# Active Archiving:

# A Smart Security Move to Protect Legacy Medical & Business Records

White Paper

harmony HEALTHCARE IT®

www.harmonyhit.com

# Healthcare providers battle to protect health information from breach by cyber criminals

**Americans Affected by Health Data Breaches, Increased by 65%**

**Legacy IT Systems Pose a Significant Security Challenge**

**TWO THIRDS OF HEALTHCARE ORGANIZATIONS SUFFER A CYBERSECURITY INCIDENT**

**Rise of Cyberattacks & Data Breaches Linked to Uptick in Heart Attack Deaths**

Health Sector Most Targeted by Hackers, Breach Costs Rise to $17.76B

Legacy Systems: The Forgotten Cybersecurity Risk

Third-Party Vendor Incidents & Phishing Cause Some of Largest 2019 Health Data Breaches

**Health IT Security Falls Short: Despite Increased Security Spend, Weakness Remains**

**Legacy Systems & Cybersecurity, a Difficult Reality**

2020 Cybersecurity: Less of a Disease that can be Inoculated – More of a "Bar Fight"

**Healthcare's Number One Financial Issue is Cybersecurity**

**Microsoft's End to Windows 2007 Support Impacts Cybersecurity Risks for Healthcare**

**40 MILLION**

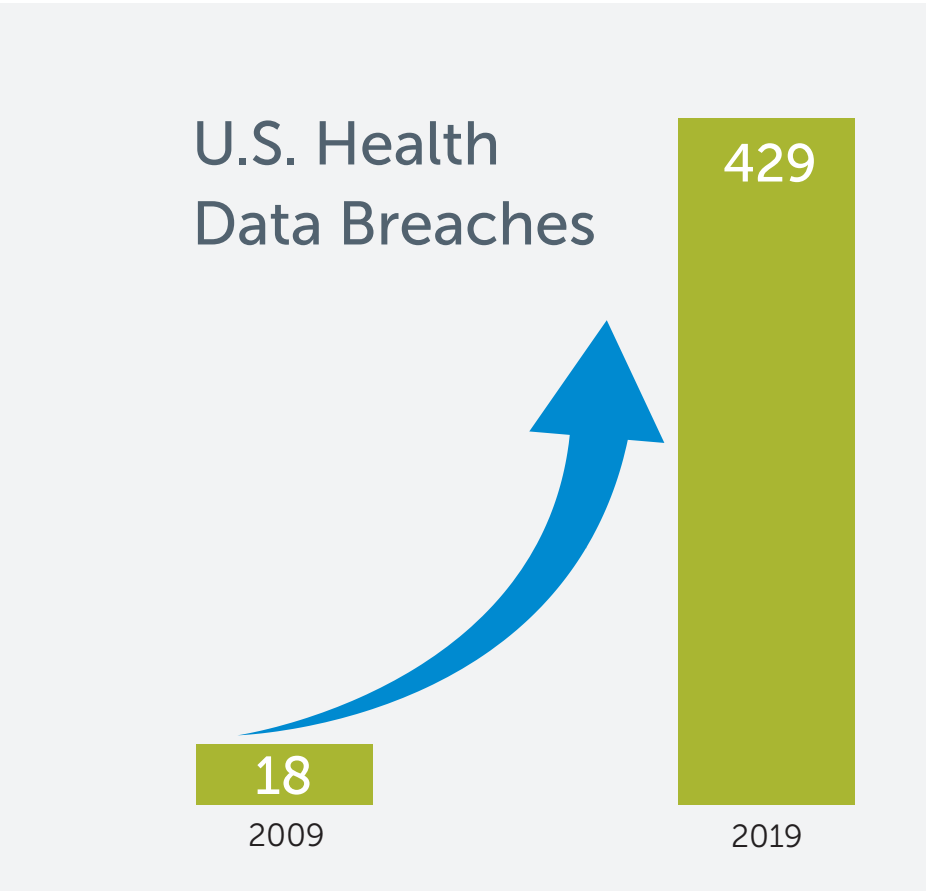
**AMERICANS AFFECTED**

by Health Data Breaches, Highest since 2015

# A Health Assessment of Data Security in Healthcare IT

Healthcare can't seem to tame its volume of security breaches. A report titled The State of Cybersecurity in Healthcare revealed that 2019 recorded the highest number of security breaches since 2015. Clearly, the war against cyber criminals is still waging.

