White Paper

BEST PRACTICES FOR PROTECTING HEALTHCARE INFORMATION IN THE CLOUD

How five healthcare companies are complying with increasingly strict US HIPPA, HITECH & International laws - with 1 solution.

CipherCloud®
Trust in the Cloud™

333 W. San Carlos Street
San Jose, CA 95110

Summary

◊ Cloud adoption continues to accelerate in the healthcare industry as many companies realize the benefits of reducing their infrastructure, lowering costs, and becoming more agile to provide better services and adapt to evolving circumstances.

◊ At the same time, there are growing concerns about the increasingly strict data privacy laws regarding sensitive personal information that is stored in the cloud. Two primary privacy laws—HIPAA and HITECH, plus a variety of differing laws in U.S. states and many countries—make organizations directly responsible for protecting regulated information no matter where it resides.

◊ Recent legal updates to HIPAA and HITECH in 2013 seek to make cloud service providers (CSPs) and business associates (BAs), defined as any entity that "creates, receives, maintains, or transmits" protected health information (PHI), legally responsible as well.

◊ The biggest driver for most organizations is the threat of mandatory breach notification requirements that come with many compliance violations. While there can also be stiff fines and personal legal liability for business executives, a key concern remains that even a minor leak can result in public disclosure, inevitable press, and massive potential damage to a company's public perception and reputation.

◊ Also discussed are an increasing number of "Safe Harbor" exemptions to these breach notification laws, if an organization can demonstrate that data has been adequately protected through encryption, and no third-party has access to the encryption keys.

To illustrate how these issues can be addressed, five major healthcare services organizations are profiled with details about how they deployed a solution to encrypt or tokenize personal health information (PHI) before it goes to the cloud, while maintaining exclusive control over encryption keys. This approach provides effective control over sensitive information regardless of where it's stored, making it safe to realize the business benefits of moving to the cloud.

Case Studies

Contents

Accelerated Cloud Adoption in Healthcare Services

The use of cloud computing is a natural fit for the healthcare industry, as most organizations need to store vast amounts of patient data for treatment, research, and billing purposes. Cloud services provide enormous opportunity for health care organizations to transform their business processes so they can deliver high quality care in a more cost efficient and effective manner—far more so than traditional internal IT delivery models. The platforms and systems available for expediently managing and sharing electronic protected health information (ePHI), coupled with the cost savings advantages, are compelling.

Utilizing the cloud has allowed healthcare companies to realize a significant reduction and consolidation in their IT infrastructures, resulting in smaller budgets, more outsourcing, the ability to scale and adapt to changing needs, immediate access to more advanced technology, and better communication between patients and providers. For example, using the cloud for storing and accessing patient data can be beneficial when a patient may be receiving care at any number of health care offices around the country, or around the world.

In the healthcare industry, up-to-date information and knowledge sharing can often mean the difference between life and death with an organizations' actual customer: the patient. After all, the accurate tracking of a patient's personal data, health records and treatment history can be essential to providing the best possible care. And in today's modern world of instant and distributed communication, it's now possible for physicians and health organizations to gain access to a patient's records from nearly anywhere, at any time.

What Are the Biggest risks for Healthcare Companies with PHI in the Cloud?

"The push to digitize health records is picking up speed for a reason: it's good medicine. It saves money, and it saves lives. In some professions, missing a key detail might cost you a contract or a client; in medicine, it can mean losing a limb or a life."

Adam Levin, columnist, *"How to Make Your Medical Records Safer".*

Because of all these compelling benefits, it's no longer viable to "just say no" to the cloud.

Yet there are legitimate public concerns regarding security and privacy as healthcare organizations inevitably handle extremely sensitive personal and private health information. To protect an individual's right to privacy regarding their personal health, many governments have instituted strict regulations regarding the storing, distribution and sharing of protected health information (PHI).

The cloud has fundamentally changed the security model used by most IT organizations. In the past, enterprises built a strong perimeter with the intention of "keeping the good stuff in" and "keeping the bad guys out." But the reality today is that many users are bypassing all legacy security boundaries and going directly to the cloud. They're also coming in from external and mobile devices, where companies have no traditional control point at all. This results in a loss of direct control over sensitive information with no ability to ensure sensitive data won't be accessed by the wrong people.

Case Study 1: Major Hospital Chain

This prominent healthcare company started out in Nashville in the 1960's as one of the nation's first hospital companies. Today, the company is one of the world's largest providers of healthcare facilities with over 150 hospitals and over 100 surgery centers in more than 20 states.

