The Data Cure: Information Management in the Healthcare Sector

A white paper for…
Healthcare IT practitioners and stakeholders responsible for defining or deploying their organization’s information governance and eDiscovery policies, or backup and service continuity/reliable recovery strategies.
Table of Contents

Introduction........................................................................................................................................3  
Part One: Information Governance .................................................................................................3  
  Data Growth: Moderation is a Must ...............................................................................................3  
  Defensible Deletion: Know When it’s Time to Trash Data..............................................................5  
  Compliance and Security ...............................................................................................................6  
Part Two: Information Availability ..................................................................................................8  
  Downtime is Money .......................................................................................................................8  
  Service Continuity and Reliable Recovery .....................................................................................9  
  Add it Up: Business Impact Analysis ............................................................................................11  
Part Three: The Benefits of Information Management ......................................................................12  
  Cut Your Costs .............................................................................................................................12  
  Information Over Infrastructure ....................................................................................................12  
  Gain Visibility to Drive Insight ....................................................................................................13  
Conclusion .........................................................................................................................................13  
  Three Truths (Honest) ..................................................................................................................13
Introduction

It’s time for a cure.

Healthcare IT leaders face numerous challenges – tight budgets, inefficient legacy systems, mandates, and enormous amounts of data, from electronic health records (EHRs) to digital images to data from connected machines. Information management solutions help healthcare organizations sort through the data clutter. They help organizations navigate the complicated regulatory landscape that defines the healthcare industry. But too often Information Governance and Information Availability programs often are a low priority. That’s beginning to change because healthcare organizations understand that Information Governance and Information Availability reduce risk, increase efficiency, save money, and improve healthcare outcomes. A progressive approach to information management helps healthcare organizations get data under control within the industry’s tight regulatory and compliance parameters.

Don’t wait – information is your cure.

Part One: Information Governance (That Thing that Only Lawyers Used to Talk About)

“Information governance… should incorporate all the tools needed to better manage information. Implementing an IG strategy will help unlock the value of data and improve decision making.”

– Information Governance Initiative

Data Growth: Moderation is a Must

“As technology magnifies the ability to generate ever more data, Information Governance has presented itself as a critical component to overall organizational health.”

– Samantha Lofton, Chief Risk and Information Governance Officer, Ice Miller LLP

Veritas understands that data represents an organization’s most valuable – and most abundant – asset.

The digital universe is doubling in size every two years and will multiply 10-fold between 2013 and 2020 – from 4.4 trillion gigabytes to 44 trillion gigabytes.¹

Data managed by the average hospital is likely to grow to 665 terabytes this year, up from 168 terabytes in 2010.\(^2\) Kaiser Permanente, the California-based health network, which has more than 9 million members, is believed to have between 26.5 and 44 petabytes of potentially rich data from EHRs.\(^3\) Healthcare used to be awash in paper – now it is awash in digital records, all of which must be stored, secured, and managed in a responsible way to protect patients and healthcare organizations. However, because of the disparate approaches to gathering information, data quality is a massive problem within healthcare.

EHRs “are notorious for data errors due to design flaws, use of templates, use of copy/paste, and use of voice recognition software without content validation. Indeed, the American Health Information Management Association (AHIMA) has acknowledged that inadequate attention to the integrity of clinical documentation in EHRs could compromise their usefulness for patient care, quality reporting, and research. AHIMA notes that information governance is critical to meeting the triple aim of quality care of the individual, population health, and lowering the per-capita cost of health care. The other, more systemic, issue is the lack of standards. Although data standards exist, they have yet to be adopted in the industry-wide way necessary to solve data quality issues.”\(^4\)

The sheer volume and quality of data has the potential to slow healthcare down if they let it.

In addition to patient medical data, employees generate data, too. The average employee creates, sends, receives, and stores conservatively 20 megabytes of data per day.\(^5\) That includes structured data like spreadsheets and data in XML files. It includes unstructured data – data that has no fixed field – in the form of email, email attachments (which are often duplicated), Word documents, and PowerPoint presentations. And it includes video and images – from work and non-work sources like social media sites.

