Privacy and security of patient data in the cloud
Cloud providers' and consumers' responsibilities under U.S. law

Erin Gilmer

April 16, 2013
(First published October 23, 2012)

This article's goal is to help both providers and consumers of cloud services comply with the security and privacy requirements of U.S. healthcare law. It starts by giving you a basic understanding of the relevant laws, then discusses their implications with respect to cloud services, covering the issues of data control, access, integrity, and availability; shared multitenant environments; incident preparedness and response; and data security. (Nothing in this article should be perceived as legal advice.)

16 April 2013 — Editor's note: This article, originally published in 2012, has been updated to include coverage of modifications to HIPAA that were finalized in January 2013.

New technologies — from electronic health records to medical devices to mobile and web applications — are enabling doctors to improve health conditions and save lives. Doctors use these technologies to collect more information than ever before, learning patients' health stories through the data they collect. These technologies and the data they contain connect and interact constantly, sending health information through increasingly complex systems with increasing risks and vulnerabilities. No longer are doctors the only ones entrusted with intimate health information. Now, among others, the individuals managing the data storage can access this information and thus have a responsibility to safeguard it.

Recognizing the sensitivity of health information, in 1996 the U.S. government enacted the Health Information Portability and Accountability Act (HIPAA) and, in 2003, the Health Information Technology for Economic and Clinical Health (HITECH) Act (see Related topics). These laws require entities that are responsible for sensitive health information to implement certain measures to ensure privacy and security, and to inform patients when the privacy and security of their information is compromised.

As consumers migrate to cloud services, understanding these standards and requiring strict adherence to them is key to fulfilling an entity's responsibilities and maintaining the trust of the patients who divulge intimate details for their health. To provide a foundation for addressing related issues with cloud services, this article starts by giving you a basic understanding of HIPAA
HIPAA consists of specific privacy standards and security standards for certain health information, which are known as the HIPAA Privacy Rule ("Privacy Rule") and the HIPAA Security Rule ("Security Rule") respectively. HIPAA applies these rules to covered entities, which include healthcare providers, health plans, and healthcare clearinghouses.

According to the U.S. Department of Health & Human Services (HHS) website, (see Related topics):

The HIPAA Privacy Rule provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule is balanced so that it permits the disclosure of personal health information needed for patient care and other important purposes.

In turn, the Security Rule "specifies a series of administrative, physical, and technical safeguards for covered entities to use to assure the confidentiality, integrity, and availability of electronic protected health information."
The HITECH Act
The HITECH Act required the Secretary of HHS (the Secretary) to expand the HIPAA Privacy and Security Rules and increase penalties for violations of HIPAA. Previously, the HHS Office for Civil Rights (OCR) had jurisdiction only over covered entities for privacy breaches. Under the HITECH Act, the HIPAA Privacy and Security Rules were extended to apply to business associates (BAs) — defined as persons or entities that perform certain functions or activities that involve the use or disclosure of PHI on behalf of, or provide services to, a covered entity. BAs often provide services such as claims processing or administration, data analysis, utilization review, or practice management. A cloud provider that stores PHI either on behalf of a covered entity directly, or indirectly through another BA, is now also considered a BA.

Omnibus Rules
In January 2013, the OCR published the final Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules — the "Omnibus Rules" (see Related topics) These rules redefine BAs, increase protections for the privacy and security of PHI, impose direct liability on BAs, amend the Breach Notification Rule’s “harm” threshold, and clarify the contents needed in business associate agreements. Most notably for cloud service providers and consumers, with the promulgation of these final rules the OCR has jurisdiction over BAs — and their subcontractors — for enforcement purposes.

The definition of a BA was significantly revised by the Omnibus Rules. The rules now state that BAs specifically include subcontractors, defined as persons who act on behalf of a BA. Subcontractors are persons to whom the BA has delegated a function, activity, or service that the BA agreed to perform for a covered entity or other BA. Essentially, subcontractors are BAs to BAs, further down the chain of entities responsible for PHI.

The key to understanding whether an entity is a BA is in understanding whether — in the course of business with a covered entity or BA — PHI is being created, received, maintained, or transmitted. The word "maintain" is of utmost importance in the new rule, particularly as it applies to cloud service providers.