The company needed to develop a more modern communication portal that would connect their hospitals with a vast network of service providers. Their portal would have an intuitive user interface, including email, to facilitate and speed communication, as well as save on the high costs of developing custom in-house systems. But first, stringent HIPAA and HITECH regulations regarding the security of patient records had to be dealt with.

Challenges

◊ Needed to develop portal for connecting hospitals to service providers
◊ Reduce high-costs and obsolescence of building custom in-house systems
◊ Key regulations: Assure privacy, HIPAA, HITECH compliance

Requirements

◊ Encrypt sensitive healthcare data
◊ Deliver cloud-based email without storing unencrypted data in the cloud
◊ Provide simple partner interface while assuring visibility

Solution

◊ CipherCloud for Salesforce
◊ AES 256-bit encryption of private patient records
◊ Secure email integration via Easylink

Results

◊ Achieved rollout of up-to-date communication CRM and email systems
◊ Reduced costs and internal infrastructure with ability to easily add more services down the road

You Can't Protect Against What You Can't See

Many healthcare organizations don't have visibility into where their data resides, what their users are doing, and whether sensitive information is being exposed. Before you can protect your data in the cloud, you first need to understand:

◊ Who should have access and who should not;
◊ What content is sensitive, proprietary, or regulated and how can it be identified;
◊ Where this data will reside in the cloud and what regional privacy, disclosure and other laws might apply.

Knowing where your data is going and what your users are doing, along with awareness of any malware or security breach attempts should they occur, is critically necessary up front so you can extend your corporate data loss prevention (DLP) policies to your external cloud applications.

Overview of Healthcare Industry Data Regulations

U.S. HIPAA and HITECH Requirements

The Health Insurance Portability and Accountability Act (HIPAA), implemented in 1996, covers protected health information (PHI) that reasonably identifies an individual and relates to health, disease, health services or payment for health services. Since 1996, healthcare organizations have had to keep electronic health information records confidential under the policy.

The security rule requires that US organizations that transmit an individual's protected health information (PHI) across electronic systems are required to meet HIPAA requirements. This means they must ensure the confidentiality, integrity, and availability of electronic PHI (e-PHI) through administrative, physical, and technical safeguards that ensure workforce compliance and protect against any reasonably anticipated threats, unauthorized uses or disclosures. HIPAA also requires covered entities (CE) to assure their customers that the integrity, confidentiality, and availability of PHI information they collect, maintain, use, or transmit is protected.

Along with HIPAA, the Health Information Technology for Economic and Clinical Health (HITECH) Act was signed into law in February 2009 as part of the American Recovery and Reinvestment Act of 2009 (ARRA). Subtitle D of the HITECH Act addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules.

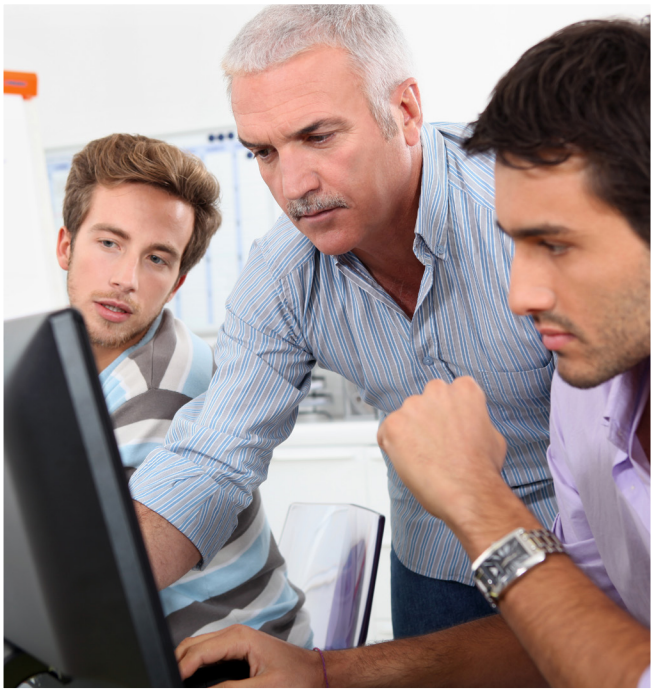
In January 2013, Health and Human Services (HHS) strengthened privacy and security protections for health data. Civil Rights Director of the Department of HHS Leon Rodriguez describes these as "the most sweeping changes to the HIPAA Privacy and Security Rules since they were first implemented." In September 2013, the HIPAA Omnibus Rules added more teeth to these regulations and deal more explicitly with health data stored with cloud service providers (CSPs).

