

WHITEPAPER

Legacy Applications: A Healthcare Cybersecurity Nightmare

In healthcare, vulnerable legacy applications have far reaching implications in terms of cybersecurity. But, what are the clinical, operational, financial and governance risks? And how can healthcare providers mitigate those risks?

Dr Saif F Abed - Founding Partner,
AbedGraham Healthcare Strategies

Gareth Griffiths - Chief Technology Officer,
BridgeHead Software



Executive Summary

Over the past two years, cyber-attacks on healthcare providers and insurers across the world, such as the WannaCry ransomware attack, have highlighted how quickly patient safety can become compromised when technology is the weak link. Although digital transformation initiatives are empowering greater patient engagement through the rise of the Internet of Things (IoT) and cloud computing, they also contribute to an increasing threat surface area for potential cyber-attacks. Increasing network connectivity and 'networks of networks' can create weak points in legacy applications providing a 'back door' for cyber criminals to exploit, threatening individual organizations or even entire health systems.

This white paper will explore how a well-considered, cybersecurity focused, application retirement strategy generates clinical, organizational, financial and governance benefits for healthcare organizations to better protect care settings. By prioritizing the retirement of applications, the provision of safe and efficient clinical workflows can be delivered at scale.

Why and How are Legacy Applications a Cybersecurity Threat?

Across healthcare, it is becoming commonplace for hospitals to continue running legacy applications to preserve historical data that is not migrated to newer, more secure solutions. The driving forces involved can be human or financial resource constraint or simple unfamiliarity with new technologies now available to deal with legacy data. The requirement to manage the entire clinical application ecosystem, in order to minimize exposure to vulnerabilities, is more urgent than ever as healthcare providers have become top targets for unscrupulous cyber-criminals.

Any hospital continuing to use legacy applications in their organization is simply inviting risk. The more these vulnerable systems remain in play, the wider the threat surface area becomes. Given the strategic shift towards interoperability across multiple, diverse care settings, the impact from cyber-attacks on so many vulnerable systems is considerable. Infection can rapidly spread throughout a hospital, and even across health systems, affecting mission critical clinical applications, with potentially catastrophic implications.

In the course of one day, WannaCry had spread across the globe, infecting more than 230,000 computer systems in 150 countries and is estimated to have cost approximately \$4 billion in financial losses.

What is HealthStore™?

BridgeHead's HealthStore™ is a modern, secure repository for clinical, financial and business data that enables hospitals to consolidate, store, protect, and share any record, document, file or image from any healthcare application.

HealthStore decouples and ingests data from the originating applications providing users access to that information from user-specific viewing interfaces (usually


based on their function and workflow). By allowing HealthStore to store patient information separately from the applications that created it, from a security perspective, healthcare organizations can more effectively isolate and protect this valuable patient information from cyber-attacks. Further, HealthStore provides a less costly, more efficient and more convenient way for hospitals to update or decommission their legacy applications. By removing these sources of risk and, thereby, reducing the spread of threats coming from these potentially vulnerable systems, hospitals can better secure their networks. HealthStore can act as an extension to the Electronic Health Record (EHR) by providing access to this valuable clinical, operational and financial information directly through its web interface, HealthStore Web Access (HWA), or through a simple integration link with a provider's primary applications, such as EHRs, integration engines or portals. This helps hospitals achieve data interoperability, safely and securely.

How does HealthStore Affect Patient Safety?

By using HealthStore, hospitals are better equipped to retire legacy applications sooner, limiting opportunities for attackers to find and exploit vulnerabilities in these systems. This, in turn, significantly reduces the risk of threats being spread to other applications involved in delivering quality healthcare to patients. The impact of malware and ransomware infecting core healthcare systems, such as Electronic Health Records (EHRs), Picture Archiving and Communication Systems (PACS), and Laboratory Information Systems; results in patient information not being accessible to treatment providers, as and where they need it, at the point of care, which creates havoc across the organization and significantly compromises patient safety.

HealthStore provides a range of security features, including encryption, roles-based access control and an inbuilt self-protection capability. Consequently, in the event that a critical clinical application is compromised, the independent patient information stored in HealthStore is still accessible to clinicians and support staff, as and where required.

By maintaining the availability of the full patient history across the enterprise, at all hours, and facilitating the continuation of smooth clinical workflows, HealthStore



reinforces clinical service resiliency. This enables medical teams to continue making accurate assessments and well-informed decisions, as well as reducing delays and errors that often impact patients following cyber-attacks, by providing access to crucial clinical details that would otherwise be trapped in compromised applications. As a result, staff benefit from a consistent and optimized clinical end-user experience, with a secure repository of patient information at their fingertips.

The effective preservation of clinical workflows avoids the disastrous impact that a cyber-attack can have on patient care. The separation of clinical information from applications that create it and the storage on which it resides is central to securing the digital ecosystem in healthcare. In acute care settings, the results of basic investigations are vital in dictating whether a patient will be admitted or returned to the community for non-urgent follow up. They can also determine whether clinicians are able to interpret the context of any patient symptomatology, such as differentiating between an acute infection or something more sinister. These scenarios have such variable outcomes and care pathways that clinicians rely on accessing information that is readily available, wherever and whenever they need to. HealthStore's capabilities help establish this.

