Get Smart About Cloud Storage and HIPAA

Healthcare organizations should take advantages of cloud storage technology, but they also need to monitor risks and maintain HIPAA compliance.
HIPAA-Compliant Cloud Storage Seen Through My Kid’s Data

I had a chance recently to download some of my son’s electronic medical records from the cloud of a Boston health system.

The data was mainly bloodwork results, which sure seem like a logical use of cloud storage. I suppose a cybercriminal prowling the web might find some of the information in the records valuable—for example, the brands of allergy medicines a kid might take.

At this point, HIPAA-compliant cloud storage comes into play for providers. As Uncle Sam pursues HIPAA audits of healthcare organizations—see News Writer Shaun Sutner’s piece in this handbook on the government’s audit protocol—healthcare providers must show they conducted related risk assessments, including for third-party business associates.

As a parent, I would not be happy if I discovered that I could not access my son’s records after a data breach, such as a ransomware attack. Part of HIPAA-compliant cloud storage reaches into disaster recovery steps, as Sutner outlines in another story. A health system he talked to keeps backup locations at two hospitals and also uses an off-site colocation center with other organizations.

Although I am not employed by the federal government, I suspect a HIPAA auditor would like the type of setup described above.

Contributor Reda Chouffani wraps up the handbook by examining the pros and cons of personal cloud storage used by clinicians. While IT departments are rightfully on guard to defend HIPAA-compliant cloud storage, such services—when maintained properly—can bring cost savings to hospitals and practices.

As a parent, I would not be happy if I discovered that I could not access my son’s records after a data breach.
I’d add convenience to the list of benefits, too, given that I downloaded years’ worth of my kid’s health exams in about 30 seconds. The reward in this case is clear; the risks may be less certain, although we all know they exist.

As time passes, the cloud contributes more and more to our everyday lives. I speak, if not for everyone, for many healthcare consumers who appreciate the technological steps providers are taking to keep cloud storage safe.

What positive experiences have you had with cloud storage of medical data? Let me know by email at swallask@techtarget.com or chime in on Twitter: @Scott_HighTech.

Scott Wallask
Editorial Director
SearchHealthIT
Healthcare organizations and their business associates now have a detailed roadmap for documenting their compliance with HIPAA privacy and security rules.

The Department of Health and Human Services Office for Civil Rights’ (OCR) HIPAA audit protocol lays out procedures for documenting everything, from authentication rules and security risk assessment to policies for employee access to electronic protected health information (ePHI). Each compliance area is keyed to the relevant section of the HIPAA law.

“It’s fairly clear. The Office for Civil Rights just wants to make sure providers are aware of all their obligations under HIPAA and are performing the minimum requirements under HIPAA,” said Dan Brown, a healthcare lawyer with the firm Taylor English Duma LLP, based in Atlanta.

The HIPAA audit protocol guidelines differ significantly from rules released in 2012 for an earlier pilot round of audits because they spell out for the first time compliance obligations for business associates, such as billing, transaction processing and medical supply companies.

This HIPAA audit protocol is also the first since the 2013 HIPAA Omnibus Rule, which gave significantly more HIPAA enforcement authority to OCR and expanded patients’ rights to their health data.

Also, with this HIPAA audit protocol, OCR is “signaling that it will also look at small physician practices, not just the big boys,” Brown said.

TOUGHER ROAD FOR PRACTICES
Brown and other HIPAA experts said many smaller physician practices may not be adequately prepared for HIPAA audits—or even aware of them—though most big
healthcare systems should be able to navigate them with little trouble.

However, the OCR protocol takes into account the size and resources of an organization. For example, there is no requirement that providers encrypt ePHI, only that health data is protected from theft, unauthorized access or loss.

Nevertheless, for small physician practices, “It can definitely be overwhelming” to respond to an audit, said Chuck Burbank, CISO at Fair-Warning Inc., a provider of healthcare information security and consulting services based in Clearwater, Fla.

Burbank noted the new protocol is much longer and more far-reaching than the last one. It also has many apparently overlapping sections, so if an organization is deficient in one area, it could likely fall short in several others as well, Burbank said.

Also, one big challenge organizations of all sizes might confront is being able to quickly provide all required documents. They may not all be digitized, or even if they are, they do not reside in a centralized location.