Violations of HIPAA come with hefty financial penalties but steep as they are, worse still is the threat of public notification and disclosure, covered in the next section.

FTC Breach Notification Rules

In addition to the HIPAA/HITECH concerns, healthcare companies face another source of liability.

Companies processing electronic health information are subject to FTC breach notification rules requiring companies to publicly announce a security breach. This includes providers of online health data repositories and applications used directly by individuals on websites and mobile phones. So ironically for many companies that are not necessarily subject to the HIPAA breach notification rule, if you provide an electronic health record, you still might be subject to the FTC's rules. This is significant because of the high costs associated with data breach disclosures, including irreparable damage to a company's reputation.



Case Study 2: Genomic Testing Provider

This is a privately held life-sciences company that provides genomic and proteomic products and services for physicians and the life sciences industry. Committed to helping physicians, families and children suffering with neurological disorders, their bioinformatics and genetic testing converts raw information into highly usable clinical data that can lead to positive changes and improvements in a child's quality of life.

This advanced technology company wanted to rely on cloud systems to manage their data and make it more accessible. This involved migrating services and data to the cloud, including sensitive information on patients, doctors, and genomics.

Challenges

◊ Using cloud system for services that require handling sensitive patient, doctor, and genomic data
◊ Meeting HIPAA-HITECH 2013 Final Omnibus Rule's higher standards for protecting cloud-based data
◊ Assuring HIPAA-compliance of ePHI data stored in the cloud

Requirements

◊ Strong encryption of encryption patient, genomics, and testing data
◊ Seamless integration with NetSuite business management platform
◊ Rapid implementation required to meet critical compliance deadline

Solution

◊ CipherCloud for NetSuite
◊ Seamless deployment of NetSuite platform to over 1,000 users in just 66 days
◊ Provided seamless strong encryption of sensitive patient, doctor, and genomic data

Results

◊ Successful launch of key applications to the cloud
◊ Assured compliance and integrity of highly sensitive patient information; protecting corporate reputation
◊ Support for NetSuite to streamline operations on a single platform

Healthcare Industry Data Regulations

The Latest New and Stricter HIPAA/HITECH Requirements as of September 2013

The new Omnibus Rules for HIPAA and HITECH announced in September 2013 strengthen patient privacy and rights to health information.

The ability to enforce the regulations is also beefed up. As HHS head Rodriguez put it,

"These changes not only greatly enhance a patient's privacy rights and protections, but also strengthen the ability of my office to vigorously enforce the HIPAA privacy and security protections, regardless of whether the information is being held by a health plan, a health care provider, or one of their business associates."

The changes include a new breach notification rule with more objective criteria on whether incidents must be disclosed, and also increase penalties for non-compliance.

These rules apply specifically to Covered Entities (CE) and Business Associates (BAs).

Covered Entities are defined as and include:

- ◊ Healthcare providers (doctors, clinics, dentists, chiropractors, nursing homes, and so on)
- ◊ Health plans (health insurance companies, HMOs, company health plans, Medicare, etc.)
- ◊ Health care clearing houses

Business Associates are defined as and include:

- ◊ Any entity that "creates, receives, maintains, or transmits" PHI on behalf of a covered entity (CE). BAs do not include conduits (i.e., ISPs).

These definitions provide some guidance as to the varying responsibilities of these parties, but they are far from clear in their practical applications and leave plenty of questions still to be answered.

> "To summarize how the new ruling changes things: there's a new sheriff in town....with bigger guns and stronger handcuffs."
>
> Gerald Stegmaier, *Esquire*

The Fog of Business Associates and BAAs

As organizations try to determine how the new rulings apply to them and their associates, what's most clear so far is that the Business Associate Agreement (BAA) waters are *not* clear. Two recent breach examples below reveal how muddy these waters are. The various parties involved—CEs, cloud service providers (CSPs), BAAs–have differing roles, perspectives, and opinions as they grapple with defining who's liable for what and where lines should be drawn.

It remains unclear whether a cloud provider that encrypts PHI but doesn't have the encryption keys "maintains PHI" under HIPAA. If so, they would qualify as a BA, and most people have concluded that cloud service providers (CSPs) that store PHI likely are Business Associates. But CSPs have argued that they often do not or cannot access the data they are housing on their servers and therefore feel they cannot reasonably be liable for managing its access. Until the dust settles, some CSPs are stepping back from signing BA agreements, or at least are pushing the decision to a later date down the road until hopefully more clarity emerges.