---


By 2017, 79 percent of all data shipped will be unstructured data, according to IDC.

Data doesn’t just grow quickly, it also grows old quickly. Once data has aged 10 to 15 days, its probability of ever being looked at again approaches 1 percent. But healthcare organizations have no choice in the matter – numerous regulations require them to retain data.

State laws generally govern how long medical records are to be retained. However, the Health Insurance Portability and Accountability Act (HIPAA) of 1996 (HIPAA) administrative simplification rules require a covered entity, such as a physician billing Medicare, to retain required documentation for six years from the date of its creation or the date when it last was in effect, whichever is later. HIPAA requirements preempt state laws if they require shorter periods. While the HIPAA Privacy Rule does not include medical record retention requirements, it does require that covered entities apply appropriate administrative, technical, and physical safeguards to protect the privacy of medical records and other protected health information (PHI) for whatever period such information is maintained by a covered entity, including through disposal. The Centers for Medicare & Medicaid Services (CMS) requires records of providers submitting cost reports to be retained in their original or legally reproduced form for a period of at least five years after the closure of the cost report. CMS requires Medicare managed care program providers to retain records for 10 years.

Keeping data around is an idea that can grow as stale as information itself, but healthcare organizations must be mindful of the regulatory landscape.

**Defensible Deletion: Know When it’s Time to Trash Data**

“Data deletion carries a potentially high ROI, but pressing the delete key is much easier said than done.”
– Alan Dayley and Garth Landers, Gartner Analysts

We are conditioned to keep all data because we believe it will be useful… sometime. Some day. Maybe. Healthcare organizations are no different, and they struggle to overcome the “store everything” mentality. Accumulation is easier than organization.

But progressive organizations of all sizes have learned a valuable lesson about data – less is more, and “delete” is not a bad word. Why keep what you don’t need? Clean out the clutter and harness the power of information. That message is even more relevant in healthcare. Arguably no other industry relies more on the timely delivery of information than healthcare. The quick, efficient management and transfer of data directly

---

6 Ibid.
The Data Cure:
Information Management in the Healthcare Sector

affects the quality of care patients receive. “To ensure the availability of timely, relevant data and information for patient care purposes; to meet Federal, state, and local legal requirements; and to reduce the risk of legal discovery, organizations must establish appropriate retention and destruction schedules,” according to the American Health Information Management Association.8

It also turns out an overwhelming amount of data that organizations hold on to has no legal, regulatory, or business value. The Compliance and Governance Oversight Council conducted a survey in 2012 and found that 69 percent of an organization’s stored information is redundant, outdated, or trivial (ROT). It doesn’t add value to an organization.

But in healthcare, simply getting a firm grip on what data an organization has represents a major challenge. Historically, healthcare IT systems have been siloed by department, location, type of service, and type of data, according to scholars.9 Often IT systems complicate rather than support integrated, multidisciplinary care.10

Practicing “defensible deletion” will allow healthcare organizations to shed ROT data. More data does not equal more value, so there is no compelling reason to retain all data. Defensible deletion is at the heart of that approach.

Old habits are hard to break, and data proliferation continues unabated throughout many healthcare organizations. Rather than save all data, healthcare organizations must figure out how to manage data appropriately and discard what they don’t need – within the regulatory framework – so their most important asset doesn’t also become their biggest, costliest burden.

Compliance and Security

“Part of the reason eDiscovery is so expensive is because companies have so much data that serves no business need. Companies are going to realize that it’s important to get their information governance under control to get rid of all the data that has no business need... in ways that will improve the company’s bottom line...” – Judge Andrew J. Peck, U.S. Magistrate

Data has a direct impact on an organization’s compliance efforts. From the Health Insurance Portability and Accountability Act (HIPAA) to Health Information Technology and Information Technology for Economic and Clinical Health (HITECH) – compliance requirements are driving the need to better manage information. More

10 Ibid.
regulations often mean higher costs, but properly maintained data requires less searching and gathering by staff and less review by counsel.