“If it were me, I’d be trying to pull together all the documents rights now,” said Burbank, a former information security manager for a physician practice with 400 doctors. “OCR has given out all the instructions. It’s like an open-book test.”

WHAT TO EXPECT FROM HIPAA AUDITS

Experts said the bulk of the protocol deals with ensuring that HIPAA-covered entities have updated policies and procedures for matters such as training, access to ePHI, risk assessment and breach notification, rather than strictly technology issues.

Also, the audits will focus much more on the risk of compromise of data, rather than risk of harm from data breaches—the main emphasis of the pilot audits.

“I can have the best perimeter access protection and firewalls, but if employees click on phishing emails, I’m sunk,” Burbank said.

“What the OCR is looking for is something they term a culture of compliance,” said Michael Brody, HIPAA compliance specialist for Webair Internet Development Inc., a cloud hosting company based in Garden City, N.Y.
“They want to see that organizations are doing everything reasonable to protect data.”

With the April 1 publication of the audit protocol—the development of which OCR has cited as a reason for delays in this first formal round of audits—the HIPAA audit process is now underway in earnest. Observers expect 200 to 500 organizations to be audited.

Key areas OCR will be scrutinizing in audits expected to start this year, and likely continue into 2017, include the following:

- Breach notification procedures. Do organizations have policies and procedures for notifying patients and the public after a breach?

- Protocols for protecting data in the event of a breach.

- Risk assessment. Have providers and other covered entities performed thorough analyses of the risk of data breaches or losses?

- Whether business associates are in compliance with HIPAA. In the pilot audit round, OCR only asked providers for lists of business associate contracts.

- Employee training policies.

- Whether organizations have security officers in place.

- Mechanisms and procedures for promptly providing health data to patients.

- Policies for controlling employee access to ePHI. —Shaun Sutner
Storage Options Evolve for Healthcare Disaster Recovery

**IF THINGS GO** bad for its data network, Virtua Health System’s IT managers are confident they can rely on a well-honed disaster recovery system to deal with the problem.

Virtua started building its healthcare disaster recovery (DR) system in the early 2000s by securing support from the C-suite for a storage architecture that could quickly get the provider back in business in case of a network failure or cyberattack.

“Since then, we’ve transitioned from traditional backup to being focused on redundancy and high availability as we enter this almost paperless world,” said Tom Gordon, Virtua’s CIO.

**HEALTHCARE DISASTER RECOVERY EVOLVING**

DR in healthcare isn’t new. HIPAA has, since its inception in 1996, required healthcare organizations to maintain healthcare disaster recovery plans for backup and recovery of health data, although there are no requirements for recovery time.

Now, however, there’s exponentially more data to store and protect since the near universal digitization of health records wrought by the 2009 HITECH Act’s EHR incentive program. The health IT world has also been seized by a profound sense of urgency about DR amid nonstop cyberattacks and ransomware attacks on health data in recent years by hackers, insider data thieves and foreign state actors.

Another driver for healthcare disaster recovery is the new round of HIPAA audits now underway by the Department of Health and Human Services Office for Civil Rights.

As for Virtua, the southern New Jersey health system uses a three-data center setup for its DR and works with security consultants from CynergisTek Inc. to test it regularly.
Virtua maintains production and backup locations on premises at two different hospitals within its own network, and an off-site recovery center collocated with other organizations’ servers a safe 70 miles away from its main hospital.

**HYBRID CLOUD FOR DISASTER RECOVERY**

Unlike with the hybrid cloud DR systems—which house production on premises and backup in the cloud—that are fast becoming popular with healthcare provider organizations, Virtua still owns and maintains dozens of its own backup servers at the “colo” center. That colocation paradigm is still common in healthcare.

More than a decade ago, Gordon said, there was a trust factor for many providers considering cloud storage and disaster recovery. They were wary of multi-tenancy in a public cloud and the potential for security problems that could come with comingling their patients’ protected health information with data from other organizations.

Now, Gordon said, his organization is envisioning someday replacing its DR infrastructure with a cloud system in which the cloud hosting company owns the hardware and essentially leases space in its cloud to the healthcare provider.