Examples of HIPAA Breaches in the Cloud

The HIPAA breach examples below clearly show the confusion surrounding CEs and cloud providers—i.e., whether they are in fact acting as Business Associates. In these cases, Google servers housed the unprotected ePHI that was in violation of HIPAA standards. As the CSP, Google hadn't signed a BA agreement, which is not uncommon. But even for cloud providers who are willing to sign BAAs, they are likely to insist on their own terms rather than the terms a Covered Entity would seek to impose. Indeed, the lines are certainly blurred.

1. **Oregon Health & Science University (OHSU) HIPAA breach:** The incident involved patient information that was inappropriately stored in the cloud (ie, unencrypted). In these two incidents:

- ◊ More than 3000 patients' information was affected
- ◊ The data was contained in spreadsheets and was unencrypted
- ◊ The data was accessible via Google cloud-based email and document storage services
- ◊ OHSU does not have a BAA with Google, though recent HIPAA Omnibus rules may indicate cloud providers are in fact considered business associates

2. **Cottage Health System breach:** This company operates five hospitals in the Santa Barbara, California area.

- ◊ 32,500 patients had their health care information exposed for 14 months
- ◊ The information was exposed on Google, but a third party was also involved, which per Cottage Health, had let a lapse occur in its Business Associate's protections, without Cottage Health's knowledge
- ◊ The server was taken offline and Cottage Health requested that Google remove the file from its systems.

These incidents raise many questions that point to the complex issues of the new business associate liabilities under the HIPAA Omnibus Rule. When all is evaluated in these breaches and others like them, whether CSPs will also be on the liability hook and face HIPAA violation penalties, with or without a signed BAA between the two parties, is not yet clear.

Healthcare Industry Data Regulations

In the End, Does it Really Matter?

Who carries what levels of responsibility between the healthcare organizations and the cloud service providers (CSPs) is a matter of ongoing debate. Parties can haggle—and many are to be sure—over this issue for months and years to come.

Even if CSPs are held liable, the prospect of doing battle with one's cloud service provider is not only unappealing, but potentially futile as well. At the end of the day, while CSPs will likely bear some yet-to-be-determined responsibility, the simple answer is that it really doesn't matter where the lines of liability are drawn between organizations (CEs) owning data and CSPs and other entities that are housing, receiving, transmitting, or maintaining the data. Ultimately, compliance responsibility rests with the owner of the ePHI, such as the healthcare organization, physicians, and staff providing care and there's no getting off that hook.

Therefore, however gray and confusing these new definitions may be, the owners of the PII and ePHI remain fully responsible for protecting their data in compliance with HIPAA and HITECH, regardless of who else may be involved. Given that reality, the most prudent course of action remains going the distance to establish best security practices to protect ePHI data in accordance with compliance regulations.

Case Study 3: Global Pharmaceutical Company

This international pharmaceutical company has 80,000+ employees working across 150 countries. Their main business objective is a focused attention on detecting and preventing diseases, including diagnosis, treatment, and patient monitoring.

Wanting to make collaboration and communication easier for their growing employee base while also finding ways to reduce in-house costs, the company planned to adopt Google's Gmail for internal communications. To move forward, they first had significant privacy and regulatory challenges to address.

Challenges

◊ Secure global rollout of Gmail for increased collaboration, remote working and cost reduction
◊ Confidential correspondence required security to assure compliance and protect intellectual property

Requirements

◊ Had to assure that sensitive emails are protected in Google Enterprise Email
◊ Needed to select and control security centrally
◊ Wanted zero change to the user experience and no impact on adoption

Solution

◊ CipherCloud for Gmail
◊ Successful outsourcing of email infrastructure with ability to scale to hundreds of thousands of global users
◊ Transparent to users, critical business data is protected and compliance requirements are met

Results

◊ Employees and partners have a more collaborative environment that's easily scalable
◊ Critical business data is protected, compliance regulations met, and costs savings in the Cloud

Healthcare Industry Data Regulations

Additional U.S. State Privacy Laws

In addition to the possible financial penalties for data breaches, the biggest concerns for most organizations are the Breach Notification requirements of most data privacy laws. Public breach notifications began with the landmark privacy law in California's State Bill (SB) 1386, enacted in 2002. SB 1386 requires any company that has lost or allowed access to unencrypted personal information to disclose the breach.