The number of entities involved in health data breaches also significantly increased. In 2019, 429 entities were affected — the highest in the period under review and a 95% increase from the 18 organizations affected in 2009. Provider organizations continue to be the most targeted, making up 78% of all breaches.



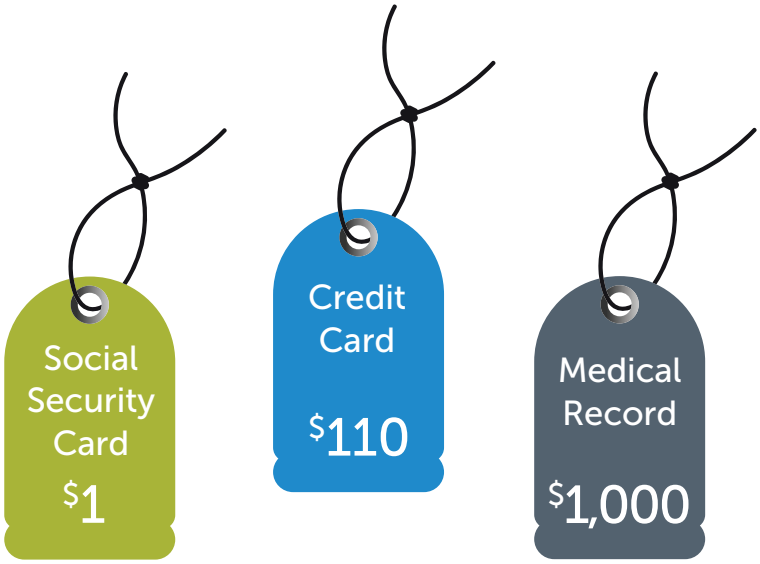

95% Increase in 10 years

While providers of all sizes are at risk, cybercriminals often find smaller healthcare practices to be ripe targets. The hackers leverage technical vulnerabilities, infiltrate the network and virtually shut down the operation until a ransom is paid or restorative measures can get the practice up and running again.

That said, larger provider organizations are not immune to attack. Any healthcare provider, or related supply chain organization, that doesn't utilize best practices for information security is at a high risk for a breach. And, unfortunately, some data is left literally out in the open without any security measures, such as the case where hundreds of servers storing patient X-rays and MRIs for more than 5 million patients in the U.S. lacked even basic security protocols like passwords. These records were so insecure that anyone with fundamental computer skills and a few lines of code could access them.

Cybercriminals, look for the easy score. And, when the financial payoffs are lucrative, cybercriminals are happy to be repeat customers.

Consider that the dark web "street value" for a full medical record that contains date of birth, credit card information, Social Security number, address and email is around $1,000. The lure of this kind of multiplier keeps cybercriminals motivated beyond the $1 for just a Social Security number or even $110 for a credit card account.



# Healthcare providers are getting hit hard, and then getting hit again



More than 50% of organizations breached multiple times

Black Book Market Research found 93% of U.S. Healthcare organizations surveyed were breached in the past handful of years. And, more than half of those breached organizations were breached again (and even again).

Plus, cybercriminals continue to cause undue harm with reports of tumors being added into MRIs to confuse and mislead medical teams.

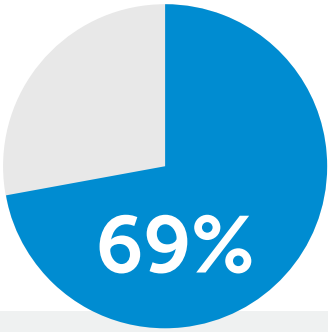
With this in mind, it's not surprising that the business of security in healthcare is rapidly growing.

