significantly more vulnerable to cyber security threats. This is no surprise since many legacy systems are forgotten and therefore do not receive the latest updates, patches, and anti-virus remedies to ensure security. Furthermore, legacy systems typically do not have active users who can identify abnormal behavior. According to the HIMSS 2019 Cybersecurity Survey and KLAS, 90% of hospitals are keeping old applications running to preserve data when an application is replaced or retired, causing 75% of hospital IT staff time to be consumed by legacy systems that cost more in annual licensing than hospitals pay in IT staff wages. In addition, the security of these legacy systems has been continuously compromised: (4.3 million health records affected in 2017; 90% of hospitals affected since 2016).

LEGACY DATA MANAGEMENT & RETENTION STRATEGY

Data governance is the bedrock of successful application portfolio rationalization, particularly for legacy data management and retention. Issues to address include:

- What information should be retained?
- How long does the information need to be retained?
- What format should be used to retain the information?
- When can the information be destroyed?
- Which applications will qualify for inclusion?
- Is information is still actively used?
- How frequently must information be accessed?
- Will the information need to be modified or updated?
- Who will need access to the archived information?

Chief among the considerations are organizational and legal retention requirements. Healthcare delivery organizations are required to retain data from two years to twenty-five years after the last date of service to a patient. That period can be slightly different when the patient is a minor, as retention requirements are typically the longer of a stated period, or until the patient turns 18 (or 21 in some instances). Here is an example of one organization's retention requirements:

- 7 years for adult medical records
- 10 years for Medicare records
- 21 years for pediatric records
- 25 years for newborns and OB records

INVENTORY, CATALOGUE & DISCOVERY



We have approximately 175 applications that we run. When I first came in about a year ago, there was no true inventory of those applications. We used a number of avenues to figure out exactly how many we actually had. It was sort of an unknown, but I certainly knew there were quite a few of them.

A lot of our application portfolio should be tracked in a system once it is implemented rather than keeping it in a spreadsheet. We've been working on adopting ITIL best practices and implementing an ITSM system to track the portfolio. We're hoping for some great things as far as doing a better job of keeping track of our applications, providing better customer service, and improved change management."

Susan Carman, Former CIO, United Health Services

An application inventory is vital for the management of a healthcare delivery organization's information assets. It will also provide insights that will be helpful for application inventory portfolio management and decision-making.

From the application inventory, data storage and legal compliance issues can be identified, as well as opportunities to save money and reduce technology footprint by sunsetting or combining systems.

While there is no single best practice for conducting an application inventory, at the very least, an inventory should capture the following information about each enterprise application:

Application Demographic	Operation	Technology Platform
Name	Availability requirements	Software
Description	Release cycle	Database
Version	Service desk ticket count	Hardware technology
IT Owner	IT governance	Distributed computing & services
Business Owner		
Usage/Integration	Data	Financial
Integration points	Information type(s)	Contract (sign date, term)
Number of Users	Data security (public, internal confidential)	Annual costs (software maintenance, storage, operating and support)
Business process(es) supported	Archiving and backup protocols	
Function		
Capabilities (document management, AP, AR, RCM)		

PORTFOLIO ANALYSIS, VALUATION & APPLICATION RETIREMENT PRIORITIZATION

Depending on organizational needs, application evaluation can be straightforward or intricate. For some organizations, a simple review of the application portfolio to ensure support of mission objectives and capture application operational costs will suffice, allowing for identification of those applications that should not be decommissioned. However, in most cases, a more rigorous evaluation will be necessary, assessing each application in the portfolio.

As part of an initial analysis, the applications should be evaluated for functional fit, that is, the level of support required for business capabilities or processes, and technical fit, the degree to which applications match the organization's technical standards. Deeper assessment will include application analysis for the following categories:

- **Strategic value:** Does the application support the business strategy?
- **Available skills:** Does the organization possess institutional knowledge to best utilize the application?
- **User satisfaction:** To what degree are users satisfied with the application's usability and benefits?
- **Availability of alternatives:** Are there better alternatives, either through existing, redundant applications or modules, or commercial off-the-shelf solutions?
- **Total cost of ownership:** What is the sum of all costs associated with the application?
- **Architecture strategy conformance:** How is the application conforming to the organization's strategic and operational technology roadmaps (e.g., standard technologies, cloud-first strategy)?
- **Security risks:** Does the application pose any security risks due to its architecture?
- **Documentation and training:** How robust are the available documents and training materials?