How does HealthStore Secure Operational Efficiencies?

Hospitals, globally, face unrelenting pressures to optimize efficiency and 'do more with less' as demand on services continues to increase. An organization's ability to meet its strategic targets, ranging from: achieving efficiency goals and financial milestones, through to avoiding breaching national regulations; needs to be underpinned by a robust cybersecurity strategy. However, since the 2017 WannaCry cyber-attack, it has been established that meeting operational targets following system outages can be significantly hampered not only through the reduction of patient flow across acute settings (with increased treatment times and delayed discharges), but also through the cancellation of outpatient appointments and elective surgical lists. In a commercial context, this would be profoundly negative from a revenue management perspective.

HealthStore's ability to manage and safeguard patient information independent to clinical applications means that hospitals can preserve access to mission critical

data in the event of a cyber-attack, thereby optimizing the recovery of critical 24/7-services. Essentially, deploying a centralized, independent clinical repository puts CIOs and CMIOs in a more advantageous position to confidently retire legacy applications and improve network security. This reduces the risks of incurring operational costs associated with devastating cyber-attacks, such as switching to inefficient and costly business contingency plans and diverting patients to neighboring organizations.

As hospitals continue to optimize their clinical and operational productivity, maintaining smooth and uninterrupted information workflows is critical. Investments in solutions that safeguard access to clinical systems, whilst addressing cybersecurity concerns, should be a priority. As such, continuing to run legacy applications is a major barrier to achieving a productive and secure environment. This is especially true given the possibility of threats spreading to cause interruption to services across entire regional healthcare systems and beyond (depending on integrations with other facilities).

Lastly, continuing to run legacy applications wastes valuable IT resources, including server room space and power, as well as the IT staff resources dedicated to overseeing these systems and the day-to-day management tasks, such as standard checks and general upkeep. In addition, end-users and administrators alike, need to maintain their skills and training for these applications. All of these could be reduced or, in some cases, eradicated, with an appropriate application retirement strategy.

How does HealthStore Maintain Financial Integrity?

Due to the challenges of healthcare organizations responding to and recovering from a cyber-attack, the financial impact of failing to manage cybersecurity threats appropriately can be disastrous. The loss of revenue that occurs from being unable to admit, triage and manage new and existing patients when added to the costs of responding and recovering from an attack can be profound.

Furthermore, there are also specific costs that only emerge in the aftermath of an attack to consider, such as settling regulatory fines as a result of cybersecurity failures [e.g. HIPAA] and lawsuits that may be levied by patients based on adverse effects on their care.

As mentioned already, the impact of a successful cyber-attack does not stop once the immediate threat has been managed, with recovery taking many more months to address. If there were not enough resources to deal with legacy applications in the first place (where their continued use was the source of vulnerability for the attack), given the financial pressures covered above, hospitals will find themselves in awkward positions with difficult decisions to make. By securing patient information in an independent repository, like HealthStore, hospitals can prevent prospective losses by being more resilient to attacks and are able to continue providing services during a crisis, whilst simultaneously reducing the time and resources required for disaster recovery. If a repeated attack does occur, these associated costs are minimized through the safeguarding and isolation of patient information away from the source applications, which also enables the prompt recovery and delivery of service.

Lastly, there are significant costs attributed to the continual running of legacy applications. There are the associated software licensing fees, maintenance costs, supports costs (should the systems continue to be supported by the vendor), as well as the operational costs we discussed in the previous section; all of which could be minimized or removed entirely by decommissioning these legacy systems.

How does HealthStore Ensure Risk & Governance Compliance?

The regulatory fines associated with data protection and cybersecurity in healthcare signals the gravity at which overseeing bodies are paying attention to this issue. In the US, for example, this is best represented by HIPAA and its associated fines. At a more global level, significant fines are being issued when critical failures occur due to major incidents, such as recently in Singapore when millions of patient records were compromised as part of a coordinated attack to steal the Prime Minister's clinical information. This is an accelerating trend that is also being seen with new legislation in Europe, with major fines being associated with cyber failures in critical sectors like healthcare.

Hospitals continue to struggle with the ongoing use and maintenance of legacy applications despite knowing that they present extreme sources of vulnerability. HealthStore helps to demonstrate to both regulators and internal hospital leadership that an organization is addressing

cybersecurity proactively by tackling issues such as service resiliency, business continuity and disaster recovery, which are key pillars for clinical care and financial integrity.

90% of hospitals keep old applications running to preserve data when an application is replaced or retired. In addition, 8% admitted they never migrate data to a new application; and 8% never extract the data into an archive.¹

How can you Plan an Application Retirement Programme?

Despite the acknowledgement that legacy applications leave healthcare organizations vulnerable to cyber threats, hospitals often face challenges in planning how to extract and where to migrate the relevant patient information, whilst having limited access to resources to retire and replace them. HealthStore takes away much of the headache associated with this.