Cloud providers as BAs
Cloud providers hold a unique position as BAs entrusted with EPHI. When HIPAA was enacted, the concept of "the cloud" didn't exist and probably could not have been predicted. Covered entities and other BAs are increasingly choosing to store health information in the cloud. Common reasons cited for doing so include cost savings, storage management, platform strength, resource availability, backup and recovery, and decreased IT maintenance (see Related topics). However, when EPHI is stored — or "maintained" — in the cloud, consumers are in effect disclosing it to the cloud provider, who in turn becomes a BA. For that reason, it is imperative that cloud providers comply with HIPAA and HITECH provisions.

Although the OCR does not specifically use the term cloud service providers, in its comments to the rules the OCR uses the example of "data storage companies" as BAs or subcontractors to
clarify the meaning of "maintain." The comments explain that even if the BA does not actually view PHI or if it only views the information randomly or infrequently, it is not a "conduit" exempt from regulation.

The updated BA definition, in concert with the comments provided, leave no doubt that cloud service providers and others entrusted with PHI from a covered entity are BAs. And as BAs, cloud service providers are now subject to direct liability and increased responsibility for PHI.

**Business associate agreements**

HIPAA allows covered entities to exchange EPHI for treatment, payment, and healthcare operations without requiring the patient's consent. However, only the minimum necessary EPHI necessary to accomplish the purpose of the exchange should be disclosed. Thus, covered entities may exchange EPHI with one another or with BAs. But in releasing this information to BAs, covered entities must obtain satisfactory assurances that a BA will appropriately safeguard any EPHI that a covered entity provided. This is done through a **business associate agreement** (BAA).

BAAs are essentially service-level agreements (SLAs) with specific provisions to address HIPAA and HITECH compliance. Covered entities are required to enter into BAAs with the BAs to whom they provide EPHI. Similarly, BAs must also enter into BAAs with those to whom they pass on this information — their subcontractors. Similarly, BAs must also enter into BAAs with their subcontractors. However, covered entities do not need to enter into separate BAAs with subcontractors to ensure the privacy and security of PHI. When the roles and responsibilities of the covered entity and BA or subcontractor are clearly defined in a BAA, liability for each entity can be mitigated and processes for breach notification can be eased.

Between BAs and covered entities, BAAs must include satisfactory assurances that the BA will agree to comply with the Security Rule, to report breaches of unsecured PHI to the covered entity, and ensure their subcontractors agree to the same restrictions and conditions on PHI that apply to BAs. If a covered entity knows of a pattern of activity or practice of the BA that violates the BAA, the covered entity must take reasonable steps to cure the breach or end the violation, and if such steps were unsuccessful, terminate the BAA. Additionally, the BAA must make clear that the BA is contractually obligated to comply with the Privacy Rule as it applies to the covered entity when carrying out a function or activity for the covered entity. These requirements similarly apply to BAs contracting with subcontractors.

Even without a BAA, business associates and subcontractors are still directly liable based on its activities, but BAAs help define important responsibilities.

**BAAs and the cloud**

The importance of clear BAAs cannot be overstated when EPHI is stored in the cloud. For cloud service providers, BAAs should include the terms and conditions for access and use of services, the period of service, conditions for termination, and disposition of data upon termination. Furthermore, a BAA should include a privacy policy that outlines information-handling practices and how consumer information is collected, used, and managed by the cloud provider. Most
important, although responsibility over security and protection of EPHI may be transferred or
shared, BAAs should clearly state that data ownership does not transfer to the cloud provider.

Because only certain functions are delegated to cloud service providers depending on the
services used by their consumers, cloud service providers should ensure that BAAs they enter
into with covered entities or other BAs or subcontractors go into explicit detail as to roles and
responsibilities for PHI. This should include spelling out who is responsible for the creation,
implementation, management, and modification of access privileges (both of the consumer and
cloud service provider); incident response; encryption; key management; and data monitoring —
among other issues discussed later in this article.

Further, the cloud service provider should clearly explain the services it is providing, those that it is
not responsible for, and the risks associated with each service that it does provide. For instance,
a cloud service provider might offer that data be stored in multiple geographic locations. Storing
data in a different location from where the consumer operates — or, if made redundant or backed
up — in several locations, can provide reassurance that critical business operations will not be
interrupted in case of emergency. However, if the data is stored in other countries, this might lead
to issues with differing international laws that change who has access to data in contradiction to
HIPAA and HITECH laws. BAAs can make clear where the consumer expects PHI to be stored —
in the United States or elsewhere — and who is expected to have access and control of the data
regardless of location.

