White Paper

Enterprise Data Management: Creating Competitive Advantage for Healthcare Organizations

Sponsored by: Commvault

Lynne Dunbrack
February 2017

INTRODUCTION

Widespread adoption of healthcare IT, along with advancements in imaging technology and the proliferation of mobile and internet-connected medical devices, is driving massive increases in data volume and complexity. Images account for more than half of a healthcare organization's data, and 80% of healthcare data is unstructured. Market consolidation and the push for interoperability mean more data sources and data aggregation activities across the enterprise. There were 102 hospital and health system transactions in 2016, down slightly from a high of 112 transactions in 2015, according to Kaufman, Hall & Associates, a financial management consulting firm. New care delivery and reimbursement models are compelling healthcare organizations to create a 360-degree view of all types of enterprise data to analyze clinical, operational, and financial performance. New alternative payment models (APMs), such as accountable care organizations (ACOs), patient-centered medical homes (PCMHs), bundled payments, and pay-for-performance (P4P) initiatives, are relatively new but are growing in number. For example, there were 838 ACOs covering 28.3 million lives at the beginning of 2016, up from 782 ACOs covering 22.5 million lives in 2015, according to Leavitt Partners in partnership with the Accountable Care Learning Collaborative. These market trends underscore the need for a robust health data management platform that manages both clinical data and financial data across the enterprise.

Healthcare organizations are under mounting pressure to improve the quality of care while reducing costs. Successful health data management addresses both challenges. For example, missing clinical information is a leading cause of medical errors. The inability to locate the correct medical image because it is stored not in the patient's electronic medical record but in a legacy picture archiving and communication system (PACS) application can delay care or prompt physicians to reorder tests, which drives up costs and exposes patients to more radiation, thereby creating potential patient safety issues. Redundant, unnecessary services go against the tenets of value-based purchasing of the "less is more" drive for value. Multiple disparate legacy systems not only add to the complexity of finding the image at the point of decision making and IT costs but also erode the confidence of patients when they are subjected to unnecessary procedures and tests because their health information is not readily available. Clinical archiving provides healthcare organizations the means to decommission legacy PACS yet retain their data so that images can be easily located.

Strong data management includes a sound backup, recovery, and archiving strategy that makes data readily accessible when needed — whether in response to a clinician's request for a patient's medical file, an IT or a hacking incident, or legal discovery and hold requests. This, in turn, leads to more

efficient IT operations and reduced storage requirements, yielding a positive return on investment. Furthermore, many of the capabilities built into a data management platform, such as disaster recovery and business continuity, encryption of data in motion and at rest, and access and data integrity controls, enable healthcare organizations to execute against their security and compliance plans, thereby serving to enhance the security posture of healthcare organizations.

IN THIS WHITE PAPER

This IDC Health Insights White Paper is sponsored by Commvault and examines the need for a robust health data management platform that manages both clinical data and business data across the enterprise. This White Paper is based on briefings with Commvault and interviews with executives as well as IDC Health Insights' security and compliance research. The objective of this document is to educate healthcare organizations about how enterprise-grade health data management can protect electronic health record (EHR), business, and IT data (e.g., email and financial data); enable clinical and image archiving; and enhance the security posture of healthcare organizations with regard to cyberattacks that compromise IT systems and data.

HEALTH DATA MANAGEMENT AND EHR DATA PROTECTION

Many of the major trends that promote the widespread deployment of healthcare IT solutions demonstrate the need for sound health data management across the enterprise. These same trends are also making healthcare organizations more vulnerable to cybersecurity threats, underscoring the need for healthcare organizations to increase their investment in IT security to execute a robust data protection and recovery strategy.

