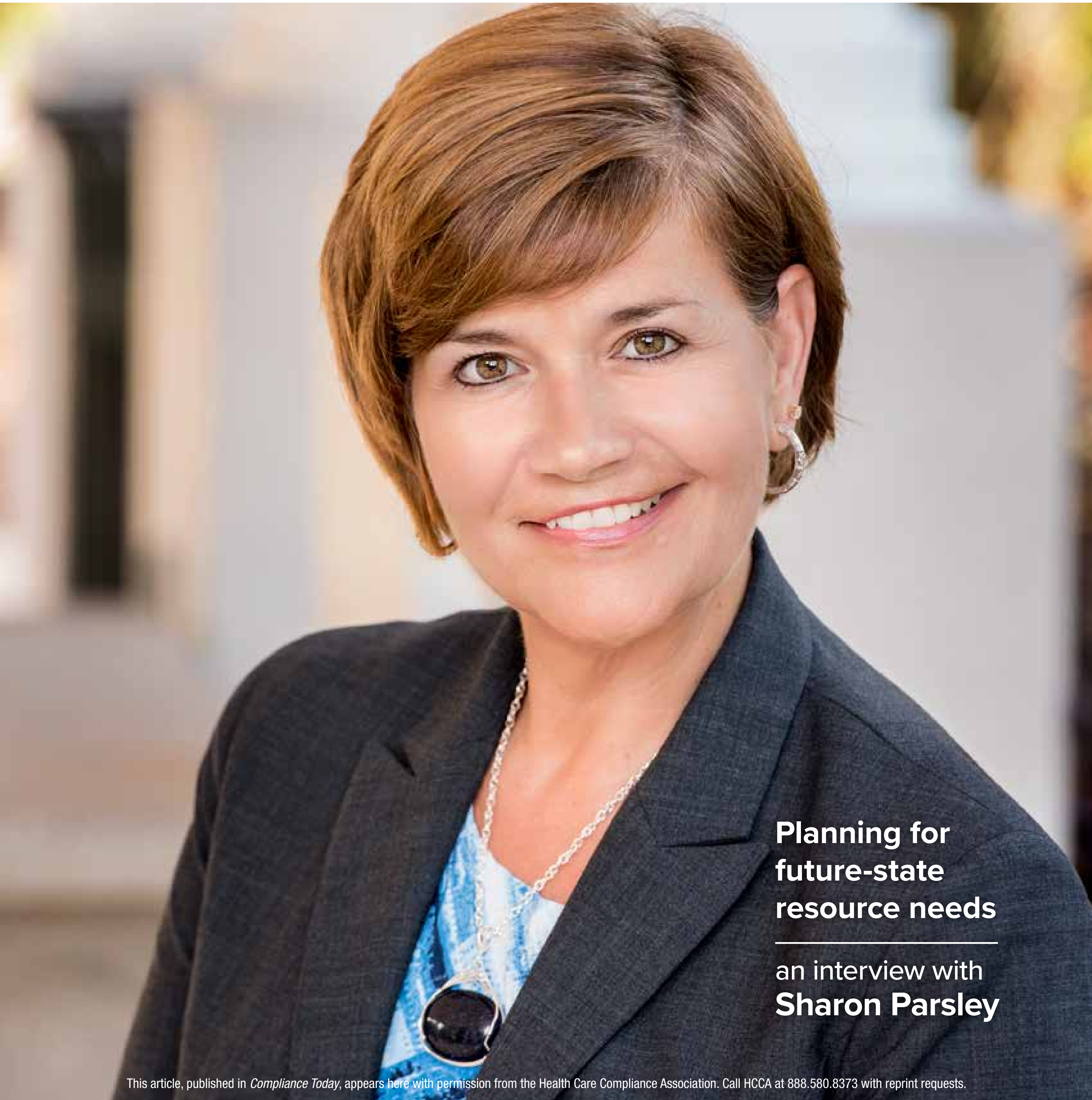
HCCA
hcca-info.org

Compliance TODAY

A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

OCTOBER 2018



Planning for future-state resource needs

an interview with
Sharon Parsley

ARTICLES

Compliance
TODAY

EXECUTIVE EDITORS: Gerry Zack, CCEP, Incoming CEO, HCCA
gerry.zack@corporatecompliance.org

Roy Snell, CHC, CCEP-F, CEO, HCCA
roy.snell@corporatecompliance.org

NEWS AND STORY EDITOR/ADVERTISING: Margaret R. Dragon
781.593.4924, margaret.dragon@corporatecompliance.org

COPY EDITOR: Patricia Mees, CHC, CCEP, 888.580.8373
patricia.mees@corporatecompliance.org