The global healthcare security market is expected to reach $12.46 billion by 2023, growing at a CAGR of 15.6% from 2017-2023. North America is expected to contribute about half of the total market share. This is based on the work needed to address new cybersecurity laws to combat the overall rise in attacks and efforts needed to adopt more comprehensive security measures.

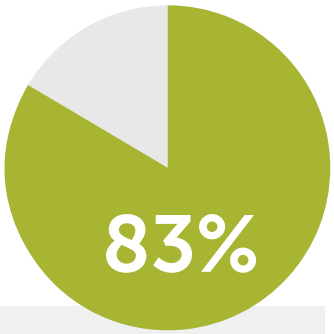
# Security risks lurk in forgotten legacy systems

Multiple silos of data stored in outdated systems offer some of the easiest entry points for hackers. These are oftentimes older and less protected legacy EHR systems. There can be upwards of 30-40 legacy systems running in maintenance mode at a health system that are not truly secure. In essence, having too many unlocked doors and windows leaves your organization unstable at best and provides a large data footprint that must be protected.

These systems — by the sheer nature of their age and diminished capacities over time — are more prone to vulnerabilities. In a HIMSS cybersecurity survey of healthcare organizations:




69% of healthcare organizations have legacy operating systems




83% of healthcare organizations operate with Legacy Windows Servers

- 69% indicated that they had at least some legacy operating systems in place at their healthcare organizations
- 83% of those still operate with Legacy Windows Servers (e.g., 2003, 2008, 2012, 2016 and XP)

**Network servers are almost always the target for hacking-related breaches.** For the many healthcare firms that rely on premise-based applications, security is often lacking. Whether the result of an application vulnerability or just the inability to control access, traditional infrastructure is no doubt a big target for hackers. Add in outdated servers and legacy systems that were installed 10-15+ years ago — that were state-of-the art then but not now — and the health IT environment is ripe for attacks.

Investing in new tools and solutions and making sure they're doing their job may be top-of-mind in your security department, but older, less-used systems could be quietly costing you money and putting you at risk.

With some systems, there are legal barriers, where you're not allowed to touch the system without losing your warranty of certification. You are in a very bad situation—you are doomed if you don't update, and you are doomed if you do. Or, if the software was written in-house, the original developers may have long since moved on and there's no longer anyone around to update the code. The key to making a business case for an upgrade to an old system that seems, on the surface, to be working just fine is to figure out a way to put a real dollar value on the security risk.

With cyber risk insurance gaining popularity, another metric could be the higher costs of insuring legacy infrastructure against breaches. Given the high costs of maintaining legacy systems and the risks that they can introduce — risks that can lead to dented reputations, reduced profitability and hindered competitiveness from stifling the ability to innovate — all organizations should take a good look at their infrastructure. A legacy data archive can be a smart, secure step forward in managing historical patient and operational data well into the future. It offers compliance with the numerous local, state and national regulations as well as a single, easy-to-use solution for historical information. As healthcare systems streamline their go-forward EHR or HIS systems, so too should they streamline their archiving systems to support easy and efficient historical record retrieval.