It costs $18,000 to conduct eDiscovery for every 1 gigabyte of data, according to Gartner’s eDiscovery report. The 2012 RAND Report, Where the Money Goes: Understanding Litigant Expenditures for Producing Electronic Discovery, found that the document review process consumes more than 70 percent of every eDiscovery dollar.\(^1\)

Keeping data also has security implications. Improved Information Governance policies mean healthcare organizations keep less data. That translates into reduced exposure – less data means there is less for hackers to steal.

The historic hack at Sony Pictures represents an important example. The theft resulted in the disclosure of thousands of personal emails that simply didn’t have to be retained. Wikileaks has built a searchable database that allows anyone to search through all the emails, and sift through the company’s digital dirty laundry.

The healthcare industry is all too familiar with the risks posed by cyber attacks, and 2015 may well be remembered as “the year of the hack.” It is unlikely the trend will improve in 2016 and beyond. The red flags are more numerous than ever with health insurers and providers being constantly targeted by hackers because of the personal data they collect.

Data about more than 120 million people has been compromised in more than 1,100 separate breaches at organizations handling protected health data since 2009, according to Department of Health and Human Services data reviewed by The Washington Post.\(^2\) Anthem, the nation’s second-largest health insurer, announced in February that hackers broke into a database containing the personal information of nearly 80 million records related to consumers.

\(^1\) Rand Institute for Civil Justice. “Where the Money Goes.”

In short, storing massive amounts of data can place organizations at significant risk – financial, legal, security, productivity, and reputational risk. If your organization is among the hoarders, there is a high likelihood that you are trending toward an information ecosystem that is not sustainable.

The pitfalls are numerous, but organizations can avoid those digital hazards by adopting Information Governance policies that allow them to:

- **Gain visibility and expose risk.** The best way to do that is by understanding an organization’s information ecosystem – determining the age of information, its location, and ownership. Understanding the risk profile of information allows an organization to shift from the “store everything” mentality to a value-focused perspective.

- **Take action and execute decisions.** Once organizations gain visibility into their information footprint, they must take action. Ultimately, the choice is between retention, protection, and deletion. By leveraging critical insights into the value of their information, healthcare organizations can assign classifications, deploy policies, and initiate cleanup. With 69 percent of enterprise information having no legal, business, or regulatory value, it is imperative that organizations clean up their information footprint – sooner rather than later.

- **Assume control and ensure governance.** Information Governance doesn’t occur overnight – it happens when healthcare organizations bring together the right people, process, and technology. Stakeholders must develop sustainable policies that outlast a single project. Technologies that integrate and automate will drastically reduce the manual effort required to manage the Information Governance workflow and improve an organization’s ability to mitigate information risk.

**Part Two: Information Availability**

“Successful and responsible organizations must have the ability to identify, locate, and retrieve the records and related information required to support its ongoing business activities… Having the right information available at the right time depends upon an organization’s ability to nimbly search through enormous volumes of information.” – Association of Records Managers and Administrators

**Downtime is Money**

“A Netflix outage is annoying, but if you can’t access medical records, it could be life threatening.” — Barry Runyon, research vice president, Gartner

Avoiding downtime is crucial because of the potential impact on the delivery of healthcare, and no healthcare organization is immune to service interruptions.
A 2013 study found that 91 percent of all data centers experienced an unplanned data center outage over the previous two years. The cost of downtime adds up fast. Over a 12-month period, outages at 67 data centers cost a combined $46.2 million—or $126,000 per day—according to the study.

In the healthcare industry, the numbers are disconcerting. Healthcare facilities experience 2.7 data center outages over a two-year period and, on average, the industry has the second-longest data center outages, which last 122 minutes per incident. The average financial hit in 2013 was a staggering $669,000 per outage.

Productivity also takes a hit when healthcare organizations experience downtime. IT downtime costs businesses, collectively, more than 127 million person-hours per year—an average of 545 person-hours per company—in employee productivity.