- **More electronic health information is widely available.** The American Recovery and Reinvestment Act of 2009 (ARRA) provided $20 billion in incentive payments for physicians and hospitals to deploy EHRs. In 2009, 9% of hospitals had adopted a basic EHR with clinician notes. Since then, the adoption rate of a basic EHR has increased more than ninefold to 84% in 2015, according to the ONC/American Hospital Association (AHA), AHA Annual Survey Information Technology Supplement. There is more electronic health data than ever before as healthcare providers have made great strides to achieve meaningful use of EHRs, investing millions in deploying EHRs, sometimes to the detriment of investing in other technologies, including security.
- **Healthcare organizations are consolidating.** In an effort to seek competitive advantage through size and access to resources, or to simply survive, a number of healthcare organizations are looking to acquire other healthcare organizations or be acquired. Portfolios expanded by merger and acquisition (M&A) activity tend to be more complex and heterogeneous with data siloed in applications scattered across the enterprise. Consequently, securing health information has become more complicated and requires a comprehensive strategy rather than a series of one-off point solutions. Healthcare organizations involved in M&A activity are looking for ways to reduce "time to value" and standardize business continuity policies across the enterprise to achieve the promised benefits of consolidation and economies of scale.

- **Consumerization of technology is driving adoption of mobile devices.** Healthcare professionals are a highly mobile workforce and increasingly want to use their personal smartphones and tablets at the point of care. According to an IDC Health Insights survey, 79.8% of healthcare organizations reported that bring your own device (BYOD) would increase in 2017 (based on a percentage of clinicians using personal devices). Mobile devices require additional security oversight because of their unique vulnerabilities (e.g., loss, theft, and introduction of malware to the corporate network). BYOD intensifies the complexity of securing mobile devices because both corporate data and personal data are stored on the device, and end users often download mobile applications with little regard to the risk of also downloading malware with the applications.
- **Healthcare data is growing in volume and complexity.** The need to rationalize storage for medical images and accommodate the growing variety and volume of unstructured content being created has become acute. Furthermore, to develop a 360-degree view of patients, innovative healthcare organizations are beginning to explore the collection of data from nontraditional data sources, such as utility companies and the weather bureau, to identify potential health risks. For example, utility bills that do not change in the summer could indicate that a vulnerable elderly patient doesn't have air conditioning and could be at risk for heat stroke or an uptick in the pollen count could trigger an asthma attack for an asthmatic. Both situations could result in an expensive emergency room visit or hospital admission.
- **Cloud technology adoption by healthcare organizations is becoming more common.** Software as a service, platform as a service, and infrastructure as a service are attractive means of deploying IT solutions because they reduce IT costs while accelerating speed to value for healthcare organizations. Many healthcare organizations initially had reservations about the security risks associated with cloud storage. However, 87.5% of provider respondents to an IDC Health Insights survey reported that now they are comfortable with cloud technology because cloud service providers should have more expertise in mitigating the risk of a cyberattack compared with the typical healthcare organizations.
- **Meaningful use requires health information exchange.** ARRA and its meaningful use requirements obligate healthcare organizations to share health information to enable population health management, care collaboration and coordination, and care transitions. Consequently, more patient information is aggregated across the enterprise so that the information is available to clinicians at the point of care. Healthcare organizations are responsible for providing Health Insurance Portability and Accountability Act (HIPAA)-compliant security for protected health information (PHI) they receive from other healthcare organizations.
- **Value-based healthcare and reimbursement models require data aggregation for analytics.** The evolving care delivery and reimbursement models, such as value-based healthcare, will require a technology platform that correctly identifies patients and provides secure access to patient health records managed by multiple healthcare organizations' IT systems, thereby facilitating secure exchange of health information among care team members to improve care coordination and collaboration and combine clinical data and financial data to feed the analytics engine and provide a full picture of clinical, financial, and operational performance. Consequently, healthcare organizations will be investing in more technology that collects, aggregates, analyzes, and shares electronic health information among medical trading partners. These data stores will be attractive targets to cybercriminals because they contain information that can be used for both financial identity theft and medical identity theft. Healthcare organizations that do not adequately protect their own systems risk their trading partners withholding vital data because of their poor security practices. Healthcare organizations are at greater risk of a cyberattack than ever before in part because electronic

health information is more widely available today than in the 20 years since HIPAA was passed. Threat vectors are increasing in number and scope of the attack in healthcare because cybercriminals perceive healthcare organizations to be a soft target compared with financial services and retailers. Historically, healthcare organizations have invested less in IT, including security technologies and services, compared with organizations in other industries, thereby making themselves more vulnerable to successful cyberattacks. The value of health information, which can be used to commit medical fraud, is surpassing the value of social security and credit card numbers on the black market, which increases the attractiveness of stealing health information. Not surprisingly, cybercriminals are increasingly targeting healthcare organizations; an industry study revealed that 88% of ransomware attacks were made on healthcare organizations.