DESIGN & LAYOUT: Pete Swanson, 888.580.8373
pete.swanson@corporatecompliance.org

PROOFREADER: Bill Anholzer, 888.580.8373
bill.anholzer@corporatecompliance.org

PHOTOS ON FRONT COVER & PAGE 16: John Jernigan Photography

Compliance Today (CT) (ISSN 1523-8466) is published by the Health Care Compliance Association (HCCA), 6500 Barrie Road, Suite 250, Minneapolis, MN 55435. Subscription rate is $295 a year for nonmembers. Periodicals postage-paid at Minneapolis, MN 55435. Postmaster: Send address changes to Compliance Today, 6500 Barrie Road, Suite 250, Minneapolis, MN 55435. Copyright © 2018 Health Care Compliance Association. All rights reserved. Printed in the USA. Except where specifically encouraged, no part of this publication may be reproduced, in any form or by any means without prior written consent of HCCA. For Advertising rates, call Margaret Dragon at 781.593.4924. Send press releases to M. Dragon, 41 Valley Rd, Nahant, MA 01908. Opinions expressed are not those of this publication or HCCA. Mention of products and services does not constitute endorsement. Neither HCCA nor *CT* is engaged in rendering legal or other professional services. If such assistance is needed, readers should consult professional counsel or other professional advisors for specific legal or ethical questions.

VOLUME 20, ISSUE 10

by Shannon Larkin

Record retention strategies when systems get replaced

- » Running out-of-production systems for record retention is risky.
- » Aging applications are a top cybersecurity concern for providers.
- » Healthcare ranked number one for cybersecurity attacks in 2017.
- » There are threats to consider during the data life cycle.
- » Consider consolidating data into one secure, vendor-neutral archive.

Shannon Larkin *(slarkin@harmonyhit.com) is Vice President of Marketing & Business Development for Harmony Healthcare IT in South Bend, IN.*

/in/shannonlarkin

Larkin

Most healthcare providers today are at risk, keeping out-of-production electronic health records (EHR) and enterprise resource planning (ERP) systems up and running simply to meet record retention requirements. Although each backstory is a little different, most organizations have at least a small collection of legacy systems — each storing personally identifiable information for patients or employees. Some of these systems were inherited during mergers and acquisitions; some were sunset by the respective vendor; others were simply replaced after failing to meet user production or workflow requirements. These outdated systems were likely built on a variety of platforms and developed sometime over the last 10–25 years. They also likely sit alongside newer "go-forward" EHR or ERP systems that actively manage the current workload, yet don't offer an easy or affordable pathway for consolidating and storing the historical data.

This multi-generational band of legacy EHR and ERP systems collectively is charged with meeting record retention regulations set at agency, state, and national levels as well as HIPAA regulations for privacy and security. Depending on medical specialty or facility type, some records might need to be kept for 25 years or more and, if there is an audit or need to access the data, there often is a tight timetable for producing the information. Efficient e-discovery and release of information can quickly become a tall order, particularly if patient or employee data is stored in multiple systems. More importantly, out-of-production systems — especially those not being routinely upgraded or patched — create risks for system failure and cybersecurity attacks.

It is not surprising that vulnerabilities from aging applications and technologies are the number one concern IT executives cited with respect to cybersecurity in the "2017 Federal CIO Survey" conducted by Grant Thornton and the Professional Services Council.[1] This concern correlates with healthcare ranking number one for cybersecurity attacks for the same year, when it previously hadn't been in the top six.[2]

As our nation's healthcare teams wrestle with cybersecurity, they also are faced with the challenge of how to manage the life cycle of health data as the volume of records continues to multiply exponentially. The 153 exabytes of health data from 2013 is expected to exceed 2,314 by 2020.[3] For reference, one exabyte is one billion gigabytes—and that's a lot.

Security threats to health data

One of the biggest challenges in health IT is security. Health records are valuable on the black market, often garnering $50 or more per record, compared to $1 for a credit card.[4] This valuable data could be considered low-hanging fruit as the healthcare industry now scrambles to protect its records and systems—both historical and active.

Outdated systems and too many data silos can be easy entry points for a hacker. Each legacy system is a potential open door that can leave the organization vulnerable for cyberattack. Several common security issues can result from outdated systems and too many data silos that need to be protected. The main issues include:

- **Unencrypted data in transit:** Many legacy applications are running on old technology that creates a multitude of data integrity vulnerabilities, especially when in transit.
- **Unsupported operating systems:** Microsoft Windows 2003 is still out there without patches. Some healthcare organizations continue to ride it out with fingers crossed.
- **Insecure legacy applications:** Older applications lack back-end features and functions such as audit logs, strong password protection, resets, and screen locks that would satisfy National Institute of Standards and Technology (NIST) or Health Information Trust Alliance (HITRUST) controls.
- **Outdated security protocols:** Lacking up-to-date conventions, older applications may auto-negotiate to a lower system's capabilities.
- **Unregulated back door access:** This is often a result of system acquisitions and sometimes self-developed systems that have vulnerable back entry points long after the developer is gone.

