IRON MOUNTAIN®

HEALTH IT DATA MANAGEMENT

BEST PRACTICES

INFORMATION IS...**YOUR ADVANTAGE**

Contents

EXECUTIVE OVERVIEW

Unprecedented data growth is proving to be a tremendous challenge for healthcare providers. There are a number of different factors contributing to this data explosion, including the migration to a paperless environment driven by Meaningful Use and ICD-10 implementation, as well as new clinical imaging, diagnostic testing, mobile applications, and remote-monitoring systems.

Although EHR and imaging data are the biggest driving forces behind this increase in data, they are not the only mechanisms responsible for data growth. Today's applications tend to produce more data than ever before.

While data continues to grow at an exponential rate, federal regulations and internal business needs are demanding long-term data retention. Yet while these requirements can create challenges pertaining to storage capacity and costs, there are further, more difficult challenges in play that tend to revolve around data protection and data governance. With the Department of Health and Human Services levying seven-figure fines for data loss, healthcare providers need to evolve their data protection strategy in order to stay ahead of regulatory requirements and to keep on top of data being generated — particularly because of obligatory data retention periods. In addition, as information proliferates, the need for a strong governance framework is essential to move from data silos to enterprise-wide information management.

Iron Mountain recently commissioned a survey with HIMSS Analytics to determine how healthcare providers were dealing with the challenges of data protection amid rapid data growth. A summary of the survey data was presented in the 2014 HIMSS Analytics Report, "The Perfect Storm: Navigating the Health IT Archiving and Data Management Challenge."

The following white paper will discuss the survey findings and provide best-practice strategies to address data growth and the storage and protection of data on a long-term basis.

INFORMATION MAPPING BEST PRACTICES

SURVEY FINDINGS

APPLICATION PROLIFERATION

One of the key factors driving growth in health systems today is the proliferation of applications and their associated data. According to the survey, 90 percent of respondents representing smaller bed segment hospitals (under 150 beds) indicated they support up to 100 applications within their organization, while half of the larger bed segment hospitals (500 beds or more) that participated reported supporting more than 250 applications. The applications represented in the survey included clinical, financial, administrative, and operational systems.

BEST PRACTICES

Health systems need to understand where their information is stored and likewise need to comprehend the relationship of one information system to another. The ability to understand the profile of systems is critical when addressing compliance, litigation readiness, and retention/disposition needs. Information mapping also enables health systems to make timely decisions regarding policy development, data migration, and systems decommissioning.

Many healthcare providers manage information about their systems, enterprise applications, and repositories in an ad hoc fashion. Such strategies lack a visual and dynamic map that could provide visibility into a given health system's high-value and high-risk information, such as protected health information (PHI). This is complicated further when it comes to the rapidly-growing volumes of both structured and unstructured electronic information, including email, text messages, social media, and voicemails. Inefficient manual methods, coupled with a lack of visibility into information, increases a health organization's risk of non-compliance, drives up storage costs, and inhibits Information Governance.

INFORMATION MAPPING BEST PRACTICES

BEST PRACTICES

IDENTIFY

Input or upload key characteristics about your systems, repositories, and applications into a web-based mapping software. (While an Excel® spreadsheet may seem expedient, a more specialized tool allows for more organized, targeted views and is often easier to keep current.) Include information such as system start dates, end dates, and compliance and retention requirements. Use a risk-based approach to begin the mapping process; start where your most high-impact information resides, then move into lower-priority applications. Create a plan to keep you on track.

INTEGRATE

Whenever possible, integrate with your existing software tools using a simple API workflow as well as a web form that gives you the ability to collaborate with system custodians and stay current with regard to system changes.

INTERPRET

Interpret your data using a visual and dynamic map that shows how systems, repositories, and applications inter-relate.

INFORM

Inform your strategic information management roadmap by showing what requires attention. When you know where your high-risk and high-value information is, you have the knowledge you need to inform your strategic roadmap. As a result, the areas requiring your attention are made visible. When considering these areas, be aware you may need additional system controls, backup plans, and/or policy structures because certain information might be PHI or might be considered vital.