Today's attacks are more insidious, targeting known vulnerabilities in unpatched web servers to penetrate networks. Of particular note is ransomware, which encrypts critical system files, rendering them inaccessible until a ransom is paid for the key to unlock the files. The impact of ransomware beyond the extortion payment is the risk of adversely affecting patient care, daily operations, and ultimately, patient safety. When vital systems are locked, staff must revert to paper-based and manual processes, which can create delays in accessing critical patient information and thus delays in providing patient care. In extreme cases, hospitals infected with ransomware may have to divert ambulances carrying patients with non-life-threatening conditions to other hospitals and cancel patient appointments because patients' electronic health information is inaccessible. Delay in receiving care and diversion have an impact not only on patient care but also on the finances of the healthcare organization under attack.

The U.S. Department of Health and Human Services recommends that healthcare organizations have a solid backup and data protection strategy in place. A clearly defined process for business continuity and disaster recovery is an essential component of a comprehensive security plan. Healthcare organizations that can quickly restore vital clinical and business systems can minimize the potential damage done to IT systems and operations, along with the resulting downtime caused by ransomware or other types of cyberattacks.

Benefits of a Health Data Management Platform

Healthcare organizations that layer their business and clinical systems on top of a comprehensive health data management platform can mitigate the risk of an IT incident; thwart cyberattacks; and reduce the potential risk of serious damage to the infrastructure, expensive privacy and security breaches, and loss of reputation and consumer confidence in the ability of the organizations to adequately protect sensitive health information. When properly deployed, a health data management platform can provide the following benefits:

- **Reduce system downtime and the associated costs and negative impacts.** System downtime is expensive, whether measured in terms of IT's effort to restore datacenter operations or the adverse impact on patient care due to the inability to access mission-critical applications. A 2016 study by Ponemon Institute estimates that the total cost of unplanned datacenter outages in healthcare is $918,000, which places the healthcare industry third behind financial services ($994,000) and communications ($970,000). Fines and penalties, plus notification fees, can cost healthcare organizations millions of dollars. Health data management systems that capture data snapshots make it easier and faster to restore EHRs and other clinical and operational systems, thereby minimizing negative cost, operational, and clinical impacts.

- **Facilitate moving backups from on-premise to the cloud.** Healthcare organizations feel more comfortable with cloud technology now than in the past. Cloud-based health data management solutions enable more elastic data storage requirements and reduce costs because healthcare organizations need to pay for only the space their data consumes. In addition, backups and archives can be housed in different geographic locations, providing access to critical data in the event of a local natural disaster such as a hurricane or a tornado.
- **Provide centralized management for data recovery.** The sheer number of clinical and business systems used by a healthcare organization has resulted in IT using a number of point solutions to back up and restore critical data. Should a system failure occur, IT may not be able to recreate a "snapshot in time." For example, the last recoverable file for the billing system may be one week old, while the recovered EHR data is two days old. A health data management platform provides a centralized approach to orchestrating backups so that IT can restore all systems back to a specified point in time if necessary.
- **Enable HIPAA compliance.** Data management platforms include a number of security features such as access and data integrity controls, encryption, and audit logs, which can help healthcare organizations meet HIPAA and other privacy and security requirements when the technology is used in accordance with the healthcare organizations' compliance plan. In the case of HIPAA, there are requirements regarding obtaining PHI in the event of an emergency (e.g., disaster recovery) and limiting access to only those who are authorized to access a given patient's health data (e.g., two-factor authentication and data loss prevention). PHI must also be encrypted when in motion and at rest.