Record retention strategies for managing legacy data when systems get replaced

As cross-functional governance teams work to determine the best course of action for life cycle data management, there are four main options to consider.

1. Convert all the data

Often, because it would ideally keep all records together, healthcare organizations discuss the possibility of migrating all historical patient, facility operations, and/or employee data into the go-forward system. The high cost and complexity of this approach—along with the time and potential risk to the integrity of the migrated data—usually rules it out as an all-inclusive option. Oftentimes, a key but limited set of data elements is converted. However, this still leaves data "left behind" for which a retention strategy must be employed.

2. Maintain the legacy system

Maintaining an out-of-production system in view-only mode offers some definite short-term benefit; however, with long-term record retention in mind (which, in certain situations, could exceed 25 years), this option will likely render the aging application and its supporting infrastructure vulnerable over time. In addition to technical risk, it can be cumbersome and less efficient to both provide release of information services from multiple systems as well as to train staff on their use with employee turnover. Finally, vendor maintenance costs must be factored in for as long as the system will remain up and running.

3. PDF the records

Occasionally, discussions center on converting all legacy data into PDFs for long-term storage. However, this approach is generally not any less expensive than a discrete archive and may leave information buried in multi-page documents, making it more difficult to locate information quickly and easily. User access tracking and audit history are also less reliable or available in this approach. Further, if record query, research, or analysis is later desired, data will be less readily accessible when stored within the PDF documents versus as discrete data elements.

4. Archive the data discretely

Aside from some up-front legacy system extraction and migration costs, an electronic archive of discrete data elements can be a positive long-term solution on many fronts. Numerous legacy systems can be migrated into one scalable and secure data archive that meets the latest security requirements. The records are simple to access, sort, filter, print (in whole or in part), and securely release or purge as required. Multi-data domain (i.e., EHR and ERP systems) as well as multi-data source (i.e., two or more different brands of legacy EHR systems) storage provides an easy method to index and readily search patient and employee records. Over time, employee training on a single archive is much more manageable compared to keeping staff trained on multiple legacy systems on varying platforms. The same holds true for technical risk, with one archive being less vulnerable than multiple legacy systems on a network. Finally, the maintenance cost on a single, updated archive system often shows a return on investment compared to keeping multiple legacy systems (from multiple vendor contracts) up and running, along with employing the technical personnel to keep multiple systems alive.

There are numerous reasons to migrate historical data into one centralized, cybersecure, vendor-neutral archive, including:

- **Compliance:** Providers are required to have data for nearly a decade or more past the date of service. Check with your legal counsel, Health Information Management (HIM) director, medical society, or American Health Information Management Association (AHIMA) on medical record retention requirements that affect the facility type or practice specialty in your state.
- **Elimination of risk:** Preserving historical patient data is the responsibility of every provider. As servers and operating systems age, they become more prone to data corruption or loss. The archiving 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.
- **Cost reduction:** Streamlining the long-term storage of historical personally identifiable information 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, but it will save on training new staff on how to access information over the next 7–25 years.
- **Simplified access to data:** We all want data at the touch of a button. Gone are the days of storing historical patient printouts in a binder or inactive medical charts in a basement or storage unit. By archiving

medical documents, data, and images, the information becomes immediately accessible to those who need it.

- **Merging of data silos:** Decades worth of data from disparate legacy software applications can be archived for immediate access, efficient e-discovery, and more effective health information management workflows.