INVEST

Invest in the information management areas that will provide you the best return on the value of your information. With the knowledge of what systems you have, what information is in them, how they inter-relate, and who owns them, you will have the facts necessary to make the right investments. These investments may include: system connectors/APIs; human resources to monitor the connectors; control charts to measure performance and recovery time objectives, to track the location of server (i.e., which data center it's in) and how the location relates to your ITIL (Information Technology Infrastructure Library) processes, and to assess related retention schedule rules and regulations; and processes to automate or semi-automate defensible destruction.

IMPLEMENT

Implement and understand the practices and tenets of your ITIL. Anyone who makes buying decisions for your business should understand the value of the information that will populate your organization's information map.

INVITE

Invite professional services partners to accelerate mapping and to manage key updates going forward. This will provide insight and visibility into high-value and high-risk information across your health system. Identify internal information stakeholders and work together to design a map that benefits the collective group and fosters information sharing and cross-collaboration across different teams.

SURVEY FINDINGS

The results of the survey revealed that a large majority of healthcare providers treat all data as active and define it as "stored onsite for immediate access" (Figure 1). This behavior was consistent across three different primary data types: clinical, operational, and laboratory. When the data was further segmented according to hospital bed size, the segment representing the largest hospitals reported a slight reduction in the volume of their active data. The majority of larger hospitals, however, still reported treating their data as active.

The survey also revealed that the data is less likely to be accessed as time progresses (Figure 2). According to the findings, data access decreased consistently across all data types over longer periods of time. For example, by year three of storage, only 22 percent of data was accessed, and nearly 20 percent of the data generated was never accessed at all. This finding holds true regardless of data type (clinical, operational, laboratory).

FIGURE 1: Active vs. Inactive Data

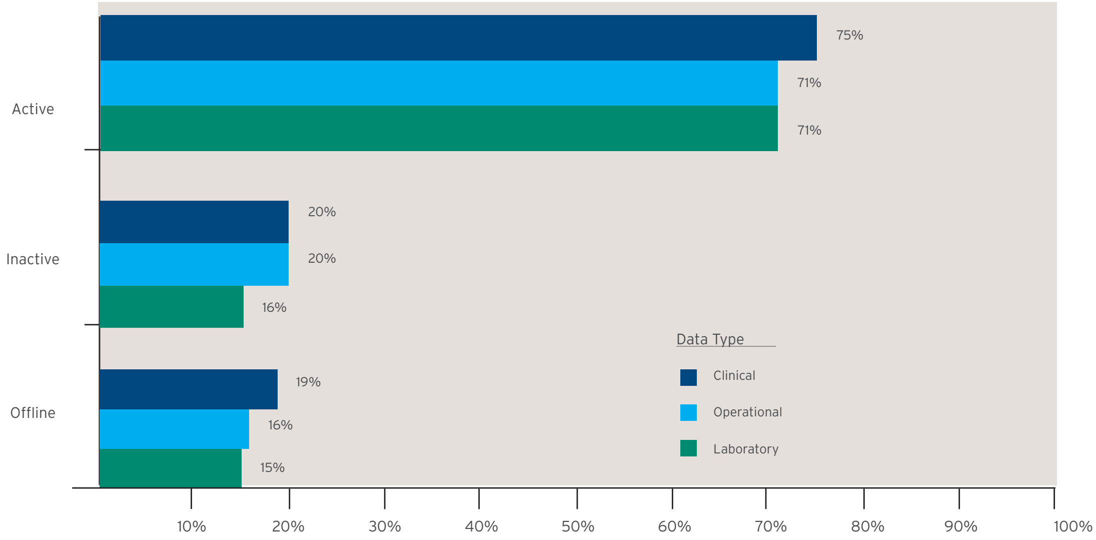
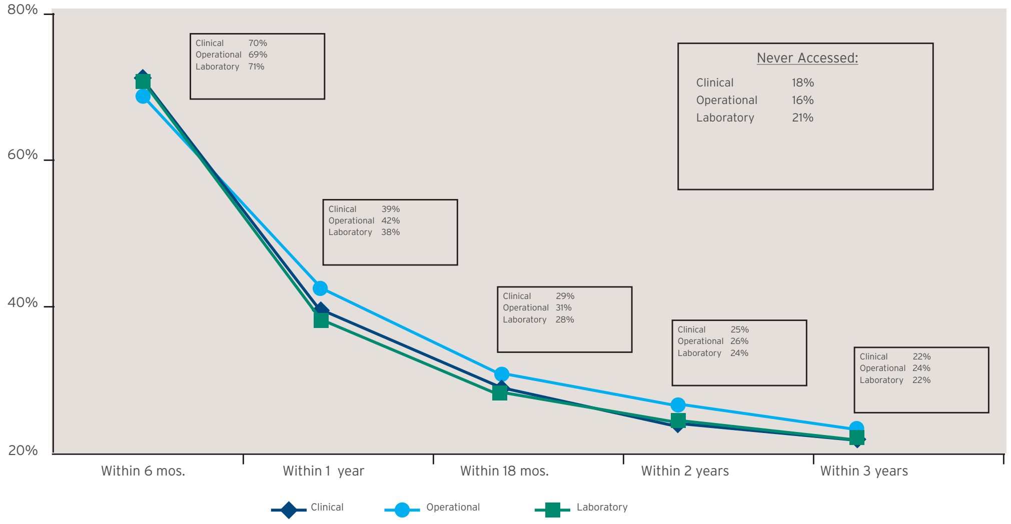