When it comes to downtime, it’s a matter of “when” not “if.” Healthcare organizations must be prepared. Human error, natural disaster, or an IT-related failure can be the culprit. No matter why it occurs, downtime is a stumbling block the healthcare industry must avoid because of the implications on the delivery of care and patient health. Downtime is money—but it could also cost lives.

Service Continuity and Reliable Recovery

“...disaster preparedness and continuity planning [is] an area where healthcare organizations tend to underspend. Business continuity is really a business responsibility, not an IT responsibility.”

Ernie Hood, senior research director for the Advisory Board Co.

Veritas understands healthcare organizations are “always on” and require constant access to data and applications. But organizations with poor Information Availability policies waste time by trying to gain access to data and applications. They also run the risk of losing their information when downtime occurs. Too often they

15 Ibid.
The Data Cure:
Information Management in the Healthcare Sector

rely on rudimentary backup and recovery approaches. Data and applications are too valuable to leave in the hands of run-of-the-mill backup and recovery solutions. Healthcare delivery is too important to rely on standard approaches.

NEARLY HALF WANT HIGH DATA AVAILABILITY

Nearly half of healthcare organizations want high data availability – 99.99 percent availability, or 5 minutes and 15 seconds of downtime annually\(^\text{17}\) – and that's why service continuity represents the best approach to maintain access to information.\(^\text{18}\)

Service continuity means making sure the applications an organization relies on are highly available. When it’s done right, service continuity means organizations never even notice when there’s a disruption or downtime. That’s because all data and applications have been replicated – not just backed up – and everything is stored safely at a reliable recovery site.

Continuous replication is a critical component for organizations to avoid losing information during long disruptions. While many healthcare organizations know they need mature service continuity and reliable recovery solutions, these important initiatives often get overlooked or passed over in favor of other IT programs.

But information management has come a long way in a short period, and Information Availability is easier than ever. As organizations consider service continuity and reliable recovery, it’s vital that they include three elements in the solution they choose:

- Automation is a key pillar of a meaningful service continuity and reliable recovery plan. Manual processes increase costs and reduce efficiency. A fully automated approach allows organizations to manage large enterprises with limited staff and resources and keep pace if data and the number of IT systems continues to grow

- Simplicity also represents a key pillar, and organizations must drive out complexity so they can adopt solutions that work with any IT platform – not just Linux or Windows. Limiting options means limiting effectiveness. Eliminating point products in favor of an enterprise-wide approach helps keep it simple


Organizations also must test their strategies so they can predict the outcome of a disruption and know what's at stake. That's why predictability is the third pillar of an effective service continuity and reliable recovery plan.

"Be prepared," may be the Scout Motto, but healthcare organizations would do well to embrace that timeless aphorism. These days, preparation requires much more than backup, which represents a one-size-fits-all approach, but no two organizations are alike.

Add it Up: Business Impact Analysis

“The BIA becomes the foundation of the plan you will build for your recovery. This is the process that will determine what needs to be recovered and how quickly. It is one of the most difficult tasks to perform and one of the most critical to get right.” – Kelley Okolita, author, “Building an Enterprise-Wide Business Continuity Program”

Being prepared also means organizations must arm themselves with information so they can determine the appropriate course of action. Conducting a business impact analysis before forging ahead will help an organization compile the insight it needs about data and applications. The analysis forces them to determine:

- What are the most critical applications?
- What data sets are most critical?
- Where do those applications and data reside?
- What do Service Level Agreements say about data and applications and what are the expectations for the delivery of those services?

Organizations also must take time to understand their recovery point and recovery time objectives. This is a truly deep dive that will allow healthcare organizations to figure out:

- How long it will take to get data and applications up and running again
- How current the data and applications will be once they are up and running again

An analysis can also enable organizations to consider the many different scenarios that could result in downtime. No service continuity and reliable recovery initiative is complete without the comprehensive internal review that a business impact analysis provides.
Part Three: The Benefits of Information Management

Cut Your Costs

Holding onto data can cost a lot of money.

