E-Guide

MANAGING DATA AND DEVELOPING A HIPAA-COMPLIANT STORAGE PLAN

TechTarget | SearchHealthIT

HEALTH REFORM AND the meaningful use program will make it critical for hospitals to develop effective data management strategies. Read on to learn more about this and how establishing HIPAA-compliant storage plans requires a three-pronged approach to meet disaster recovery, data backup and emergency operations criteria.

TIP: AS PRESSURE GROWS ON HOSPITALS, MANAGING DATA BECOMES PARAMOUNT

Ed Burns

Unless healthcare organizations put effective strategies for managing data into place, they could face major challenges in successfully navigating federal initiatives and operational improvements in the years ahead. Many might not even be able to keep their doors open.

In his keynote address at the Institute for Health Technology Transformation's Health IT Summit in Boston, Scott Lundstrom, group vice president at IDC Health Insights, said he believes half of existing hospitals will go out of business within the next 10 years. He cited a number of factors, including the focus on accountable care through the health reform law and the meaningful use incentive program, as obstacles for organizations. Whether it's the move toward accountable care, quality initiatives or technology programs, the ability to manage data effectively will help providers deal with these challenges, he said.

Still, hospitals have a long way to go. Healthcare providers traditionally

Home

Tip: As pressure grows on hospitals, managing data becomes paramount

Tip: Developing a HIPAA-compliant storage plan

have done a poor job of selecting and managing technology investments, Lundstrom said. They often don't even know how many servers they have or which applications are running on them.

The consequences of poor planning for managing data will first start to show as providers transition to accountable care, Lundstrom said. This model of care relies on engaging patients, managing the health of populations and providing targeted preventive health measures. All these put a premium on leveraging data to its full potential.

For Lundstrom, this situation presents a good opportunity for hospitals to move to cloud services. Rather than buying servers that depreciate in value rapidly or investing staff hours in setting up networks and configuring applications, hospitals can get third-party cloud vendors to do the work for them. The key is that the vendor be willing to sign a business associate agreement (BAA). Signing a BAA was an issue when vendors first started showing up on the scene, but there are now more healthcare-focused technology companies that are willing to sign such an agreement.

"Organizations that remediate and plug-and-patch in a traditional model are going to fail," Lundstrom said. "You can't remediate your core stack and launch a patient portal and do remote visits all at once. You can have partners

Home

Tip: As pressure grows on hospitals, managing data becomes paramount

Tip: Developing a HIPAA-compliant storage plan

do that. To think that we can make modest, incremental changes to a system that is already letting us down is naïve."

About 80% of healthcare providers lack a strategy for managing data, which prevents them from being able to accomplish many of their goals, said William Hudson, senior healthcare strategist at VMware. "Until we get to the point where we can create a real strategy, we're not going to get to where we want to go," he said.

Part of the problem is that the volume of data that hospitals create and manage is growing exponentially. This makes it difficult to identify pieces of information that can be used in direct patient care, financial risk management or patient engagement. A hybrid strategy might be best for managing all this data, Hudson said, because some information, such as patient records, needs to be easily and quickly accessible, while other information, such as log files, needs to be accessed only occasionally. Frequently accessed data could be stored on enterprise servers, while less critical data could be stored off-site through cloud storage providers.

Developing a standardized IT infrastructure could be one way to manage data effectively, because it will enable data to be shared across platforms. There might be many ways to accomplish this, but Cara Babachicos, CIO of community hospitals for Partners Healthcare, said her organization is going with an enterprise-wide Epic installation. This will improve standardization across many care settings, making it easier for providers to get the information they need when they need it, she said.

Babachicos still expects challenges, however. The entire health system will use the same standards, but there still are different ways of interpreting standards. Additionally, IT workers will have to think about how data is organized across the system, which is no small feat. "Just purchasing a one-vendor system will not get you there," she said.