Direct liability

The OCR recognizes that all who are entrusted with PHI must be held accountable to keep it
private and secure. In setting forth these rules, the OCR explained that it wanted to "avoid having
privacy and security protections for protected health information lapse merely because a function
is performed by an entity that is a subcontractor rather than an entity with a direct relationship with
a covered entity." Thus, downstream entities working at the direction or on behalf of BAs (such as
subcontractors), as well as BAs working on behalf of covered entities, are subject to direct liability
and the imposition of Civil Monetary Penalties (CMPs) for noncompliance with HIPAA.

Specifically, BAs are directly liable for:

- Impermissible uses and disclosures ("breaches")
- Failure to provide breach notification to the covered entity or the BA as appropriate
- Failure to provide access to a copy of electronic PHI to the covered entity or individual whose
  information it is
- Failure to disclose PHI to the Secretary as required to investigate or determine the BA's
  compliance
- Failure to provide an accounting of disclosures
- Failure to comply with the Security Rule Subpart C of Part 164

Because cloud service providers are now directly liable, they must be vigilant about data in their
control. To help avoid or mitigate violations, they should continually monitor and audit access
to their consumers' data as well as establish and ensure proper authentication procedures (as
discussed later in this article). This can decrease the risk of vulnerabilities; increase the chances that threats are found and corrected in a timely manner before any harm is suffered; and ease cooperation between other BAs, covered entities, or the Secretary if necessary to address a breach of PHI. In fact, with proper vigilance and by being proactive, cloud service providers can claim an affirmative defense to any violations by taking corrective action within 30 days.

**Civil monetary penalties**

This new liability imposed on BAs can be quite costly — including CMPs of up to $1.5 million per year for violations of an identical provision. The OCR makes clear, though, that this cap is *per type of violation.* It notes the likelihood that a BA could have multiple violations (for example, an impermissible use or disclosure as well as safeguard violations) that could result in much higher penalty amounts. The penalties are tiered and based on the BA’s *mens rea* (state of mind) — increasing in severity from *no mens rea* (that is, did not know) to *assumed mens rea* (that is, willful neglect). Table 1 lists the CMPs for violations:

**Table 1. Civil monetary penalties for HIPAA violations**

<table>
<thead>
<tr>
<th>Violation</th>
<th>Amount per violation</th>
<th>Maximum amount for all violations of an identical provision in a calendar year</th>
</tr>
</thead>
<tbody>
<tr>
<td>(A) Did Not Know</td>
<td>$100 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>(B) Reasonable Cause</td>
<td>$1,000 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>(C)(i) Willful Neglect — Corrected</td>
<td>$10,000 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>(C)(ii) Willful Neglect — Not Corrected</td>
<td>$50,000</td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>

The Secretary will take many factors into account when determining CMPs and can modify CMPs when the penalty might not fit the violation. The Secretary will consider all of the following:

- The nature and extent of each violation
- The nature and extent of the harm resulting from the violation
- The number of individuals affected
- The time period during which the violation(s) occurred
- Whether reputational harm occurred affecting an individual's employment, standing in the community, or personal relationships
- The financial condition of the covered entity
- Indications of noncompliance or compliance

Cloud services are unique to each consumer — particularly private clouds tailored to a particular consumer. Thus the cloud services provided may be an important factor in determining CMPs. For instance, some consumers might want to use software as a service (SaaS), thereby relinquishing control of much of their data, including PHI, to the cloud service provider. Consumers might also want to use public clouds. In both cases, cost savings can be realized with efficiencies in data management. However, with these services, a breach — perhaps through a malicious attack or unauthorized access by an insider — might affect many individuals at once in a short time period, whereas a consumer who uses infrastructure as a service (IaaS) or private clouds might be better able to control breaches. (See this article’s [Control of data](#) section for more information.)
However, regardless of the cloud service model — because the OCR decided to amend the Omnibus Rules to read "prior indications of noncompliance" instead of "history of violations" in addition to the affirmative defense noted above — the Secretary seems to have some leeway to consider a cloud provider working with the Secretary in good faith, BAs they might be contracted with, and covered entities to cure or mitigate breaches. Because cloud service providers are unlikely to have a "history of violations," being proactive with compliance could go a long way toward ensuring lower penalties.

Breaches

HHS defines a breach of EPHI as "an impermissible use or disclosure ... that compromises the security or privacy of the protected health information such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual."

Since 2009, EPHI of nearly 21 million individuals has been compromised in large medical-record breaches, defined as breaches that affect 500 or more people (see Related topics). Of the large breaches, 21 percent affected a BA. Additionally, tens of thousands of breaches involving fewer than 500 records have been reported to the OCR.