Similar privacy laws with breach notification requirements now exist in 46 U.S. States and over 50 countries. Laws differ on specifics, but common themes hold data collectors responsible for protecting personally identifiable information—including names, social security numbers, drivers license numbers, account numbers, credit and debit card numbers, and access codes or passwords that allow access to medical or health insurance information.

Companies risk enormous hits to their brands and reputations if they are listed in a major notification. Many sites track these and news organizations are hungry to highlight mistakes by the latest big name company.

Details on all U.S. state breach notification laws can be found on the National Conference of State Legislatures website.

Global Healthcare Privacy Regulations

As business becomes increasingly global, healthcare organizations can be subject to overlapping or even conflicting laws in multiple countries. For example, forced data disclosure laws in some countries might violate the privacy laws of another country if the data crosses national boundaries—almost inevitable with the cloud.

European Union Data Privacy Directives

European Union has enacted both the Data Protection Directive of 1995 (46/EC) as well as the Internet Privacy Law of 2002 (58/EC). These were developed to create standards among EU member states, as diverging laws were impeding the free flow of data within the EU. These Directives reflect broad personal privacy laws throughout Europe, and cover the electronic processing and storage of personal information.

More than 28 EU countries have established privacy laws that reflect the EU Directives, although there are regional differences in how these are interpreted.

Healthcare Industry Data Regulations

The UK Data Protection Act

In the UK, the Information Commissioner's Office (ICO), which has the ability to levy half a million pounds in fines for companies that contravene the Data Protection Act, has recently turned its attention to the cloud. In November 2012, it published guidance outlining the responsibilities for companies storing their customers' data in cloud environments. The guidelines assign responsibility for data security unequivocally to the company that owns the data, rather than the company taking care of it.

Australia Privacy Ammendment

Australia has actually had a Privacy Act in place since 1988, but has now taken steps to bring its law up to date with The Privacy Amendment Act of 2012 (Enhancing Privacy Protection Reform Act). The updated Privacy Act is explicit that enterprises that hold Australian customer data are responsible for protecting that data, regardless of where it's located, or whether breaches are caused by cloud providers.

Case Study 4: Australian Insurance Provider

As the largest provider of private health insurance and solutions in Australia, this organization provides health services and benefits to millions of people every year in Australia and New Zealand. Their over 4,000 employees process billions of dollars worth of hospital and allied health claims, as well as deliver over 550,000 clinical services annually.

This government-owned, private health services organization planned to make their phone and web-based healthcare services available to users across Australia and New Zealand. Because their information included highly confidential medical and personal information, they needed to meet strict requirements of government mandated data residency and privacy controls.

Challenges

◊ Placing their innovative phone and web-based healthcare services on cloud platforms
◊ Protecting their sensitive information while in the cloud
◊ Meeting strict government mandates regarding data residency and privacy control

Requirements

◊ Encryption with granular control by field, location, and type of data
◊ Tokenization for information with strict data residency requirements
◊ Geographically distributed deployment in Australia and New Zealand

Solution

◊ CipherCloud for Salesforce
◊ Flexible combination of encryption and tokenization
◊ Maintain key functionality and performance of Salesforce platform

Results

◊ Able to save costs and offer greater customer accessibility on a new cloud-based platform in multiple regions
◊ Meeting compliance with strict privacy and data residency laws in Australia and New Zealand

Healthcare Industry Data Regulations

Safe Harbor Exemptions

After all the grave scenarios above, it comes as good news that most state privacy laws specifically exempt the theft of private data as being a breach if it has been adequately encrypted*, meaning it has been "transformed into a form in which the data is rendered unreadable or unusable without use of a confidential process or key."

For HIPAA/HITECH, adequately applied encryption is considered a "safe harbor" and is likely to be seen as "reasonable" security—assuming that the encryption keys are protected. In the case of the FTC and state data breach laws, encrypted data is typically exempted from breach disclosure requirements if it has been "rendered unreadable without use of a confidential key."

Put another way, these regulations take into account the use of encryption when the data loss occurs. In numerous cases, these laws recognize that if your data is adequately encrypted or "rendered unintelligible," then Safe Harbor exemptions from notification and legal liability apply.

> "You do not need to tell your subscribers about a breach if you can demonstrate that you have measures in place which would render the data unintelligible and that those measures were applied to the data concerned in the breach."
>
> UK Information Commissioner's Office (ICO)

*encrypted through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Pub. L. 111-5.