The conversation for legacy system retirement begins with business leaders, with cross-sectional representation from stakeholders including research, compliance, regulatory, risk, etc., to understand needs and requirements. This requires an exercise in examining vendor contracts and understanding vendor relationships and partnerships. From there, an analysis is performed to identify which applications are at the most risk, specifically producing a risk profile for application groups. Assessment of security was an important part of evaluating risk, not just technology, but also the human behavioral aspect.”

Suma Gaddam, Former Senior Vice President and Chief Information Officer, Care New England

To understand the risk profile of the application portfolio, a risk framework should be developed to rank applications based on their functionality, type of information processed and overall business value. The context of the risk assessment is to define a plan for consolidation, remediation, or elimination of the legacy applications. Categorization of applications depends on the criteria specified in the risk framework. Identification and prioritization of high-risk applications must be based on total cost of ownership and potential savings, and, of even greater importance, business impact, security threats, compliance requirements, and overall operational risk. Prioritize applications for decommissioning based on the following key drivers:

- Usage
- Cost
- Functional overlap
- Compliance risk
- Operational risk
- Security risk
- Business benefits
- IT portfolio sustainability
- Strategic value
- Institutional knowledge
- Documentation and training
- Accessibility

EDGI ;D AD6EE A86I D CH8D G:8 6G9

EXECUTION & RATIONALIZATION

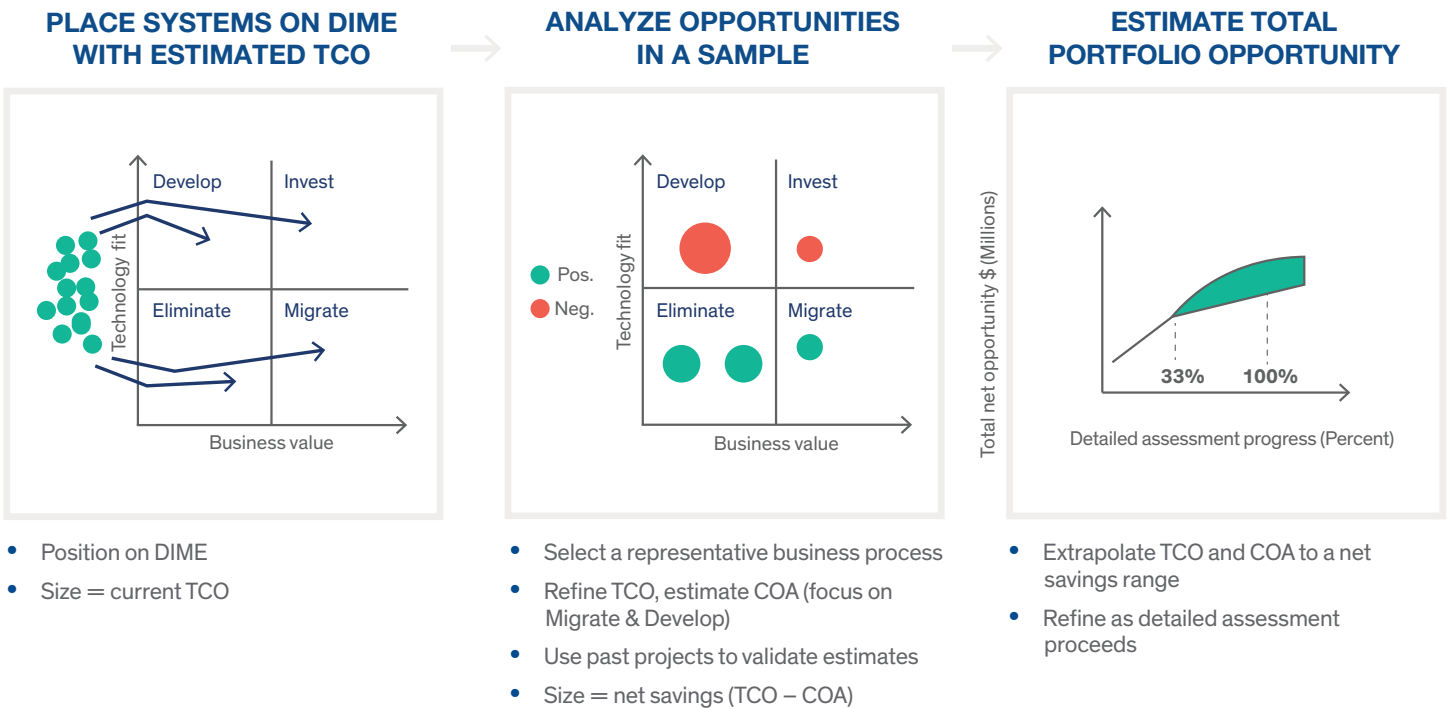
After the portfolio has been inventoried, assessed, and scored, categorization of the portfolio is applied to sort the applications and determine action that should be taken. Popular formats use the 2x2, 4 quadrant matrix. An example is **DIME** (Develop, Invest, Migrate, Eliminate):