FIGURE 2: Data Access



Respondents were told: Please estimate the percentage of all data (includes active, inactive, and offline) that is accessed at each time point below. N=150

DATA STORAGE BEST PRACTICES

BEST PRACTICES

CONSIDER ALL DATA SOURCES

In order to develop reliable data growth estimates that predict proper data storage needs, it is important to know what type of data a health system has in its possession. In addition to the primary applications and data types, there are multiple sources of new data. Newer technologies – including genomics, digital pathology, biomedical sensors, and proteomics – are becoming more prevalent and are therefore impacting future data growth.

ESTIMATE STORAGE GROWTH

As more organizations continue to compile data volume, the need to properly plan for data storage and archiving will become a necessity. By simply planning for the next storage purchase, organizations are thinking tactically, not strategically. In order to develop an effective data management strategy, it is important to think long term. By determining the data growth projections over the next five years, a health system can better understand how its data storage (and associated infrastructure) will need to evolve over time.

> The balance between speed, access, and cost should be determined for all the varying data types within a specific hospital. This will enable the IT organization to develop the correct tiering model for its data storage when facing increased data growth.

UNDERSTAND ACCESS REQUIREMENTS

A proper data management strategy requires health systems to accurately define how their data should be stored. Because data comes in multiple formats and its requirements differ according to application, a data management strategy will always need to address the varied storage needs for all data categories. The balance between speed, access, and cost should also be determined for all the varying data types within a specific hospital. This will enable the IT organization to develop the correct tiering model for its data storage when facing increased data growth.

BACKUP BEST PRACTICES

SURVEY FINDINGS

Backups aren't only mandated by HIPAA, they're also essential for protecting against loss of data and for maintaining industry compliance. While all of the healthcare providers surveyed reported performing backups within their respective organizations, the methods used varied widely. In addition, nearly half of providers reported using multiple data backup approaches.

The survey revealed that the most popular data protection method involved backing up onsite. This was the preferred option for 25 percent of respondents. In larger bed segment hospitals, 42 percent of respondents indicated they send backup data offsite within a designated distance or region, while one-third of the medium-to-large bed segment hospitals reported using a combination of different approaches for data backup.

BEST PRACTICES

REVIEW EXISTING PRACTICES

When backing up data, it is important to review the existing backup processes and policies for all applications and data types. It is likewise important to determine what needs to be backed up, how it should be backed up, and how long it must be kept.

CLASSIFY DATA

As part of this process, it is important to classify your organization's data. Data classification will help create clarity in terms of risk management and access requirements. Such classification demands that data be segmented into "backup" or "archival" groups. Backup data is characterized as having shorter recovery time and recovery point objectives (RTOs/RPOs,) and is typically considered "dynamic data" (that is, frequently updated or accessed). By contrast, archival data is characterized as being more "static" (having fewer updates) and as being accessed relatively infrequently.