Healthcare Industry Data Regulations

The table below outlines which major compliance regulations require mandatory breach notification and have exemptions if data is adequately encrypted:

Country/ Region	Regulation	Data Type	Mandatory Breach Notification	Safe Harbor Exemptions to Notification	Recommendations on Encryption
U.S.	HIPAA	ePHI, PHI, PII	Yes	Yes	Safe harbor only applies "if encryption has been applied adequately"
U.S.	HITECH	ePHI, PHI, PII	Yes	Yes	Safe harbor only applies "if encryption has been applied adequately"
Europe	EU Directive 1995/46/EC	Personal Information	Proposed	Proposed	New draft regulation proposes notification safe harbor exemption if data was adequately encrypted.
Europe	EU Directive 2009/136/EC "EU Cookie Law"	Personal Information	Yes	Yes	Safe harbor exemption if data was adequately encrypted.
U.K.	ICO Privacy Amendment Data Protection Act?	Personal Information	Yes	Yes	Breach notification not required if there are "measures in place which would render the data unintelligible."
Australia	ICO Privacy Amendment	Personal Information	Yes	Not Specified	Does not specify encryption but requires organizations to "take adequate measures to prevent the unlawful disclosure" of protected information.
U.S. States	California SB 1386 (and similar laws in 46 states)	Personal Information	Yes	Generally Yes	Most state laws have similar definitions on: • *Personal Information:* "data elements that are not encrypted" • *Breach:* "unauthorized access to unencrypted data" • *Encrypted:* "use of an algorithmic process to transform data into a form which is rendered unreadable or unusable without use of a confidential key"

Bottom Line: There's No Excuse for Not Encrypting

Legal regulations requiring healthcare services organizations to protect personal and medical data do not actually mandate specific methods of meeting requirements. Instead, the language consists of terms like "reasonable" and "adequate security" to define the steps that must be taken to provide this protection. This clarifies a common misconception that regulations spell out specific technologies companies must adopt in order to be compliant. They do not.

But while such specifics may not yet be currently written into the HIPAA and HITECH legal language, the latest updates released last September leave little leeway for a solution other than encryption. Data encryption is one of the primary and best means of securing patient data from accidental data loss, hackers, and other threats, and as such, remains highly recommended.

The HIPAA encryption standard specified in the security rule indicates responsible parties (CEs) must either implement encryption or come up with a 'reasonable and appropriate' solution to meet the regulatory requirement. As encryption technologies have developed and become more affordable, it is becoming more difficult to take the position that there are any 'reasonable and appropriate' alternatives to encryption.

With encrypted data, secret codes (keys) are used to encrypt digital information. Without these keys—which should always remain in the possession of the healthcare data owner—the software cannot be decrypted. Encryption therefore protects your vital data against prying eyes, regardless of where it is stored. Entities who attempt to circumvent the company's protocols for data access will retrieve only scrambled information.

> "Before [the Edward Snowden disclosures], many enterprises were running unencrypted data on their internal networks, which they believed were secure. Now they are beginning to use encryption internally as well, so we expect 2014 to be the year of encryption."
>
> Dave Frymier, Unisys chief information security officer, *Info Security Magazine*

Data Residency and Data Sovereignty Risks

Several of the major regulations listed previously have a significant impact on healthcare services organizations seeking to remain compliant with domestic and international regulations.

As described, different countries have different laws regarding privacy of data, ranging from how data can be accessed, how or whether data can be stored in certain foreign countries, and whether foreign governments have a right to legally access certain data. Concerns include the following.

◊ For many healthcare services organizations, especially outside the U.S., forced disclosures by law enforcement agencies can potentially violate national data privacy laws. This is often cited as a concern or inhibitor for many corporate cloud initiatives—the organization is legally required to protect personal information, but can't be certain that it won't be accessed by law enforcement in other countries.

"[Encryption] is an indispensible tool for securing patients' electronically stored and transmitted data. It is so fundamental, in fact, that even though it has not been strictly "required" by HIPAA and HITECH … it is, as a practical matter, impossible to comply with HIPAA regulations without using encryption."

Adam Levin, credit.com Blog.

http://blog.credit.com/2013/10/making-your-medical-records-safer/

HHS Office of Civil Rights (OCR) Director Rodriguez stated last year that OCR "loves encryption," and went on to say "in the event of a breach, using encryption assures that that information is unreadable, unusable or undecipherable, which, basically, would qualify for the safe horbors under our breach notification rule."**

**http://www.modernhealthcare.com/article/20130105/MAGAZINE/301059959

◊ Most organizations regularly deal with legal subpoenas to turn over data, but they want to manage and accurately comply with specific requests themselves. The risk of having a cloud provider turn over potentially large amounts of data causes heartburn for most corporate legal departments.