Develop – continue hardware & software investment, focus on system development for new business processes.

Invest – increase software & hardware investment, push for more business processes to use the system.

Migrate – schedule system for upgrade or migration to stronger system, evaluate business process for standardization.

Eliminate – schedule system for deactivation, cancel contracts, decommission hardware.



Once applications were prioritized, we developed a queue for decommissioning and quantified ROI by determining what was being paid in SMA, and what we were investing in institutionally to support the application. In our case, we lacked institutional knowledge for some applications and were spending money on consultants to fill those gaps.”

Suma Gaddam, Former Senior Vice President and Chief Information Officer, Care New England

Once the applications have been categorized, candidates for decommissioning can be identified. Using the catalogued attributes such as contract term, early termination penalties, and decommissioning costs, a total cost of ownership (TCO) can be formulated to quantify the long term financial benefit and return on investment (ROI) of a data migration or a data archiving solution.

It is important to keep in mind that decommissioning of applications can come with its own risk as well. Typically, these fall into two categories:

- **“No Risk”**: Software or service that references only data stored elsewhere, and that does not save any unique data itself.
- **“Some Risk”**: Solution generating unique data that is not stored anywhere else, or is duplicated in a non-comprehensive manner in a separate solution.

As such, when decommissioning systems, careful attention and consideration must be given to determine the risk of:

- Loss of comprehensive data sets
- Loss of audit trails from systems
- Loss of versioning information
- Data reconciliation (nomenclatures, dictionaries, ontologies)

APPLICATION DECOMMISSIONING ENABLED BY DATA ARCHIVING

A result of the application portfolio rationalization process will be the identification of those applications that qualify for decommission. Many systems will need to be decommissioned, yet much of the data residing in those decommissioned systems must be maintained and retrievable. The data that must be accessed is often sought by various departments (clinical, financial, administrative), each with its own set of needs and functional requirements for the post-production data lifecycle. The challenge for each organization is therefore to employ a records management strategy that concurrently ensures accessibility, security, and legal compliance.

An organization's capacity to preserve the integrity and completeness of the original record, especially the ability to recreate a copy of the record as it existed at the relevant time in question, is vulnerable to compromise when legacy systems are decommissioned, and legacy data is archived.

In addition, beyond the legacy system security risk, many data archiving platforms may also be a security risk if they are not managed as a true production application. We have all seen times where the data is archived to an old server, or even a desktop computer as a bunch of PDFs. Is there a worse security risk? Archiving data to an effective, secure data library that's treated as a production application is key to cybersecurity efforts.

WHAT MUST BE ARCHIVED?

According to AHIMA Fundamentals of the Legal Health Record and Designated Record Set, any information that may have been used to make a clinical decision at a particular point in time, as well as any information that shows what and how care was delivered, must be maintained when decommissioning legacy systems.

The “Legal Medical Record” includes data supporting clinical decision making and data documenting care that was delivered, and must be archived. The “Designated Record Set,” which includes data not directly related to patient care, might also need to be archived.

HAVE YOU EVALUATED YOUR ACCESSIBILITY NEEDS?