ENSURE A COPY OF DATA IS OFFSITE

Data protection plans that revolve solely around onsite backups are inadequate. In order for data to be properly protected, multiple copies of the data are required: the original data itself, an onsite backup (which is useful for rapid restoration), and an offsite backup (which protects the data against facility-level disasters such as fires or floods). Healthcare providers must also consider the proximity of any offsite copies of their data in the event of a large-scale regional disaster. Any remote data copies can reside on tape or on spinning media in public or private clouds.

TEST THE PLAN

Any test of your backup and recovery processes is time well spent. For backup processes to work efficiently, your staff needs to be trained in how to respond to disasters. Cross-training to prepare for lack of staff availability in a disaster situation is likewise a necessity.

Take a fresh, new look at your existing backup technologies and then assess the strengths and weaknesses of each as honestly as possible.

Backups aren't only just mandated by HIPAA, they're also essential for protecting against data loss and for maintaining compliance.

BACKUP OPTIONS: TAPE AND CLOUD

Tape has been known as "old reliable" in the data storage and backup market and has likewise been recognized for its high capacity and low cost of ownership. However, in recent years, a perception has arisen in the industry that tape has become a slow, expensive, inflexible, and untrustworthy technology.

IN FACT:

1. TAPE IS LOW-COST: LTO-5 tape costs 15 times less than SATA disk for long-term archiving of large quantities of data. In addition, tape's TCO is approximately two-to-five times less expensive than a virtual tape library method of backup.[1]

2. TAPE IS ADVANCING: The Linear Tape-Open (LTO) format has greatly increased tape's capacity (e.g., 6.25TB for LTO-6) and transfer rates (e.g., 400MBps for LTO-6)[2], and the Linear Tape File System (LTFS) has increased tape's flexibility, thereby enabling tapes to be mounted and accessed in a manner similar to disks and to other removable media.[3]

3. TAPE IS RELIABLE: Tape cartridges are two-to-four orders of magnitude more reliable than SATA disk drives, and tape systems have a proven reliability of more than 99.999 percent.[4]

4. TAPE CAN MEET SLAs: Because many organizations keep too much inactive data in their backup stream, they are at risk of missing their specific windows for backup. By properly tiering data and removing inactive data from the backup stream, organizations can leverage tape to meet their SLAs.

Cloud backup is a form of disk backup provided over a given network in which data resides on multiple spinning disks within the cloud. Due to its speed and accessibility, cloud backup is a good choice for datasets that require "anytime, anywhere" access. With the cloud, health systems can:

1. ENABLE MORE FREQUENT BACKUPS: Because the cloud allows you to move data offsite faster and more frequently, it's a good option for data that is constantly changing and/or requires short RTOs and RPOs.

2. INCREASE AUTOMATION: A cloud-based solution increases automation and enables you to perform continuous backups without requiring the physical handling of backup media.

[1] Spectra. "Why Tape is Back (Although it Never Left)." 2012.
[2] Mearian, Lucas. "LTO-6 tape with up to 6.25TB capacity ships." Computerworld. 2012.
[3] Moore, Fred. "Tape Storage Future Directions and the Data Explosion." Horison, Inc. 2012.
[4] Spectra. "Why Tape is Back (Although it Never Left)." 2012.

ARCHIVING BEST PRACTICES

SURVEY FINDINGS

Exponential data growth – combined with the tendency for providers to treat all data as active regardless of its age – will eventually cause challenges in terms of proper protection and management of data. One of the most effective techniques for dealing with such challenges is to implement an archival strategy that moves aging data from the active set to less-expensive archival storage. This technique can also simplify backups, since archive data is unchanging and does not generally need to be backed up in and of itself. In addition, proper archiving is necessary to meet regulatory compliance for most organizations.

The study revealed that nearly half (46 percent) of the healthcare providers surveyed do not have a data archival strategy in place. This also held true for larger facilities with higher bed counts. Only 50 percent of these larger hospitals reported having an archival strategy in place.

When providers were asked whether they had an enterprise archiving strategy, only 31 percent of those surveyed indicated that they had such a system, while 29 percent reported having a plan to implement such a strategy. Still, 26 percent indicated that they have no such strategy in place whatsoever.

BEST PRACTICES

Healthcare providers should consider archiving as a part of their comprehensive data management strategy. Incidentally, it is important to treat archiving and backup as distinct disciplines. Any thorough data protection strategy should include specific plans regarding which content should be archived and which should be backed up.