Ultimately, developing strategies for managing data could be more of a cultural challenge than a technical one. Jeffrey Brown, CIO at Lawrence General Hospital in Massachusetts, said cloud storage makes a lot of sense for some things, disaster recovery, for example. But moving to the cloud requires IT staff to give up some measure of control over services they've managed for decades. Sometimes workers may be slow to get on board with the change. One of his hospital's recent programs to increase cloud adoption focused mainly on education, he said.

TIP: DEVELOPING A HIPAA-COMPLIANT STORAGE PLAN

Brien Posey

An important part of establishing and maintaining HIPAA compliance is the creation of a storage plan. Although the HIPAA regulations do not specifically require a storage plan, HIPAA Part 164.308(a)(7)(i)does require your organization to develop a contingency plan. Specifically, this regulation states:

> Standard: Contingency plan. 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 information.

Part ii outlines the implementation specifications for this regulation. HIPAA requires the creation of five separate documents as outlined below:

> (ii) Implementation specifications:
> (A) Data backup plan (Required). Establish and implement procedures to

Home

Tip: As pressure grows on hospitals, managing data becomes paramount

Tip: Developing a HIPAA-compliant storage plan

create and maintain retrievable exact copies of electronic protected health information.

(B) Disaster recovery plan (Required). Establish (and implement as needed) procedures to restore any loss of data.

(C) Emergency mode operation plan (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

(D) Testing and revision procedures (Addressable). Implement procedures for periodic testing and revision of contingency plans.

(E) Applications and data criticality analysis (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components.

A storage policy is made up of documents A, B, and C ("Data Backup Plan," "Disaster Recovery Plan" and "Emergency Mode Operation Plan"). The "Testing and Revision Procedures" and "Applications and Data Criticality Analysis" documents are required by HIPAA, but are beyond the scope of this article.

Home

Tip: As pressure grows on hospitals, managing data becomes paramount

Tip: Developing a HIPAA-compliant storage plan

A WORD ABOUTHIPAA COMPLIANCE

As evident in the section above, the HIPAA requirements for the various plans are rather vague. HIPAA states what each of the three plans must accomplish but leaves the details to each individual organization's own discretion. Therefore, the challenge becomes creating a Data Backup Plan, Disaster Recovery Plan, and Emergency Operation Plan that not only meet HIPAA's required objective but also fit into your own, unique organizational logistics and budgetary constraints.

DATA BACKUP PLAN

As the name implies, the Data Backup Plan reflects a healthcare organization's plan for backing up systems containing patient health data. The first thing that administrators must understand about the Data Backup Plan (and the Disaster Recovery Plan and the Emergency Mode Operation Plan) is that simply developing a document for the sake of compliance is not enough.

As an administrator, you are free to back up your data in any way that you see fit as long as your backup methodology fulfills the HIPAA requirement to create and maintain retrievable exact copies of electronic protected health information. However, your backup plan must accurately document the backup

Home

Tip: As pressure grows on hospitals, managing data becomes paramount

Tip: Developing a HIPAA-compliant storage plan

methodology that you are using. It is expected that your Data Backup Plan will be a living document. In other words, as your backup requirements and methodologies evolve over time, the Data Backup Plan must be kept up to date so that it always matches the backup procedure that is being used.

The exact nature of a Data Backup Plan's contents will vary from one health care organization to the next. Generally, however, the plan should document the backup hardware and software that is being used as well as outline the backup procedures in granular detail.

It stands to reason that a Data Backup Plan would document the organization's tape rotation scheme, but the plans typically provide a greater degree of depth with regard to the backup process. For example, the plan might outline the tape-labeling scheme as well as the tape retention cycle. Typically, a Data Backup Plan will also document methods used for storing backup copies off-site as well as for testing your backups. Your Data Backup Plan should ideally also document the schedule for any backup-related maintenance, such as cleaning tape drives.

DISASTER RECOVERY PLAN

An organization's Disaster Recovery Plan is a natural complement to its Data

Home

Tip: As pressure grows on hospitals, managing data becomes paramount

Tip: Developing a HIPAA-compliant storage plan

Backup Plan. After all, backing up data is only one step in protecting a health care organization's systems against failure. It is critically important for administrators to know how to restore the backups should the need ever arise.