Most people do a good job evaluating how accessible their retired IT system's data needs to be from a clinical and business perspective. If clinical and business continuity is needed, the data is often loaded directly into the go-forward system or is made easily accessible to the end user through a simple web interface. If clinical or business continuity is not needed, then other options such as cold storage, or even static exports of all the data, can be used for legacy data storage. However, this approach is fraught with exposure to risk given potential compromise to the fidelity and accessibility of the legacy data.

While accessibility may not be pertinent from a clinical perspective, archived data accessibility from the perspective of the entire organization must be evaluated. For example, when an ROI request comes to HIM from a patient, ask, "Is the data accessible so this ROI request can be appropriately fulfilled? Does it need to be? How about a legal request as part of e-Discovery in a legal case? Could this data be retrieved quickly enough to meet the legal requirements (including allotted time frames)?" Depending on your answers to these questions, cold storage or other static exports may or may not be fine. The key is to ensure the chosen archive approach matches your accessibility needs.

Among the considerations that will dictate which archiving approach should be pursued are:

- **Data Fidelity:** How complete the data set is relative to the original data source. Clinical continuity often requires a subset of compliance and legal data sets. Transformation and mapping reduce data fidelity.
- **Accessibility (Clinical):** How easily can a clinician access archived information to facilitate care delivery or other clinical tasks? This includes operations such as finding a particular record, as well as drilling down and filtering data within that record. It also encompasses how closely the data is visualized relative to what a clinician expects.
- **Accessibility (Compliance):** Can a compliance officer or legal team member analyze data pertaining to audit trails, change history, or clinical data so internal or external requests for records, in the requested format, are sufficient? This can be especially critical during e-Discovery.

DO NOT FORGET THE METADATA

Successful healthcare data archiving with minimal risk requires preservation of the legal medical record (as defined by the organization), data sets such as contextual audit trails, referenced data in ancillary systems, data change and version history, and even database metadata. A navigable audit trail is essential to relate the precise sequence of events; this trail provides evidence that justifies and/or explains what actions have occurred.

The most common and vital metadata item forgotten in data archiving is the audit log. Avoid this pitfall by ensuring your data archiving efforts include the appropriate metadata.

COLD STORAGE APPROACH

Simple cold-storage solutions can be deployed when cases of data access are narrow in scope and frequency, that is, where it is simply held for compliance and regulatory requirements. The data is held in an offline database, in a read-only state. However, simple data visualization requires SQL query or another tool.

The greatest benefit to this approach is that access to the data via underlying data stores is almost always easily found in built-in backup mechanisms. Indeed, the ability to back up data is a certification requirement for EMRs, as well as a HIPAA and HITECH legal requirement. This strategy also offers “perfect” data fidelity, as the data is in the raw, original format.

However, once it is time to access the “archived” data, the organization is forced to fully reverse engineer the underlying database schemas and file system encodings. This leads to mammoth costs and protracted timelines for even simple data visualization, and it is a major undertaking to offer direct data access to clinicians or for compliance.

Another danger with raw database backups is that many clinical system vendors have language in their licensing related to the “reverse engineering” of their products. So while it may be “your” data, the vendor may consider their schema intellectual property — and the act of deciphering it, not to mention keeping a copy of it after the licensing agreements with the system vendor have been terminated — may well be a direct violation of the original licensing agreement.

The manner in which a data archiving system organizes data from primary and ancillary clinical systems, and how relationships between these systems and the primary EMR system are preserved, is critical not solely for the purposes of medical continuity, but also for business continuity. A comprehensive archiving solution organizes data from both primary and ancillary clinical systems and presents it in ways that emulate the original systems’ documentation workflow.



We had 50 applications in the portfolio that qualified for retirement and were able to drastically reduce the timeline to six months by having buy-in and discipline within the organization. We didn’t have bench strength, so we relied on consulting for data extraction and implementation of an archiving solution. As part of our process, our team took on data validation and end user acceptance. In some cases, there were certainly challenges in getting access to the data, and outside partners were used if we could not rely on the vendor. In addition, there were instances where we lacked institutional knowledge for the application, and a cold storage approach made more sense than archiving the data. In those cases, the likelihood of needing access was low, and if access was required, we were comfortable with taking on the risk that we would need to learn how to get at the data.”