◊ CSPs who do not maintain and cannot access data encryption keys cannot provide unencrypted data to law enforcement or other entities when there is an investigation or litigation related request. Instead, these requests must require the direct involvement of the CSP customer (i.e., the healthcare organization) who can then choose to comply or challenge the data access request as opposed to having the decision made by the CSP, a far more preferable situation to organizations.

Best Practices for Cloud Information Protection

The new HIPAA Omnibus Rule puts healthcare organizations and their business associates on the alert, advising they will be "under more scrutiny than ever before to protect patient information."

Security Rule Requirements

- ◊ Ensure the confidentiality, integrity, and availability of e-PHI through administrative, physical, and technical safeguards
  - ¤ Protect against any reasonably anticipated threats or hazards"
  - ¤ Protect against any reasonably anticipated unauthorized uses or disclosures
- ◊ Ensure workplace compliance

Administrative Safeguards

- ◊ Perform a risk assessment of potential riskds and vulnerabilities to the confidentiality, integrity, and availability of e-PHI
- ◊ Implement policies and procedures to:
  - ¤ ensure workforce has appropriate access to e-PHI
  - ¤ authorize access to e-PHI only where appropriate
  - ¤ address security incidents
  - ¤ respond to disasters (e.g., backups)
- ◊ Identify security official responsible for compliance
- ◊ Security awareness and training program
- ◊ Periodic compliance assesment of itself and its BAs

Technical Safeguards

- ◊ Implement policies and procedures to:
  - ¤ allow access only to those persons or software programs that have been granted access rights
  - ¤ protect e-PHI from improper alteration or destruction
  - ¤ verify that a person or entity seeking access to e-PHI is the one claimed
- ◊ Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use e-PHI.
- ◊ Guard against unauthorized access to e-PHI transmitted over network.

Staying on the safe side of compliance begins with reviewing and updating your security policies and procedures and once established, making sure those policies are shared with the workforce. Most important of all is performing a thorough risk assessment to discover your points of vulnerability. And the first step to doing that effectively is learning what types of data you need to protect.

Know Thy Data

Where It Resides, Who's Accessing It, and What's Happening in Its Environment

Data Discovery—As mentioned earlier in this paper, before you can protect sensitive corporate information in the cloud, you first need a detailed understanding of:

- ◊ Who should have access and who should not;
- ◊ What content is sensitive, proprietary, or regulated and how can it be identified;
- ◊ Where this data will reside in the cloud and what range regional privacy, disclosure and other laws might apply.

CipherCloud's technology provides out-of-the-box DLP controls and policies that can spot potential violations of HIPAA/HITECH or other regulations. CipherCloud also enables you to monitor exactly what your users are doing in cloud applications, including Salesforce, Chatter, Box and many others. Details on login activity, file downloads, exported reports, and potential DLP violations are clearly visible, with real-time drill-down for additional details.

You can easily configure dashboard alerts on any unusual user activity that might indicate problems, such as excessive downloads, after-hours activity, or unauthorized access to sensitive content.

Case Study 5: Regional Insurance Leader

This leading state insurance provider employs over 1000 employees onsite committed to providing their members with access to affordable, high-quality healthcare. Founded in 1939, the company now operates in 20 US states and the UK, supporting over 600,000 memberships. This particular state's facility is committed to the health and well being of the residents in their community, with the vision that improving their customers' health promotes better quality of life as well.

They had plans to create a cloud-based patient portal which would allow them to engage more users and lower infrastructure costs. The portal would house both structured and unstructured data, including PII, so they were challenged to protect it per HIPAA and HITECH compliance regulations.

Challenges

- ◊ Creating cloud-based patient portal while assuring HIPAA compliance for all patient data
- ◊ Implementing strong encryption and key management for all PII fields
- ◊ Keeping functionality and ease-of-use for integrated web2lead and email systems

Requirements

- ◊ Protecting both structured an unstructured data
- ◊ Granular field-level control for structured and free-form data
- ◊ Assuring HIPAA compliance for all patient data, regardless of location

Solution

- ◊ CipherCloud for Salesforce
- ◊ Applied AES 256-bit encryption to 15+ fields within Salesforce, multiple orgs
- ◊ Integrated and encrypted email and web2lead systems for 200+ users

Results

- ◊ Experienced significant cost savings by moving to a cloud-based portal platform
- ◊ Reduced internal infrastructure
- ◊ Assured data security and HIPAA compliance for all personal patient information

The CipherCloud Encryption Solution

CipherCloud can be deployed in many ways, but most commonly it is deployed as a gateway at the perimeter to your organization to provide a control point where you can enforce security policies. A number of granular security policies can be enforced, but the most common is encrypting using top-level standards—AES 256—or tokenization. Encryption or tokenization can be applied selectively, on a field-by-field basis, or automatically triggered by the content itself whether it is a Social Security number or other PHI information.