The most common cause of large-scale breaches was theft (55 percent), followed by unauthorized access to or disclosure of EPHI (20 percent), loss of information (11 percent), hacking (6 percent), improper disposal (5 percent), and unknown/other (3 percent). Figure 1 illustrates this breakdown:

Figure 1. Healthcare data breaches

But perhaps these numbers are misleading. Theft no longer means just theft of paper charts, but also theft of laptops. Likewise, loss of information might mean the loss of a flash drive. And these numbers reflect the state of data breaches in the past; the fact that more and more information is being entered electronically and stored in new formats — including in the cloud — will inevitably change the makeup of these statistics. With migration to the cloud, new methods of malicious attacks to EPHI arise. These attacks now threaten EPHI stored off-site, where those initially entrusted with the EPHI have less control.

Regardless of how a data breach occurs, HIPAA violations come with both criminal and civil penalties on both the state and federal level — penalties that were increased under the HITECH Act. Federally, civil penalties can add up to $1.5 million per year (see Table 1), and criminal
penalties can include 10 years' imprisonment and up to $250,000 in fines. This does not take into account state penalties.

**Breach notification**

Now, BAs are directly liable for breaches that occur to the unsecured PHI in their control and are also required to report these breaches to covered entities (and subcontractors are required to report to the BAs they contract with). Specifically, BAs that access, maintain, retain, modify, record, destroy, or otherwise hold, use, or disclose unsecured PHI must notify the covered entity when it discovers a breach of such information. Reports must be made without delay and in no case less than 60 days from discovery of the breach. The report must provide the covered entity with the identity of each individual whose unsecured PHI has been affected by the breach. BAs may provide notice of the breach immediately and then follow up with further information as it becomes available. Reporting the identity of each individual whose unsecured PHI has been affected may be a difficult task for some BAs like cloud service providers, but the rules do ask that BAs provide the information “to the extent possible.” This standard takes into account that BAs may be unaware of the identification of the individuals whose unsecured protected health information was breached.

Cloud service providers may hold PHI of multiple covered entities. They only need to notify the covered entities to which the breached information relates. However, as may be the case for some providers because of the structure of the cloud (e.g. shared tenant environments), if it is unclear as to which covered entity the breach affects, all covered entities should be notified.

Once the breach has been reported, the covered entity has the ultimate responsibility for notifying individuals affected as well as the Secretary, media or others as required. However, the OCR allows for the entities in their BAAs to define who will notify individuals and how. The OCR encourages covered entities and BAs to define who will take the responsibility of notification and, between themselves, define the requirements regarding how, when, and to whom a BA should provide notification.

Likely, the covered entity is best suited to notify individuals of a breach and not cloud providers who may be subcontractors and far removed from the individuals affected. But, a cloud provider may be in a better position to gather the information the covered entity is required to include in a notification because they hold the EPHI. Thus, the BA is required to provide the covered entity with any other available information that the covered entity is required to include in the notification. While this information may not be available at the time the breach is discovered, again the BA can notify their BA or covered entity of the breach and follow up with further information. And further, to ensure the covered entity is aware of all the available facts surrounding a breach, the Rule also requires that a business associate provide this information even if it becomes available after notifications have been sent to affected individuals.

**HIPAA compliance: Unique issues with the cloud**

Transferring data to the cloud comes with unique issues that complicate HIPAA compliance for covered entities, traditional BAs, and now cloud providers themselves. They include issues of control, access, availability, shared multitenant environments, incident preparedness and response, and data protection, all of which I discuss in the remainder of this article. Although
storage of EPHI in the cloud has many benefits, consumers and cloud providers must be aware of how each of these issues affects HIPAA and HITECH compliance.

**Control of data**

When consumers rely on cloud providers to store their data, they relinquish direct control over that data, starting at the application level. From there, data control is further sacrificed as issues of cloud deployment models are compounded with geographical location of data, which then leads to the issue of who has data access. Knowing who has control of data, and thus who is responsible for that data, is critical to understanding how compliance will be maintained. Because of this shift in control when EPHI is transferred to the cloud, the consumer and provider should explicitly state in a BAA who will then take responsibility for the privacy and security of the data before services are provided.