It costs organizations an estimated $5 million a year to store 1 petabyte of data.\(^1\) Some organizations believe they are addressing the problem by off-loading data into the cloud to cut costs. But cloud storage encourages organizations to retain data. What would you do with $5 million saved through defensible deletion? Think dollars and sense.

Other organizations “tier” their data – rank its value and then store it accordingly. This approach recognizes that not all data is equal. But it also encourages data hoarding and data fragmentation, or the dispersion of data and applications across tiers, data centers, and clouds that make information increasingly complex to manage.

Hoarding data is not a strategy, and organizations shouldn’t waste money holding on to ROT data that provides no value.

Information Over Infrastructure

\[ \text{\$10 spent} = \text{\$6.20 maintenance} = 62\% \text{ of spending on maintenance} \]

Of every $10 spent on infrastructure, $6.20 is spent to maintain it – that’s 62 percent of spending. Infrastructure represents a lost investment, and healthcare organizations can’t afford to waste their resources spending on infrastructure to store data they don’t need.

No project can overlook the potential impact on an organization’s bottom line, and CIOs have a significant role in IT investment decisions and oversight of those investments.

Data-driven policies can help CIOs meet those cost-cutting goals by setting priorities, shedding data, and then reducing infrastructure. CIOs have the power to end the “store everything” approach and save money.

\(^1\) Veritas. “Information Governance: Fighting Back Against the Exponential Data Curve.”
Gain Visibility to Drive Insight

“If you have good information, you can make good decisions. If you have bad information, you’re at risk of making decisions and spending money only to find out later that you didn’t have the right information at your fingertips.” – Lynne Thomas Gordon, CEO, American Health Information Management Association

Big data is all the rage. Just like leaders in any industry, healthcare professionals understand the value data can provide. Analyzing data can help researchers make groundbreaking insights that can improve the quality of care by improving clinical trials or detecting medical problems earlier.

But healthcare professionals must reign in data if they hope to unlock secrets from that information.

By 2020, the percentage of useful data could grow to more than 35 percent, mostly because of the growth of data from embedded systems. According to a PriceWaterhouseCoopers report, 95 percent of healthcare CEOs said they are exploring better ways to use and manage big data.

Availability drives insight. That means knowing where data is. It means being able to access data when you need it. It means faster access and retrieval. High-value data needs to be kept separate from run-of-the-mill information. It needs to be stored in advanced disk storage for quicker retrieval.

Data growth has led to haphazard storage and data fragmentation. Progressive healthcare organizations leverage the power of their information to learn more, improve the quality of care, gain time, and save money – all within the complex regulatory landscape they operate in.

Conclusion

Three Truths (Honest)

Information Governance and Information Availability programs help healthcare organizations overcome data chaos. Veritas empowers them to recognize the value of information management. That’s the easy part. The hard part is the cultural shift required – organizations must overcome the “store everything” mentality.

Organizations that take an information-first approach become masters of their data – not controlled by their infrastructure.

They understand the “three truths” of information management:

- Data isn’t the same as information, and they shouldn’t treat them the same. High-value data requires storage in advanced disk storage for quicker recovery
- More data doesn’t mean more value
- And information is more important than infrastructure

Proper Information Governance policies allow organizations to get the most value out of their data, cut costs, improve efficiency, and avoid risk – financial, legal, security, productivity, and reputational.

Healthcare organizations must apply Information Governance policies to records management, compliance, storage and archiving, risk management, and eDiscovery. And they must understand that storing data that has no value costs a fortune.

Proper Information Availability policies ensure that healthcare organizations can access what they need, when they need it, wherever it resides. Wasting time and money trying to access data is both expensive and frustrating. Healthcare organizations must apply Information Availability policies so they aren’t hobbled by downtime or jeopardizing the quality of care that patients trust them to provide.

Data is your ailment. Information is your cure.

Take control of your information today to help unveil your information potential tomorrow.

For more information, please visit www.veritas.com/solution/healthcare.