While the prospect of shifting away from your organization's existing storage model can seem daunting, there are steps you can take to begin this process. These include the following:

BUILD AN INFORMATION GOVERNANCE TEAM

It's likely there isn't a single individual within any given health system that has enough knowledge to make a definitive decision about which data should be considered archival and which should not. This is especially true for large facilities with high bed counts. Therefore, the first step in establishing a comprehensive archival strategy policy is to build an Information Governance team. This team should consist of representatives from IT, compliance, and legal, as well as from any other required departments.

It is important to treat archiving and backup as distinct disciplines. Any thorough data protection strategy should include specific plans regarding which content should be archived and which should be backed up.

SELECT AND ORGANIZE COMPLIANCE AND RETENTION REQUIREMENTS

Once the Information Governance team has been assembled, it must work to assess the organization's data retention requirements. These requirements should be evaluated by reviewing HIPAA regulations, any applicable state laws, and the health organization's own internal retention standards.

EVALUATE THE DATA

Once the Information Governance team has assessed the data retention requirements, the health provider's data must be evaluated to determine what information needs to be archived as well as how and where it should be retained. Not all archive data is the same, and different applications have different definitions of what archiving actually means. For some applications, archiving is seen as another tier of storage, with data that is readily accessible at the click of a button. For other applications, archiving is defined as having the data offline but still accessible by the end users after a slightly longer retrieval time. In either model, it is possible to segment storage to preserve data in the appropriate storage tier. There is, however, an access/cost tradeoff that needs to be taken into account as an archiving strategy is developed.

TEST THE ARCHIVAL PROCESS

It is important to regularly test any and all access to archival data. In some cases, testing will require a simple push of a button. In other cases, it may require the retrieval of tapes from an offsite location and the running of an application that may not be used on a regular basis. In either case, it is important to regularly test the processes of accessing data from an archive location.

ARCHIVAL BENEFITS:

- **Business Intelligence:** Gain insights from legacy information and deliver more comprehensive care
- **Compliance:** Address retention requirements and accelerate discovery
- **Reduce Cost:** Reduce primary storage and simplify storage management

SURVEY FINDINGS

Healthcare providers have learned the hard way that the consequences of not being able to recover from a disaster (which include the loss of electronic protected patient data) far outweigh those of missing the occasional backup window.

Because disaster recovery is so critical in healthcare, nearly two-thirds of the healthcare providers surveyed reported having a formal disaster recovery and business continuity strategy in place. In addition, respondents indicated that the majority of these strategies comply with HIPAA guidelines.

Virtually all survey respondents who reported that they have a business continuity strategy likewise indicated that their strategy included protocols for clinical, operational, and laboratory data, as well as all respective applications. Approximately one-third of respondents reported having an RTO metric within their organization, while less than one-third reported using an RPO metric.

Out of all of the respondents surveyed, 21 percent stated they have experienced a disaster recovery or data loss event, while the majority (69 percent) stated they have not. The remaining 10 pecent were unsure or chose not to respond.

BEST PRACTICES

For covered entities, developing a formal disaster recovery and business continuity plan is mandatory. HIPAA requirement 164.308 (7) (i)* states that all covered entities must "establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health records." The steps on the following page are important guidelines for creating a comprehensive disaster recovery and business continuity plan.

*Source: Department of Health and Human Services.

For covered entities, developing a formal disaster recovery and business continuity plan is mandatory.

DISASTER RECOVERY AND BUSINESS CONTINUITY BEST PRACTICES

CREATE HIPAA-REQUIRED PLANS

Among other things, the implementation specifications for this regulation require protected entities to do the following:

– **Implement a Data Backup Plan** (Required): Establish procedures to create and maintain retrievable exact copies of electronic protected health information.

– **Create a Disaster Recovery Plan** (Required): Establish (and implement as needed) procedures to restore any loss of data.

– **Implement an Emergency Mode Operation Plan** (Required): Establish procedures to enable continuation of critical business processes to maintain the security of electronic protected health information when operating in emergency mode.

In order to create these necessary plans, health systems need to evaluate their data protection and business continuity requirements and establish a set of goals. In addition, healthcare providers must review their existing policies and procedures to determine whether or not they adequately address the stated industry requirements.