**Consumers' control of data with IaaS, PaaS, and SaaS**

With IaaS, the cloud provider offers processing, storage, networks, and other resources, enabling the consumer to deploy and run arbitrary software. The consumer controls the operating systems, storage, deployed applications, and perhaps some networking components, and therefore must assume greater responsibility. PaaS enables consumers to deploy their own or acquired applications on the cloud infrastructure using languages and tools supported by the provider, but this leaves the consumer with control only over those applications. With SaaS, the consumer uses the cloud provider's applications and thus has very little control. At each level, the covered entity or BA is choosing to sacrifice control for the opportunity to realize the benefits of services provided. (This article's description of cloud level-of-service models is largely based on the CSA's "Security Guidance for Critical Areas of Focus in Cloud Computing"; see [Related topics](#).)

**Application and infrastructure**

Cloud-computing level-of-service models — software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) — give consumers different levels of control that often involve a corresponding trade-off in security. Both consumers and providers must find the right balance for their organizations and the risk they are willing to assume when forfeiting control of data. Although none of these models gives consumers control of underlying cloud infrastructure, consumers do have more control when they use IaaS, and less control when they use PaaS and SaaS, respectively. What remains unclear when an agreement is entered into at any application or infrastructure level is whether the responsibility for data is transferred to the cloud provider in part or in full because the original data owner no longer has full control. The implication for compliance with HIPAA and HITECH is that whoever has control of EPHI data bears an increased responsibility for access security, data-breach monitoring, audits, and risk management, to name a few areas.

**Deployment models**

Regardless of application or infrastructure level, cloud deployment models themselves affect control of data. With a public cloud model, the infrastructure is open to the public and thus inherently control is lost when data is deployed. At the other end of the spectrum, the infrastructure of a private cloud is open only to a single consumer. A community cloud is open to a specific community, and a hybrid cloud uses both public and private cloud models. For the greatest level of control and thus the greatest privacy and security, a private cloud model should be used for EPHI.
However, public clouds can be used to store EPHI, and in fact the Centers for Disease Control have used such a model for syndromic surveillance data (see Related topics). However, using the public cloud exposes EPHI to more vulnerabilities, so consumers that choose to use this model should exercise extra consideration.

Many cloud providers are realizing the unique nature of EPHI and are changing their deployment models to offer cloud services that are particularly attuned to storing EPHI. For instance, some providers have segregated part of their cloud services particularly for EPHI-related data. Still, many have not, and such services might come at a cost consumers are unwilling to pay. Therefore, as with application and infrastructure levels, consumers are choosing the degree of risk they are willing to take on by deploying on public, private, community, or hybrid cloud models. Regardless of where consumers deploy, cloud providers are still under obligation to keep EPHI private and secure as per HIPAA and HITECH regulations, considering the control they possess of that data.

Geographical location

Cloud services allow for data to be stored in multiple locations, which can be beneficial if an emergency (such as a power outage, fire, vandalism, system failure, or natural disaster) occurs. Storing data in a different location from where the consumer operates — or, if made redundant or backed up — in several locations, can provide reassurance that critical business operations will not be interrupted.

However, consumers that do not know where their data resides lose control of EPHI at another level. Knowing where their data is located is essential for knowing which laws, rules, and regulations must be complied with. Certain geographical locations might expose EPHI to international laws that change who has access to data in contradiction to HIPAA and HITECH laws.

Data access

Considering that a consumer loses control over data at several levels, the issue then becomes who then has access to it and how to manage access. Following the minimum necessary rule, access to EPHI must be restricted to only those with a need to access it. But because data maintained by a cloud provider might be stored in several locations — with each location having its own employees, if not contracts with third parties — this can be complicated. Because of the number of entities involved, more and more individuals have the opportunity to access EPHI in the cloud, exposing the data to increased security risks.

Cloud providers and consumers must work together to ensure security by implementing and managing the creation and modification of access privileges. This starts with determining whether a user or computer system has the right to carry out a certain activity such as reading a file or running a program.

Granting access to personnel

It is the consumer's responsibility to define who should have access to the data it stores in the cloud, and the cloud provider's responsibility to enforce these decisions. But in general, all
employees who might have access to EPHI should undergo workforce clearance procedures. Consumers, cloud providers, and those the cloud providers work with should create job descriptions that accurately reflect each individual's assigned duties and responsibilities, and implement supervision.

All employees who are granted access to EPHI in the cloud — whether as employees of the cloud provider or consumer — should be given unique user names and trained as to how to keep their login information confidential, on top of receiving formal training on the Privacy and Security Rules. Each user should be granted access as per his or her defined role, and access privileges should be immediately modified or revoked as needed.