Suma Gaddam, Former Senior Vice President and Chief Information Officer, Care New England

ONGOING APPLICATION PORTFOLIO OPTIMIZATION

Above and beyond a one-time portfolio rationalization exercise, it is imperative for healthcare IT leadership to prioritize Application Portfolio Optimization (APO), a strategic initiative to adjust to a changing application landscape and its continued downward cost pressures. More than a one-time portfolio rationalization exercise, APO will foster an application governance framework that will serve as a formal mechanism to support organizational goals consistent with existing IT architecture, aligned with primary business, and sensitive to lower operating and support costs. Unlike a one-time review, ongoing governance prevents the “patchwork problem” from recurring, and pays dividends for years to come.

This ongoing activity can inform an organization’s transformation with guidance for investment in technology that is effective and sustainable. Current healthcare technology spending models can allocate up to 90% of their non-labor costs to maintaining and supporting systems of record (e.g., EHRs, enterprise resource planning, revenue cycle management, and more). These models must evolve to allow strategic growth in consumer-facing areas (e.g., mobile, voice, chatbot, and virtual reality).

An effective system-of-record investment that supports consumer-centric digitization can be managed with approximately 65% of non-labor costs. To support that systems-of-record investment goal, organizations must adopt an overall buy-versus-build strategy based on strategic partnerships which place responsibility on those partners to decipher system integration and devise an investment strategy based on fewer, but fully integrated, systems-of-record.



This initiative was executed in an environment where we didn't have a static set of applications, and as such, at some point, the initiative becomes operationalized so that there is an enterprise approach and rigor applied for acquisition of new applications to the portfolio – a true application lifecycle, end-to-end approach. Again, security plays a big part of that assessment, and due diligence with regard to application security is required when acquiring a new application.”

Suma Gaddam, Former Senior Vice President and Chief Information Officer, Care New England

CONCLUSION

ACTION IS NEEDED TO STAY COMPETITIVE

Health systems that have made significant investments to their information technology infrastructure are finding they must upgrade their technology continuously. At the same time, they are experiencing downward cost pressures generated and intensified by COVID-19. Meanwhile, mergers and acquisitions continue to increase year after year sparking more healthcare IT portfolio rationalization and complicating efforts to retain certain data.

It is undeniable, however, that we are experiencing information technology portfolio bloat which threatens healthcare delivery organizations by diminishing their agility. A recent report from Forrester observes, “If you don’t know what you have, it’s difficult to know how much it costs and decide whether to keep it.” As complexity in healthcare IT continues to increase, costs rise with it. Responsiveness and speed lag. And, security breaches are becoming daily events.

But there are steps CIOs can take to mitigate the effects of these trends and permit HCOs to regain and maintain a healthy financial posture as we rebound from the virus.

What should be done right away?

- Get started now
- Examine your portfolio
- Address overlapping and duplicative applications to improve your organization’s financial posture

As John Lynn, chief editor and founder of Healthcare Scene observed about application decommissioning: “Done right, it can save your organization a lot of time and money that would have otherwise been spent managing legacy applications. Done wrong, you can face a lot of legal scrutiny and cybersecurity issues. No one wants either of those, so take the time to make sure you have a well thought out process and don’t be afraid to ask someone for help who’s been down this road before.”

The collective knowledge we have built over the past decade in implementation, optimization, data migration, and data archiving projects lend itself well to application portfolio management. Leveraging that knowledge, Galen has assisted health systems to improve IT responsiveness, reduce costs, and increase security using a unique, field-tested approach of application portfolio management.

PARTNERING FOR A SUCCESSFUL FUTURE

Change inside the healthcare information technology portfolio of any healthcare organization can be volatile. At Galen, we partner with our clients to help them navigate their technology transformation initiatives, helping them understand where they are and how to get to where they want to go. We provide thought leadership and experience to help our clients understand the current state, define their vision for the future, execute the plan, and measure success.

System decommissioning prompts you to identify which applications are critical in both short and longer-term plans. Galen will provide the structure and guidance you need to successfully execute a vision for a right-sized technology footprint, ensuring that application, infrastructure, and data ecosystems are aligned.

Galen helps our clients measure their success by identifying the business drivers that define successful outcomes, then using those business drivers and key success metrics to measure success each step of the way. In short, Galen gives executives the clarity they must have to measure progress towards the goal.

VISIBILITY. STRATEGY. RETURNS.



MEASURE AND COMMUNICATE SUCCESS