As is the case with the Data Backup Plan, the Disaster Recovery Plan is intended to be a living document that is updated on a regular basis. The document must accurately reflect the procedures that will be used to recover electronic health records (EHRs) and other types of critical information after a disaster.

As you develop a Disaster Recovery Plan, the document's structure should lend itself to being easily updatable. Typically, the document body contains nontechnical information that is relatively static (but that must be kept up-to-date nonetheless). Technical information updated on a regular basis is typically included in the document's appendix.

The nontechnical portion of the Disaster Recovery Plan should discuss the logistical aspects of the disaster recovery process at length. For instance, many disaster recovery plans begin by presenting an overall recovery strategy. It is important to keep in mind that a good disaster recovery plan should discuss a variety of recovery operations. For example, a disaster recovery plan might discuss bare-metal server recovery, recovery of a virtual machine, file-level recovery, application recovery, Active Directory recovery, and the recovery

Home

Tip: As pressure grows on hospitals, managing data becomes paramount

Tip: Developing a HIPAA-compliant storage plan

of infrastructure components such as DNS and Dynamic Host Configuration Protocol (DHCP) servers.

Disaster recovery planning isn't always about an organization's ability to restore a backup. Sometimes disasters occur that do not directly impact servers or storage components. For example, the failure of a network switch could be considered a disaster, and a contingency plan should be outlined within your disaster recovery plan even though no data will need to be restored.

In addition to discussing recovery strategies, a good Disaster Recovery Plan should also provide the contact information, roles and responsibilities of those who will be involved in the recovery process. Some health care organizations even go so far as to document the vendors who may be called upon to provide supplies or technical assistance.

EMERGENCY MODE OPERATION PLAN

The third document making up a healthcare organization's storage policy is the Emergency Mode Operation Plan. The Disaster Recovery Plan is designed to deal with data recovery after a small-scale disaster, such as the loss of a server or a storage array failure. In contrast, the Emergency Mode Operation Plan deals with a health care organization's ability to cope with larger-scale

Home

Tip: As pressure grows on hospitals, managing data becomes paramount

Tip: Developing a HIPAA-compliant storage plan

disasters, such as the destruction of the organization's primary data center.

The bulk of the Emergency Mode Operation Plan is nontechnical in nature. Its primary purpose is to document the organization's policies and resources used in an emergency failover to an alternate data center. For example, the Emergency Mode Operation Plan should document the systems that contain critical data and the systems that need to be brought online in order to achieve continuity of business (or at least skeleton functionality).

The Emergency Mode Operations Plan should also document the location of the alternate data center and the computing and storage resources that are available for hosting critical workloads during times of disaster. Additionally, the Emergency Mode Operation Plan should list the members of the disaster recovery team and their responsibilities with regard to restoring functionality.

One easily overlooked aspect of the Emergency Mode Operation Plan is having the plan accessible from outside the data center. After all, the Emergency Mode Operation Plan does no good if the plan itself is destroyed along with the data center. Typically, an Emergency Mode Operation Plan should include a statement indicating that each member of the disaster recovery team must keep a copy of the plan off-site in a secure location.

Home

Tip: As pressure grows on hospitals, managing data becomes paramount

Tip: Developing a HIPAA-compliant storage plan

CONCLUSION

As you develop your storage policy, it is important for Data Backup Plan, Disaster Recovery Plan, and Emergency Mode Operation Plan to complement one another and to collectively form a comprehensive disaster recovery strategy. Just as importantly, the three plans must accurately reflect the procedures that the organization actually uses. As these procedures evolve, the various plans must be updated in order to remain relevant and accurate.

FREE RESOURCES FOR TECHNOLOGY PROFESSIONALS

TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web's largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more —drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

WHAT MAKES TECHTARGET UNIQUE?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.