**Authentication**

Under HIPAA, procedures must be implemented to verify that a person or entity seeking access to EPHI is the one claimed. This can be done through the login system, including an employee's unique user name and password or other metrics. But because administering multiple logins for both a consumer's system and the cloud provider's system can be cumbersome, some cloud providers offer integration with the consumer's in-house authentication system. This can be done through Lightweight Directory Access Protocol (LDAP) mechanisms or by using single-sign (SSO) technologies. However, these methods might themselves introduce other security risks.

Cloud providers can also use Security Assertion Markup Language (SAML) to perform real-time authentication, authorize transactions, and to grant and revoke user access. But, according to the NIST Guidelines on Security and Privacy in Public Cloud Computing (see Related topics), SAML might not be enough, and cloud providers might also use eXtensible Access Control Markup Language (XACML) "to adapt cloud consumer privileges and maintain control over access to resources."

**Auditing access**

Most important in terms of access, both cloud providers and consumers need to agree on access-auditing procedures. The Security Rule requires the regular review of records of information system activity — such as audit logs, access reports, and security incident tracking reports — so that any inappropriate disclosure of EPHI can be discovered. Also, hardware, software, and/or procedural mechanisms must be implemented to record and examine activity in information systems that contain or use EPHI. The HITECH Act further requires monitoring for breaches of EPHI. This is an important consideration for HIPAA and HITECH regulations, because it applies to incident response and breach notification laws and ultimately the ability to stop and then mitigate any breaches.

**Integrity**

Integrity of EPHI is affected by who has access to data. Not only must consumers and providers establish who has access to EPHI that is stored in the cloud, but it is also important that the integrity of data be maintained and protected from fabrication. In fact, integrity is one of the primary goals of the Security Rule. The Security Rule defines integrity as "the property that data or information have not been altered or destroyed in an unauthorized manner." When EPHI is
stored in the cloud, access to EPHI is increased in a number of ways. Consequently, ensuring the integrity of data is ever more difficult.

**Shared multitenant environment**

Public cloud services can offer cost savings because the infrastructure often includes shared multitenant environments, whereby consumers share components and resources with other consumers who are unknown to them. But this feature comes with many associated risks, including the opportunity for one consumer to access the data of another, and the possibility that data could be co-mingled. Additionally, in a shared multitenant environment, usage by one consumer might decrease the availability and performance of resources for another, and cloud provider upgrades or patches might interfere with consumers' business operations. Furthermore, shared infrastructure comes with the risk that cloud providers might not be able to separate the activity of one tenant from that of another. This then has implications for access monitoring and audits and for data deletion, which are both crucial to maintaining compliance with HIPAA and HITECH. To address these issues, cloud providers should clearly define their isolation approaches, which could include virtualization technologies, application-level isolation, or database-level isolation.

**Availability of data**

One of the tenets of the Security Rule is availability of EPHI, particularly in the face of an emergency or other incident. One of the benefits of moving EPHI to the cloud is that cloud services can increase the availability of data in various ways. Cloud services that store redundant data in multiple locations can be better able to recover from emergencies. In addition, on-demand resource capacity allows for resiliency when service demands increase and can enable the platforms to minimize scheduled service interruptions for patching and maintenance. Furthermore, cloud services can mitigate denial-of-service attacks, which can render data unavailable as multiple, bogus requests saturate a target, preventing responses to legitimate requests in a timely manner.

Finally, cloud services can be delivered over the Internet or a virtual private network (VPN) using a web browser or an application supplied by the cloud provider — in other words, interfacing services. However, interfacing can expose EPHI to risks that data will be intercepted while in transit, falsification or corruption of data, and authentication risks at client and server endpoints. The Open Web Application Security Project (OWASP) has a list of the Top 10 web application vulnerabilities that should be addressed in the architecture and design of applications and throughout the software-development life cycle (see Related topics).

**Incident preparedness and response**

Incident response can be a key issue for HIPAA and HITECH compliance. Knowing that not all incidents — whether disasters, unauthorized access, theft, hacking, loss, employee error, or others — can be prevented, regardless of the number of safeguards implemented, the Privacy and Security Rules emphasize:

- The importance of incident response and mitigation of damages
• Limiting interruptions in critical business operations
• Maintaining security and privacy of EPHI

Incident preparedness
Even before an incident occurs, consumers and providers must have in place certain policies and procedures, such as contingency plans. They must also be proactive in monitoring for threats and vulnerabilities. The first safeguard required by the Security Rule is to perform a risk assessment. Consumers should perform their own risk assessments regularly both for data stored in-house and data stored elsewhere, such as in the cloud. Additionally, cloud providers should perform risk assessments of their infrastructure. Any vulnerabilities discovered should be documented. In the case of cloud providers, these vulnerabilities should be reported to consumers so that they can determine if the risks associated are acceptable or how to address the vulnerabilities.