Considering Commvault

Commvault (Nasdaq: CVLT) was founded in 1996. Over the past 20 years, the company has experienced significant growth, with 2,400 employees and offices in 6 continents. Commvault's core offering is an enterprise-class data management platform that provides data protection, recovery, and search capabilities to midlevel and enterprise-level organizations on-premise or in the cloud. Advanced capabilities manage the content of cloud applications and search for data on mobile devices and other endpoints. Commvault's healthcare solutions are built off of Commvault's data management platform to provide a single platform to manage clinical and business data assets across the enterprise. Commvault has more than 2,500 healthcare customers worldwide.

Healthcare Business Solutions

Core functionality of Commvault's health data management platform encompasses backup, recovery, and archiving; application and data management; mobile and endpoint data protection; search and eDiscovery; and cloud services. Commvault provides a complete view of all stored data regardless of whether the data is stored on-premise or in the cloud, thereby simplifying healthcare organizations' data storage needs across all types of data and data formats: insurance claims, EHRs, medical images, and data from mobile devices and sensors including consumer wearables. Built-in deduplication reduces network backup traffic and optimizes storage, allowing healthcare organizations to retrieve data faster and reduce the storage footprint. Commvault takes a vendor-neutral approach to storage, working with a variety of hardware vendors and more than 25 cloud storage service providers.

Commvault EHR Data Protection

Commvault EHR data protection streamlines the snapshot and storage process, creating data snapshots of all databases and file systems. Embedded compression and deduplication software results in a smaller storage footprint. Data is copied to disk, tape, or cloud, or any combination of media, using the customer's preferred storage hardware, thereby reducing the total cost of ownership by leveraging existing storage infrastructure. Using snapshots, Commvault EHR data protection recovers file systems and databases within minutes of system failure versus hours or days, thereby reducing costly EHR downtime. Data is then indexed, further enabling data management functions, including the ability to manage and recover data and report on system performance. Currently, Commvault provides EHR data protection services for Epic and MEDITECH.

Enterprise Image Archiving

Commvault provides the following enterprise image archiving solutions to enable healthcare organizations to decommission legacy PACS and migrate to new archival systems:

- **Commvault Clinical Archive.** The Commvault Clinical Archive is a clinical data-aware data repository that is integrated with EHR and medical imaging systems. The Clinical Archive can manage structured and unstructured data, along with DICOM images. It can be deployed both on-premise and in the cloud. Two primary use cases for Commvault Clinical Archive are PACS decommissioning and enterprise image archiving. As healthcare organizations move to vendor-neutral archives or application-independent clinical archive systems, the need to retain legacy PACS to store images and unstructured data declines. Reducing the number of PACS through decommissioning leads to obvious cost savings by lowering hardware, maintenance, and administration costs associated with operating multiple PACS. Similarly, centralized image archiving provides a permanent archive for legacy PACS data and helps minimize the number of data silos. The Commvault Clinical Archive provides access to data created across multiple legacy PACS and thus supports a variety of common data standards (e.g., DICOM, non-DICOM images, PDF, and JPEG).
- **PACS migration.** In 2015, Commvault announced a strategic partnership with Laitek that combines the respective expertise of Commvault in data management and Laitek in rapid data migration and storage services for PACS replacements. Together, the companies will jointly enhance Commvault's clinical data management platform to make migration faster and less expensive through the use of 30+ prebuilt connectors to multiple legacy PACS. Customers do not need to change their storage vendor or technologies (e.g., RAID, SAN, tape, flash, web scale, or appliance), eliminating the need to invest in new storage infrastructure. The combined solution was designed with cloud technology in mind from the beginning, and healthcare organizations can archive enterprise images in the cloud.