HIPAA does not offer any specific recommendations or requirements as to how healthcare providers must implement their plans once these plans are created. It is up to each individual provider to develop policies and procedures that are appropriate for their specific organization.

ESTABLISH A REMOTE LOCATION

For true business continuity, it is important to establish a remote location where critical systems can be run offsite if necessary. Consider where such a facility should be located based on distance from the health system itself and on the required level of access for the appropriate staff.

CONTINUALLY TEST AND MODIFY

Test and modify the plan as your IT environment evolves. Testing involves measuring responses and can be a learning experience that can aid in improving processes.

LEVERAGE EXPERTS

Review your policies and processes with data protection and business continuity experts. Leverage both internal and third-party experts in an effort to establish a comprehensive set of policies. Make sure that everyone involved has a healthcare background and understands HIPAA requirements.

CONCLUSION

Health systems are expected to achieve Meaningful Use and ICD-10 implementation while keeping on top of technology that will improve patient experience, system efficiency, and safety. The resulting data created through these initiatives drives the need for providers to develop an effective information lifecycle management strategy.

Providers should take action immediately and begin developing a plan to address their explosive data growth and long-term retention requirements. It is unrealistic to expect that the current model of treating all data as active can scale to accommodate continual data explosion. Even if raw storage capacity is not an issue, backup, archival, and disaster recovery planning become much more challenging as the dataset grows.

If a steady increase of data remains unchecked, healthcare providers may find themselves unable to recover from a disaster in a timely manner – if they can recover all. The end result can include hefty government penalties, loss of patient trust, and, depending on the nature of the incident, civil litigation. To mitigate these risks, the best strategy for coping with the demands of protecting a large dataset is to reduce the size of the dataset through the use of automated-archival and effective data lifecycle management policies.

By leveraging these best practices, providers can also manage their data as a strategic asset, thereby augmenting its value. These strategies also support the journey to an enterprise-wide Information Governance framework. With comprehensive and consistent application of policy across the organization, providers can achieve higher levels of integration and interconnectivity.

ENGAGE PARTNERS

Although it is possible that larger healthcare providers may have experts on staff to address data management challenges, most facilities will likely need to seek outside help. When doing so, it is important to seek advice from qualified experts that have healthcare experience and a comprehensive understanding of HIPAA and the HITECH Act. By consulting with such experts, the health system can make better use of its resources for more strategic initiatives and improve its ability to deliver superior patient care.

BEST PRACTICE RECOMMENDATIONS CHECKLIST

INFORMATION MAPPING

- ✓ Identify information and where it lives
- ✓ Collaborate with system custodians to stay current
- ✓ Prioritize high-value, high-risk information
- ✓ Understand practices and tenets of ITIL

DATA STORAGE

- ✓ Consider all data types
- ✓ Estimate storage growth
- ✓ Understand access requirements

BACKUP

- ✓ Review existing policies
- ✓ Classify data
- ✓ Get a copy of data offsite
- ✓ Regularly test your backup plan

ARCHIVING

- ✓ Build an Information Governance team
- ✓ Collect and organize retention requirements
- ✓ Evaluate your data
- ✓ Test your archival process regularly

DATA RECOVERY AND BUSINESS CONTINUITY

- ✓ Create HIPAA-required plans
- ✓ Establish a remote location
- ✓ Test and modify your plan continually
- ✓ Leverage experts

For More Information:

» Visit our webpages: **www.ironmountain.com/healthIT**

» Follow us on Twitter: **@IronMtnHealth**

» Read our Blog Series: **blogs.ironmountain.com/healthcare**

IRON MOUNTAIN®

ABOUT IRON MOUNTAIN. Iron Mountain Incorporated (NYSE: IRM) is a leading provider of storage and information management services. The company's real estate network of over 67 million square feet across more than 1,000 facilities in 36 countries allows it to serve customers around the world. Its solutions for records management, data management, document management, data center management, and secure shredding help organizations to lower storage costs, comply with regulations, recover from disaster, and better use their information. Founded in 1951, Iron Mountain stores and protects billions of information assets, including business documents, backup tapes, electronic files, and medical data. Visit www.ironmountain.com for more information.