Along with identifying the location of EPHI and performing a risk assessment, consumers must ensure that their data is backed up. More specifically, a "retrievable exact copy" of the EPHI must be created and maintained. Cloud services provide off-site data backup that can help meet this requirement. But the issue of where it is backed up remains, as well as how to gain access to that backed-up data, how recently it was backed up, and how long it is retained.

Also, as noted previously, access management is important. Consumers and cloud providers must monitor access and ensure that only those who are authorized and can be authenticated can access EPHI. Users who should no longer have access must be removed from the user list.

Finally, cloud providers and consumers should continually test for vulnerabilities and revise their policies and procedures accordingly. Cloud providers should immediately report any changes they make or issues they find as a result of these tests to their consumers.

Incident response
The cloud provider plays an integral role in incident response and should be responsible for incident verification, incident analysis, containment, data collection, preservation, problem remediation, and service restoration. As mentioned previously, access to audit logs is one of the crucial first steps in attack analysis and incident response. After the provider reviews these logs and other forensic information, its containment efforts should move forward while it keeps in mind the need to ensure confidentiality, integrity, and availability of EPHI. With the use of redundant or backed-up data, the cloud provider might be able to remediate or restore to an earlier state.

Consumers should outline what they expect from cloud providers in the event of an incident — in particular, how the incident will be verified and how the information to analyze the incident will be gathered. Additionally, consumers and cloud providers should discuss recovery-time objectives and recovery-point objectives, as well as ensure that both can respond in a coordinated fashion.

Data protection
Data that is in transit, at rest, or backed up can be protected in several ways. Most protection measures should be undertaken by cloud providers because they control EPHI. These measures include monitoring for data breaches, encryption, key management, and data deletion.
Monitoring for data breaches

Because consumers give control of data to the cloud provider, they must rely on the processes the cloud provider uses to monitor its systems for data breaches. These might include use of firewalls, network intrusion detection, server-log monitoring, and end-user access-file monitoring. Whichever methods they use, cloud providers should regularly perform checks to ensure they are working properly. And if a breach is detected or a vulnerability found, the cloud provider must report it to the consumer.

Encryption

Entities can encrypt data to render it unusable, unreadable, or indecipherable to unauthorized individuals. Under the Security Rule, EPHI encryption consists of “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key” and that the confidential process or key that might enable decryption has not been breached. According to the OCR, consumers and cloud providers can use encryption processes tested by NIST that are deemed valid. For data at rest, data encryption should be consistent with NIST Special Publication 800-111; for data in motion, data encryption is valid when it complies with NIST Special Publications 800-52 and 800-77 (see Related topics).

Key management

Encryption key management schemes are another means of securing data. This tool can be used by consumers or offered by cloud providers. Although some have adopted key management, industry standards are still emerging such as those by the Institute of Electrical and Electronics Engineers (IEEE) and the Organization for the Advancement of Structured Information Standards (OASIS), developer of the Key Management Interoperability Protocol (KMIP). Those already using key management schemes must take several considerations into account, including how to keep key stores secure, limiting access to key stores, and ensuring they implement backup and recovery solutions.

Data deletion

Under the Security Rule, covered entities and BAs must "implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored." Therefore, when requested, cloud providers must ensure that EPHI will be properly deleted and cannot be re-created, including from backup copies. Such data sanitization can involve expunging EPHI from storage media by overwriting, degaussing, or other means. The OCR considers the media on which EPHI is stored or recorded to be cleared, purged, or destroyed when the NIST Guidelines for Media Sanitization are followed. In a public cloud, physically collocated or commingled data can complicate data destruction and require extra effort.

Directions forward

The Omnibus Rules modifying HIPAA Privacy and Security Rules, the Breach Notification Rule, and Enforcement as required by the HITECH Act significantly change the role and responsibilities
of business associates and subcontractors. The definition of BA now includes subcontractor and
emphasizes that merely maintaining PHI on behalf of a covered entity or another BA subjects the
BA to regulation. As such, BAs — of which cloud service providers are included — must consider
undertaking new steps to ensure compliance with HIPAA and the HITECH Act or face steep
penalties.