Since the HIPAA Omnibus Rule of 2013 extended HIPAA compliance requirements to cloud vendors, many cloud hosting companies and consultants have been selling to the healthcare industry. More healthcare organizations are becoming comfortable with cloud vendors’ security assurances.

“I do feel that hybrid cloud and cloud is the wave of the future,” Gordon said.

**HOT SITES, PAPER FADING**

Another healthcare disaster recovery format that is receding in popularity is subscription-based “hot sites,” off-site physical locations to which providers can move IT operations after a disaster, according to Angela Devlen, a healthcare disaster recovery and business continuity consultant for Wakefield Brunswick, based in Tampa, Fla.

In the past, hospitals could move paper
records to the hot site and try to keep serving patients while rebuilding the electronic information. Now, while paper still exists at many providers, members of the new generation of clinicians and health IT professionals generally are not familiar with printed records as a primary resource, Devlen noted.

“Ten years ago, we could more easily go back to paper,” Devlen said. “The recovery time tolerance was much longer. Now, recovery time is much less, measured in minutes and hours.”

Bryson Hopkins, director of global solutions architects at Equinix, a data center and colocation and cloud consulting firm, said healthcare organizations have only started moving substantially toward the cloud over the past 18 months.

HEALTHCARE WARMING TO CLOUD
They are also starting to use cloud for everyday applications and patient care and are getting comfortable with the cloud and its cost-saving and data-sharing benefits, Hopkins said.

For example, “some of these urgent care doctor practices are starting to embrace the use of office automation stuff from [cloud vendors],” Hopkins said.

He said providers like these are asking themselves: “How can we also be a little more survivable when things [like cyberattacks] start happening?”

The new generation of clinicians generally is not familiar with printed records.

“It’s no longer people trying to set up stuff in their office,” he said. “They’re more comfortable with DR in the cloud.”

Despite the growing popularity of cloud technologies, Hopkins predicted that many storage applications and daily workflow applications, especially those that require super-fast response, will continue to be handled on premises for a long time.

WARINESS AND WELCOME FOR CLOUD
Virtualization expert David Davis—a co-founder of ActualTech Media LLC who has...
written about healthcare disaster recovery—said when considering DR systems, organizations should evaluate risk, or how much data they’re willing to lose, as well as recovery time.

They should also carefully review contracts for security provisions and be attentive on their side to building networks and data pipelines that can handle the cloud traffic, he said.

If organizations are buying disaster recovery as a cloud service, the faster they want data recovered from the cloud and less they’re willing to lose if a failure occurs in their data center means higher costs, especially for high-bandwidth data such as medical images.

“It’s just going to cost a lot more money, a lot more bandwidth, a lot more storage,” Davis said.

Davis noted that at the same time that many organizations are opting for some kind of cloud storage, others are moving back to on-premises approaches after absorbing huge bills from public cloud vendors.

Nevertheless, the advantages of cloud DR can be compelling, Davis said. They include pay-as-you-go and charge-back to assess usage time, scalability and agility, and eliminating hardware overhead.

As for big healthcare providers’ long-standing wariness of the cloud, Davis said: “I don’t blame them.”

“Any company should be leery of cloud to some degree. Initially, we have high expectations. We think it’s just always on and perfect,” he added. “That’s not to say they don’t also have problems. And when they have problems, they’re massive. You lose a lot of control.”

—Shaun Sutner
Attain HIPAA Compliance With Personal Cloud Storage

The adoption of cloud storage among end users has surged in recent years. With the different options available in the marketplace, the task of managing and ensuring compliance with HIPAA has forced several in IT to take a strong stand against—and in some cases, completely block—individual cloud storage options. So what can IT do to take advantage of personal cloud storage while still meeting true HIPAA compliance requirements?

The constant threat of data leaving the safety of the hospital network has made it very difficult for storage cloud providers to gain a wider acceptance in healthcare. Not only is health IT concerned about the compliance of where the data resides, but it is also fearful that the end users’ access to the data through the cloud providers outside the hospital may accidently cause a breach.

Despite the uncertainties around cloud storage options, the online service holds some advantages that can prove useful to end users and deliver cost savings to hospitals and large healthcare organizations. Users are constantly storing much of their data on local machines. With the risks associated with data loss, most IT departments would recommend that users leverage the network storage for the purpose of general work-related digital content.