Importantly, CipherCloud preserves the functionality of cloud applications, including searching and sorting of encrypted data. But someone who's unauthorized coming in without appropriate access will see only encrypted gibberish.

Any authorized user accesses sensitive data through CipherCloud's secure gateway, which automatically decrypts data and renders it viewable. This includes any users accessing data through mobile devices.

Conclusions

Adoption of the cloud is now a fact of life for many if not most healthcare services organizations. As cloud technology advances, organizations are more and more on the hook with regard to their legal responsibilities to protect their patient's health information more tenaciously than ever before. HIPAA and HITECH compliance laws, and other international privacy laws, have kept pace along with technology with increasingly strict privacy laws and data residency restrictions.

With the latest HIPAA ruling in September of 2013, Business Associates share in this responsibility more than ever before, requiring data owners who gather patient data to sign business agreements with them. And regardless of who else may be on the hook, data owners (Covered Entities) are and will continue to be fully responsible. As such, organizations and IT departments need to collaborate in finding the appropriate security models that allow them to leverage the full advantages of the cloud while assuring full and reliable protection for patient information.

As illustrated by the customer examples in this paper, CipherCloud provides comprehensive cloud information protection for many of the world's largest and most security-conscious healthcare services organizations.

Glossary of Terms

AMA—American Medical Association
ARRA—American Recovery and Reinvestment Act
BA—Business Associates
BAA—Business Associate Agreements
CEs—Covered Entities
CSPs—Cloud Service Providers
EHRs—Electronic health records
ePHI—Electronic protected health information
HHS—Health and Human Services
HIPAA—Health Insurance Portability and Accountability Act
HITECH—Health Information Technology for Economic and Clinical Health
PII—personally identifiable information,
PHI—protected health information

Additional Resources and Information

Public Resources

- **The Health Insurance Portability and Accountability Act (HIPAA) Omnibus Final Rule Summary** http://www.ama-assn.org/resources/doc/washington/hipaa-omnibus-final-rule-summary.pdf
- **Health and Human Services website:** http://www.hhs.gov/
- **Health Information Privacy:** http://www.hhs.gov/ocr/privacy/
- **HIPAA News Update January 17, 2013:** http://www.hhs.gov/news/press/2013pres/01/20130117b.html
- **Omnibus Final Rule:** http://www.ama-assn.org/resources/doc/washington/hipaa-omnibus-final-rule-summary.pdf
- **State Security Breach Notification Laws:** http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx
- **Breaches Affecting 500 or More Individuals:** http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html

CipherCloud resources:

- **Best Practices for HIPAA Cloud Security:** http://www.ciphercloud.com/2014/02/06/best-practices-hipaa-cloud-security/
- **Healthcare and the Cloud On-Demand Webinar: Interview with Gerard Stegmaiar, Attorney, Washington DC** http://pages.ciphercloud.com/HealthcareandtheCloudSolvingtheSecurityDilemmaondemand.html
- **Healthcare and the Cloud: CipherCloud Solves the Security Dilemma** http://www.ciphercloud.com/2013/07/26/healthcare-cloud-solving-security-dilemma-encryption/
- **Four Benefits of Managing HIPAA Compliance with Cloud Data Privacy** http://www.ciphercloud.com/2013/12/20/four-benefits-managing-hipaa-compliance-cloud-data-privacy/
- **Three Critical Requirements of HIPAA Cloud Security** http://www.ciphercloud.com/2014/01/27/3-critical-requirements-hipaa-cloud-security/

CipherCloud is the leader in cloud information protection enabling organizations to securely adopt cloud applications by overcoming data privacy, residency, security, and regulatory compliance risks.

Visit **www.ciphercloud.com** for more information, online demos, or free trials.

Email **sales@ciphercloud.com** or call +1.408.520.4937

Corporate headquarters:
333 W. San Carlos Street
San Jose CA
95110, USA