Because cloud service providers as BAs are directly liable for breaches, they should immediately
perform risk assessments of the PHI they create, receive, maintain, or transmit — looking for
vulnerabilities and addressing them with haste. Cloud service providers should also perform
internal audits of their policies and procedures to ensure compliance with the Privacy and Security
Rules. Employees should undergo appropriate training of these Rules and a Privacy Officer and
Security Officer should be appointed so that employees can immediately report incidences they
become aware of. Business Associate Agreements should be updated as discussed above to
define roles and responsibilities between all parties and should cover everything from the services
provided to who will notify individuals of a breach of unsecured PHI.

To best achieve compliance, cloud services providers should follow the OCR Audit Protocol (see
Related topics), which covers: Privacy Rule requirements; the Security Rule requirements for
administrative, physical, and technical safeguards; and requirements for the Breach Notification
Rule. This comprehensive tool was developed specifically for covered entities and BAs, containing
the requirements to be assessed through audits the OCR is required to perform under the HITECH
Act.

The Omnibus Rules are an extension of the concepts first embodied in HIPAA to protect sensitive
information about patients' health and to ensure that this data is available and correct when
needed for treatment. In undertaking responsibility of PHI as BAs or subcontractors, cloud service
providers are now held to the same standards as covered entities — particularly the providers in
whom the patients place their trust. Through understanding and clearly defining its role as a BA or
subcontractor, a cloud service provider can not only avoid harsh penalties, but also preserve its
reputation as a reliable partner in healthcare.

Ultimately, responsibility is important not only for HIPAA and HITECH compliance but also for
ensuring trust. A doctor entrusts a BA with critical information shared by patients who have
divulged their most intimate details and whose EPHI might be stored in the cloud. If their EPHI is
compromised, patients might lose trust in their doctors and consequently their care might be put
at risk. Thus, the significance of HIPAA and HITECH goes beyond law. EPHI is not merely data; it
represents individuals, their health, and their lives.
Related topics

- HIPAA and the HITECH Act:
  - Health Information Accountability and Portability Act: Public Law 104-191
  - Final Rule Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules (Final Rule)
  - HIPAA Privacy Rule: 45 CFR Part 160 and Part 164, Subparts A and E
  - HIPAA Security Rule: 45 CFR Part 160 and 164, Subparts A and C
  - OCR HIPAA Audit Program Protocol
  - Health Information Technology for Economic and Clinical Health Act: Public Law 111-5
  - HITECH Breach Notification Interim Final Rule
  - HITECH Act Rulemaking and Implementation Update
- AHIMA Analysis of Omnibus Rules: The American Health Information Management Association has published this analysis of the HIPAA Omnibus Rules.
- HIPAA Omnibus Rule Reference Chart: This chart compares the proposed and final HIPAA Omnibus Rules.
- Understanding Health Information Privacy: Read about the HIPAA Privacy Rule and Security Rule on the HHS website.
- HIMSS Cloud Security Toolkit: The Healthcare Information and Management Systems Society (HIMSS) offers the Cloud Security Toolkit to help organizations understand cloud computing and prepare for the relevant security risks, opportunities, and implementation challenges.
- "6 reasons healthcare organizations should archive to the cloud" (Michelle McNickle, Healthcare IT News, June 2012): This article outlines the benefits to healthcare organizations of archiving in the cloud.
- The High Cost of HIPAA Violations: As this page shows, HIPAA violations by covered entities and even individuals can incur surprisingly high penalties.
- Slideshow: 10 biggest HIPAA data breaches in the U.S.: Details about the biggest HIPAA breaches in the United States as of September 10, 2012.
- "Large medical-records breaches affect nearly 21 million: OCR" (Joseph Conn, ModernHealthcare.com, August 2012; free registration required) and "OCR Reports Over 21 Million Impacted by Large-Scale Breaches" (Chris Dimick, Journal of AHIMA, September 2012): These two articles summarize the OCR’s data on breaches.
- Cloud Security Alliance: CSA promotes best practices for providing security assurance within cloud computing, and provides education on the uses of cloud computing to help secure all other forms of computing.
• **Privacy Rights Clearinghouse**: Privacy Rights Clearinghouse is a consumer-information and consumer-advocacy organization.
• **DataLossDB**: The Open Security Foundation's DataLossDB is a research project aimed at documenting known and reported data-loss incidents worldwide.
• **OWASP Top Ten Project**: The OWASP Top Ten represents a broad consensus about the most critical web application security flaws.
• **Evaluate IBM products** in the way that suits you best: Download a product trial, try a product online, or use a product in a cloud environment.