Having assessed the level of vulnerability that outdated applications present via a graded risk approach, and having balanced this with stakeholder demand for the associated patient information (together with its operational value), the relevant patient information can be migrated, consolidated and protected in HealthStore. This provides peace of mind that patient information is secure, available and accessible to the entire organization and can be held there and presented to whichever application requires it, if not accessed directly. When resources eventually become available, the relevant applications can be retired accordingly. Due to the open standards-based approach taken by BridgeHead Software, the patient information residing in HealthStore can be readily presented to the new, secure applications, when the hospital deems it appropriate.

¹ 'How Do You Manage Legacy Systems?'
BridgeHead Software Online Survey, Jan 2017



Summary & Conclusion

Though the global drive towards digital transformation in healthcare continues, the continued use of legacy applications within hospitals still presents substantial risks to core ambitions, such as achieving interoperability, value-based care and integrated care between healthcare organizations.

While current attention may be evolving beyond optimizing current investments, such as EHRs, to addressing emerging areas including IoT, cloud computing and population health management, the pivotal role that a central software repository can have in supporting the security of the data that these systems depend on should not be overlooked.

It is important to remember that all applications will eventually become outdated and increasingly less secure as time goes on. Unless a robust application retirement strategy is present, any application that a hospital procures will ultimately become a source of future vulnerability waiting to be exploited. This, in turn, could result in the spread of threats to multiple systems and settings at scale, with potentially very serious consequences.

HealthStore offers robust safeguarding capabilities that enable hospitals to securely manage patient information. By providing increased resilience to cyber-attack (due to its ability to isolate and protect patient data away from compromised applications), and maintaining digital working from any clinical setting, across the ecosystem, at all hours, HealthStore delivers peace of mind to healthcare providers that patient information remains secure while applications are waiting to be retired. Further, as patient information is no longer locked into these legacy systems, organizations have more flexibility and a wider choice of application vendors to choose from, allowing a quicker transition to newer solutions.

With HealthStore, healthcare organizations can protect patient safety and secure financial integrity with a cost-effective solution, while assuring hospital leadership that they are responding to the demands of an increasingly complex and regulated environment.

About The Authors



Dr Saif F Abed

Founding Partner,
AbedGraham Healthcare
Strategies

Dr Abed is a medical doctor and healthcare cybersecurity/national security expert. He is a recognized subject matter expert within all sub-sectors of healthcare IT with a primary field of specialization in cyber-warfare and crime targeting public sector healthcare systems.

He is a Founding Partner and Director of Cybersecurity Services at AbedGraham, Europe's leading exclusively clinically-based strategy consultancy providing public policy, business development and project management services for a range of large health IT, cybersecurity companies and government agencies in European public sector healthcare markets, including Microsoft, IBM, Dell, VMware, Citrix, BridgeHead Software, Nuance Communications and Imprivata.

Dr Abed is regular speaker and contributor to a range of organizations, including Business Insider, HIMSS, Forbes Middle East, the BBC, HITConsultant Media and the Irish Government.

He is a multiple international award winning and published researcher in the field of oculoplastic surgery whilst a trainee at St. George's Hospital Medical School, London.



Gareth Griffiths

Chief Technology Officer,
BridgeHead Software

Gareth has worked with systems design, product management, and leading software development teams for more than 30 years. As a founding member of BridgeHead Software, Gareth is responsible for the development and technology plan for all of BridgeHead's products and solutions.

He previously led VMS technical development groups at Raxco-UIS and was technical director for software at MTI and, subsequently, at MultiStream. Gareth has kept what is now the BridgeHead core development team together through several company mergers and acquisitions. He was instrumental in the management buyout that allowed BridgeHead to acquire and grow the development group and the technology portfolio that is the basis of the company's business today.

Gareth holds a BA [Hons] in Mathematics from Oxford University.

With over 25 years' experience in data and storage management, BridgeHead Software is trusted by over 1,200 hospitals worldwide.

Today, BridgeHead Software helps healthcare facilities overcome challenges stemming from rising data volumes and increasing storage costs while delivering peace of mind around how to **STORE**, **PROTECT** and **SHARE** clinical and administrative information.

BridgeHead's Healthcare Data Management [HDM] solutions are designed to work with any hospital's chosen applications and storage hardware, regardless of vendor, providing greater choice, flexibility and control over the way data is managed, now and in the future.

For more information on how BridgeHead Software can help lower the cost and administrative burden of managing your healthcare data, email us at: info@bridgeheadsoftware.com or visit: bridgeheadsoftware.com



UK

BridgeHead Software Ltd.
BridgeHead House
215 Barnett Wood Lane
Ashted, Surrey, KT21 2DF

+44 [0] 1372 221950
+44 [0] 1372 221977 fax

USA

BridgeHead Software, Inc.
400 West Cummings Park
Suite 6050
Woburn, MA 01801

+1 781 939 0780
+1 781 939 5607 fax

Follow BridgeHead on Twitter at:
www.twitter.com/BridgeHeadHDM