Commvault Data Security Solutions

Commvault's products feature built-in security, which provides multiple layers of protection. User security is provided through extensible credential infrastructure with two-factor authentication. Commvault is expanding the use of directory services to include RADIUS and JumpCloud in addition to more common directory services. Commvault provides endpoint data protection for laptops, mobile devices, and even cloud file-sharing services. With the proliferation of personal mobile devices and laptops as a result of "bring your own device" programs, the ability to offer endpoint data protection as a service becomes increasingly important. Network security is also an essential consideration because

many cyberattacks exploit known network vulnerabilities. Spam prevention built into CommServe, along with the security certificates, protects secure client communication. Commvault can detect when PHI is contained in email to ensure additional protection. Commvault's media security prevents unrecognized processes from corrupting the storage system. Encryption of data at rest and in motion also plays an important role. Commvault is exploring a number of partnerships with data management vendors, such as AES and Blowfish, to protect data.

Commvault's health data management platform, along with its built-in security features, helps healthcare organizations prepare for ransomware or other forms of cyberattacks. Frequent backups that are readily accessible and can be quickly restored enable healthcare organizations to refuse to pay a ransom to obtain the key to unlock data encrypted by the criminals. These backups should be tested regularly and stored offline. In the event that a network is compromised, backups and archives stored on the network often can also be compromised. Commvault software also tracks system activity and detects the presence of ransomware on client computers. If unusual activity or ransomware is detected, alerts are automatically sent to system administrators. Depending upon the severity of the warning, systems can be shut down to prevent further damage. As an additional layer of protection against ransomware, Commvault software provides write protection for mount paths from all processes except for Commvault processes.

CHALLENGES/OPPORTUNITIES

The market challenges that Commvault faces can also present opportunities for a company with strong healthcare expertise and a broad market portfolio in the following areas:

- **Security.** As more patient information is moved into EHRs and made accessible both inside and outside the organization via a range of devices, including mobile devices, the risk of a privacy breach rises.
- **Continuous operations.** Many healthcare settings are 24 x 7 operations requiring round-the-clock access to mission-critical clinical applications. In extreme situations, lack of access to essential patient health information could mean the difference between life and death. Thus uptime, computing performance, access to vital clinical and operational data, and reliability are critical considerations when evaluating technology to be used in a healthcare setting.
- **Cost pressures.** More than half of U.S. hospitals are operating in the red. Declining reimbursement rates by private and public payers are exacerbating an already precarious financial position for providers. Careful consideration of the total cost of healthcare IT ownership is essential. More efficient IT operations will enable healthcare organizations to reinvest IT cost savings in more innovative technologies and security.
- **Legacy systems.** Healthcare IT portfolios are notoriously made up of siloed systems, some of which are nearing the end of their product life cycle. In an effort to reduce hardware and software licensing, along with maintenance and support costs, IT staff are endeavoring to rationalize their systems portfolios and decommission these applications. However, the data must be retained and migrated to the replacement systems or at least be accessible in the event it is needed.
- **Competitive portfolios.** Commvault competes with a number of point solutions in the areas of health data management, disaster recovery, and business continuity. Competitors are similarly interested in expanding their solution portfolios in terms of breadth and depth of product capabilities, professional services, and cloud computing options for health data management.

PARTING THOUGHTS

Enterprise and patient health information is the lifeblood of healthcare organizations. Effective health data management enables healthcare organizations to unlock enterprise data trapped in multiple healthcare IT systems, document repositories, PACS, archives, and other information silos. Today's healthcare organizations need a complete view of financial and clinical information, whether they are negotiating at-risk contracts as part of a value-based health strategy or merging with or acquiring other entities to gain economies of scale. In the event of an IT incident or a cyberattack that results in system outages, disaster recovery and business continuity solutions minimize downtime and mitigate damage not only to IT systems but also to the reputations of organizations. More importantly, patient safety is ensured because access to critical patient health information is not delayed.

Healthcare organizations must treat enterprise and patient health information as a strategic asset and protect it accordingly. A solid enterprise data management platform provides the foundation for healthcare organizations to get ahead of the curve on such pressing market trends as personalized medicine, genetics, and predictive analytics. Forward-thinking healthcare organizations will leverage this agility to advance the efficacy and value of care they provide and thus will create a competitive advantage for themselves in an intense data-driven market.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.935.4445
Twitter: @IDC
idc-insights-community.com
www.idc.com