This practice typically drives up the demand of storage for the organizations. With benefits such as versioning, remote access and cost savings, choosing a cloud-based storage option is much more favorable in comparison with hosted storage.

There is an inherent increase in data breach risks when users determine that cloud storage is beneficial to them and adopt third-party personal cloud providers such as Box, Dropbox, Google Drive and OneDrive. Without the appropriate data governance and safeguards, these scenarios where users elect to choose
a technology service independently can have serious ramifications. By not ensuring that only the appropriate IT best practices are applied, data stored in the cloud may find itself in the wrong hands and cause serious violations of HIPAA compliance requirements and rules.

Hospital IT departments have a number of common best practices and features they look for when it comes to personal cloud storage.

- **Implementation of a storage authentication model.** If external access is needed, it is important to ensure that the users who will have access to possibly sensitive data are who they say they are. There could be cases where physicians and nurses use their home PC for access, but their password may be compromised or known to others. With the implementation of multifactor authentication (MFA), hospital IT can rest assured that only the authorized users have access to the files stored in the cloud.

- **Data leak prevention.** By not ensuring that only the appropriate IT best practices are applied, data stored in the cloud may find itself in the wrong hands and cause serious violations of HIPAA rules.

  Giving staff members access to folders to store their data is one thing, but being able to control what they store is a whole new ballgame. Historically, IT had to settle for training end users on what not to store on their cloud drive and hope for the best, but there are certainly no true mechanisms that can easily monitor and ensure compliance. With some of today’s cloud capabilities, IT can roll out specific storage policies to the end user’s storage in order to monitor and prevent accidental uploads of sensitive data. IT can also be notified when users upload data that may contain medical records, patient’s personally identifiable information and any other data that may be considered highly sensitive.

- **Cloud storage management tools.** While end users are able to manage their own folder structure and what goes into their personal drives most of the time, IT can still help manage the storage and backup of these files centrally. Since different cloud storage vendors have different retention policies, having IT roll
out its preferred cloud storage option allows IT to better manage storage software and ensure all the appropriate options for backups and compliance are rolled out properly. So using the right cloud provider that offers enterprise features for management becomes key.

- **Controls of folders available online and offline.** Personal cloud storage provides the convenience of access to files anywhere and anytime. For that very reason, many professionals have opted to adopt these tools in order to gain flexibility when working from different locations. But with that comes the challenge of ensuring that files are not synchronized in places where they should not be. As a result, IT generally recommends and only adopts the platforms that allow for controls over what can and can’t be available offline.

- **Enterprise compliance features.** One of the last and most critical components that IT looks for when selecting enterprise-grade online storage is monitoring and auditing capability. Components such as e-discovery, in-place hold, data access reports and activity logs all help ensure that the platform meets the compliance requirements that hospitals must follow. If IT is alerted that a local physician’s account is attempting to download large amounts of data into a computer abroad, IT can verify that and also challenge the access via MFA or simply block it until it is confirmed that the user needs access from a foreign country.

Security and privacy for personal cloud storage in healthcare are important topics. While the capabilities offered in many of the various products on the market seem to be equal, only a few options can truly live up to HIPAA compliance requirements. End users must work with IT, and IT must recognize and understand the convenience of these options to help meet the business requirements. Having the proper cloud option to store end-user data and make it safely accessible from anywhere and anytime is essential. —Reda Chouffani
REDA CHOUFFANI is vice president of development at Biz Technology Solutions Inc. Follow him on Twitter: @healthcareITGuy.

SHAUN SUTNER is news and features write for SearchHealthIT. Email him at ssutner@techtarget.com and follow him on Twitter: @ssutner.

© 2016 TechTarget Inc. No part of this publication may be transmitted or reproduced in any form or by any means without written permission from the publisher. TechTarget reprints are available through The YGS Group.

About TechTarget: TechTarget publishes media for information technology professionals. More than 100 focused websites enable quick access to a deep store of news, advice and analysis about the technologies, products and processes crucial to your job. Our live and virtual events give you direct access to independent expert commentary and advice. At IT Knowledge Exchange, our social community, you can get advice and share solutions with peers and experts.