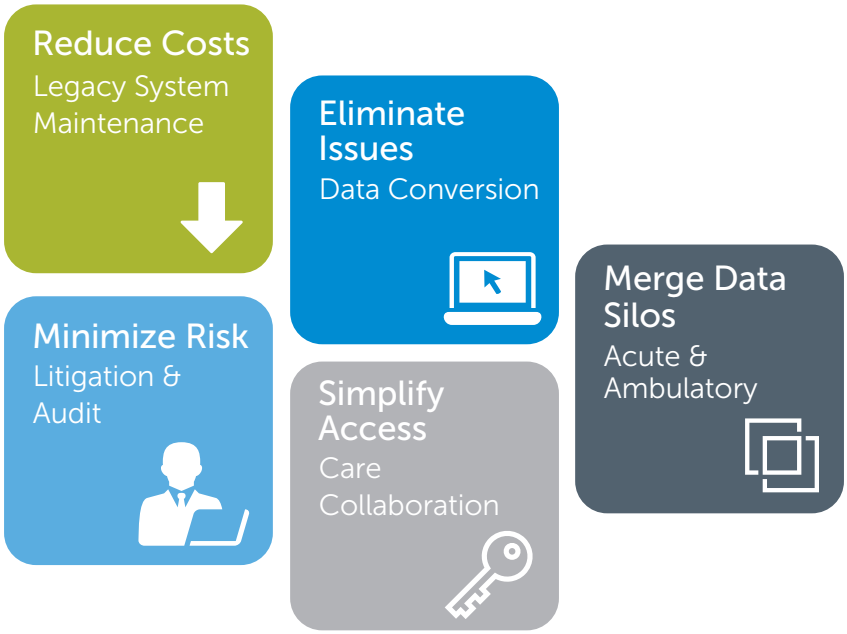
Besides supporting best business practices for information technology, HIPAA requirements specify that healthcare organizations must identify and implement the most effective and appropriate administrative, physical, and technical safeguards to secure electronic protected health information (ePHI). With security concerns rising at healthcare organizations globally, it is more vital than ever to have a handle on everything involved in managing your organization's systems and data. True legacy data management means more than just compiling a list of systems. As the HIPAA Security Crosswalk to NIST states, managing assets enables "the organization to achieve business purposes that are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy."

*"An active archive provides a secure, compliant and accessible solution for healthcare organizations to preserve vital information."*
Tom Liddell, CEO, Harmony Healthcare IT

# The story of active archiving

An active archive is a data management platform that provides a single point of access to historical patient, employee or business data for healthcare enterprises. These web-based solutions, often with release of information workflows, Single Sign-On integrated clinical views, revenue cycle features and eDiscovery capabilities, provide a significant return on investment for healthcare delivery organizations decommissioning legacy systems. The solution consolidates data stores, reduces out-of-production system maintenance costs, mitigates technical risk, complies with record retention mandates and offers both interoperability and data analytics capabilities.

Not all archives are equal. It is important to compare in terms of technical features, services included, upgrades, security practices, add-ons and more.



# With an active archive, you should expect to:

## Reduce Costs

Streamlining the long-term storage of historical PHI now will save money in the long-run. Not only will it reduce costs paid for the support and technical maintenance of an antiquated system, it will save on training new staff how to access information over the next 7-25 year retention period.

## Eliminate Issues

Preserving historical patient data is the responsibility of every provider and health institution. As servers and operating systems age, they become more prone to data corruption or loss. The archival of patient data to a simplified and more stable storage solution ensures long-term access to the right information when it's needed for an audit or legal inquiry. Incorporating a data archive avoids the costly and cumbersome task of a full data conversion, yet provides the ability to search the discrete data elements for ongoing access to historical records. Audit logs may be sent to a third party monitoring solution that offers alerts of potential threats for the lifetime of the record.

## Minimize Risks

Providers are required to retain data for nearly a decade or more past the date of service. Check with your legal counsel, HIM Director, medical society or AHIMA on medical record retention requirements that affect the facility type or practice specialty in your state.

## Simplify Access

A comprehensive active archive can provide immediate and ongoing access to the complete health record. With single sign-on capabilities, the clinician can access the health record at the point of care. Further saving time, a Consolidated Clinical View in an archive aggregates a single patient's encounter data across multiple legacy data sources to a single screen. Plus, when an archive stores data discretely, it opens up to the time-saving feature of filtering and sorting. Not only can data like medications or lab values be readily discovered and reviewed, but they can also be sorted in ascending, descending, alpha or numeric order. Overall, workflows are improved across the healthcare continuum as health, business and operational records are retained and available for future needs.

## Merge Data Silos

Decades worth of data from disparate legacy software applications is archived for immediate access via any browser-based workstation or device. This consolidation makes eDiscovery searches and release of information workflows for legal and HIM users more efficient.  It also makes data analytics and interoperability available.