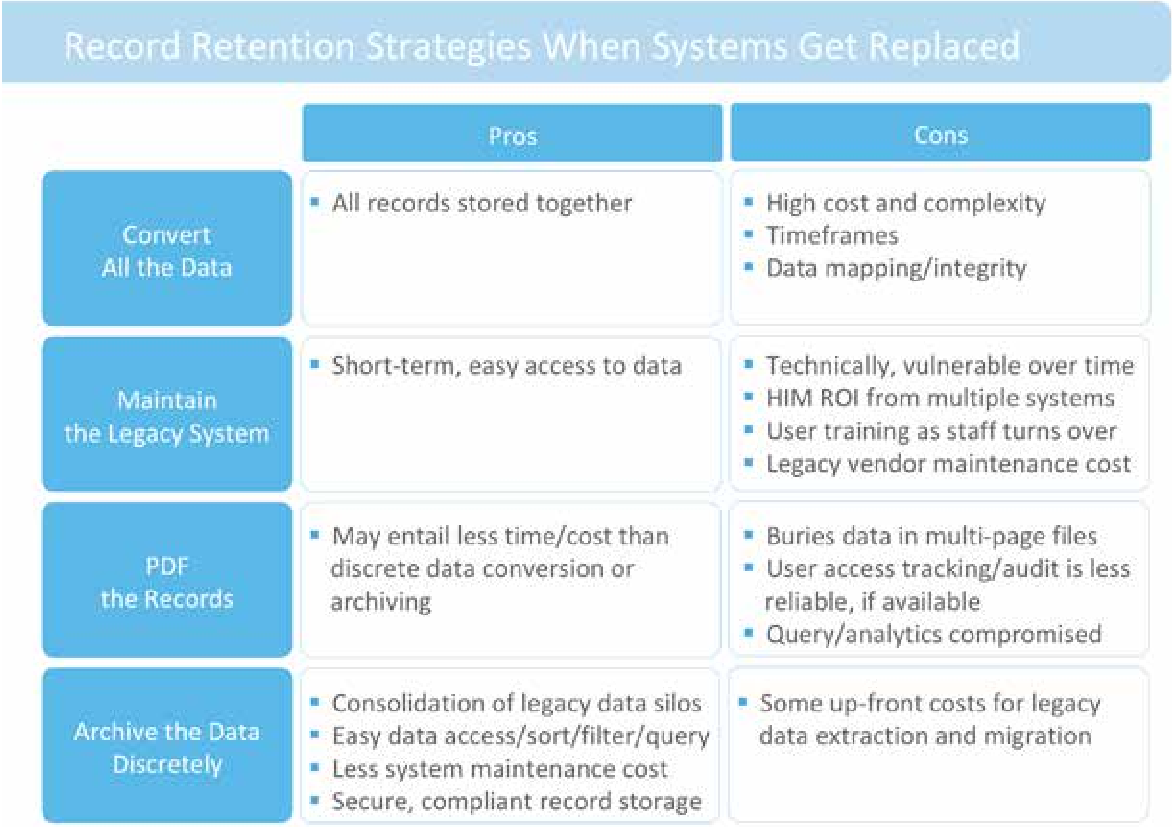
The future of legacy data management

Planning ahead to manage legacy data when an EHR or ERP system gets replaced is key to securely complying with record retention policy. An electronic archive with a searchable data function for historical records may prove less costly over the long term and most effective when records must be accessed for e-discovery, analytical query, or an audit. Some healthcare organizations have developed stand-alone methods for data management in-house; others rely on vendor-developed systems and/or architecture developed by private companies.

A data archive offers a secure and efficient method to batten down the hatches to protect legacy data from cybersecurity breaches while providing ongoing access to records and compliance with the highest standards.

Shannon Larkin will present "Patient & Employee Record Retention Strategies When Systems Get Replaced" at 11:00 a.m., Tuesday, October 9, 2018, during the Clinical Practice Compliance Conference in San Diego.

1. Grant Thornton: "2017 Federal CIO Survey" September 2017. Available at https://bit.ly/2OBHxYt
2. "McAfee Labs Report Sees Cyberattacks Target Healthcare and Social Media Users" *Business Wire*; September 26 2017. Available at https://bit.ly/2wf1NYn
3. Kenneth Corbin: "How CIOs Can Prepare for Healthcare 'Data Tsunami'" *IDG Communications* December 16, 2014. Available at https://bit.ly/2watDEQ
4. FBI Cyber Division—Private Industry Notification: "(U) Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain" April 8, 2014. Available at https://bit.ly/1iiu1GI



Record Retention Strategies When Systems Get Replaced

	Pros	Cons
Convert All the Data	▪ All records stored together	▪ High cost and complexity ▪ Timeframes ▪ Data mapping/integrity
Maintain the Legacy System	▪ Short-term, easy access to data	▪ Technically, vulnerable over time ▪ HIM ROI from multiple systems ▪ User training as staff turns over ▪ Legacy vendor maintenance cost
PDF the Records	▪ May entail less time/cost than discrete data conversion or archiving	▪ Buries data in multi-page files ▪ User access tracking/audit is less reliable, if available ▪ Query/analytics compromised
Archive the Data Discretely	▪ Consolidation of legacy data silos ▪ Easy data access/sort/filter/query ▪ Less system maintenance cost ▪ Secure, compliant record storage	▪ Some up-front costs for legacy data extraction and migration