As the IT team continues to refine and update the health system's long-range plan for cybersecurity, it makes sense to include a review of the landscape the team is protecting. Bottom line, a health team's best defense is to limit the number of systems it needs to safeguard. There are many business reasons to consolidate legacy systems into a single and secure archive, but perhaps the most important is the added security of having less systems at risk for attack.

Active Archiving is the **one big defensive move** your healthcare organization can take immediately to protect its EHR, ERP and HR systems to keep cyber criminals locked out.

# 10 privacy and security questions to ask your future data archiving partner to make sure your data is safe.

When going through a data migration, finding a legacy data archiving partner you can trust is a critical piece of the puzzle. We've put together a list of ten questions for you to ask during vendor selection that will make you feel certain you are investing in a partner that will protect you and your data.

## 1 Do you have a full time Privacy and Security Officer and/or Compliance Officer on staff?

*With so much at stake, it is appropriate to expect and verify that a senior level resource is dedicated to managing security and privacy 100% of the time.*

## 2 Will your ePHI and PII be stored within a Tier III (or higher), SOC 2-certified data center?

*The classification of the data center is pertinent to data security but also to ensure the product will operate at the up-time levels a healthcare provider requires.*

## 3 Have you committed to security excellence by obtaining a HITRUST or other CSF Certification?

*This sort of credentialing is voluntary and can be indicative of their priorities when it comes to data security. Ask if they've taken the time and resources to achieve this level of certification.*

## 4 Have you made a formal commitment to employee security training and awareness?

*Ensuring protection against the latest threats to your healthcare data is a moving target. Ask how their workforce maintains its HIPAA knowledge base and stays ahead of the curve.*

## 5 What is your process to maintain privacy and security policies and procedures?

*Their policies and procedures should be reviewed and updated routinely in order to keep up with the changes in policy and risk management best practices.*

## 6 Will our data be fully secure while in transit and at rest?

*With lots of data to manage, it is critical to protect it at every stage. Ask about their security framework for this process.*

## 7 What are your data validation standards to ensure we meet data retention requirements?

*Ask how your archiving partner about the process for ensuring 100% data integrity through automated and manual validation processes.*

## 8 Do you offer features like Single Sign-On and role-based security?

*Features that allow easy clinical access to data and allow for monitoring of security enhance the overall security of your archive. Ask about break the glass.*

## 9 Does your archive solution contain robust audit solutions like FairWarning® to monitor initial and ongoing access?

*Push beyond the general assurances and ask about how data will be tracked at each stage of user access. Can they send their audit logs, automatically, to one integrated audit product?*

## 10 Do you carry adequate Cyber Security Insurance to protect all parties involved?

*As stewards of your data, a good data archiving vendor will be prepared to cover you and themselves in the event of a breach.*

# About Harmony Healthcare IT and HealthData Archiver®

Harmony Healthcare IT (HHIT) is a legacy data management firm in South Bend, IN that archives patient, employee and business records for healthcare organizations nationwide. To strengthen care delivery and improve lives, HHIT preserves vital information in a way that keeps it secure, compliant, accessible and usable. Since 2006, the HHIT team of experts has extracted, migrated and retained billions of records and petabytes of data from over 500 different clinical, financial and administrative software brands. That information is secured on a cloud-based storage platform, HealthData Archiver®, which is live in production on Epic's App Orchard. Harmony Healthcare IT has been ranked #1 in the 2020 Best in KLAS Software & Services Report as a Category Leader in Data Archiving, and as the top data extraction and migration healthcare IT company according to Black Book™ Market Research in 2019 and 2020. HHIT was also selected by Modern Healthcare as one of the 2019 Best Places to Work in Healthcare.


FOR MORE INFORMATION, PLEASE CONTACT:

Amy Holmes, Director of Marketing

info@harmonyhit.com

(800) 781-1044


harmony HEALTHCARE IT®

© 2020 Harmony Healthcare IT. All Rights Reserved. HealthData Archiver® is a registered trademark of Harmony Healthcare IT.