



Making Sense of the Healthcare Cloud's Confusing Shared Responsibility Model



Making Sense of the Healthcare Cloud's Confusing Shared Responsibility Model

Table of Contents

Page 2

HIPAA Security Rule

The Business Associate
Agreement

Page 3

The Fundamental Purpose of a
BAA is to Protect Patient Data

Page 4

Cloud Service Models

Page 5

Cloud Infrastructure Models

Page 6

Key Roles in Data Ownership

Page 7

Shared Responsibility

Page 8

The RACI Matrix

Page 9

Best Practice Tips for Ensuring
a Secure & Compliant Cloud

Conclusion

As cloud adoption in healthcare increases, many organizations grapple with understanding who is responsible for the confidentiality, integrity, and availability of protected health information (PHI) as it moves across the cloud supply chain. To help resolve any confusion, it is first important to review some fundamental aspects of HIPAA compliance, Business Associate Agreements (BAA), and cloud service models. We will also examine key roles in the data ownership chain.

HIPAA Security Rule

HIPAA was originally designed to make insurance information portable. The HIPAA Security Rule, the Privacy Rule and Breach Notification Rule were designed to ensure certain rights to patients relative to the privacy of their personal health information (PHI). Over time, HIPAA has evolved to be more inclusive of the patient's right to receive notice of a healthcare provider's privacy practices, and to receive a copy of, review and amend their information. Patients also have the right to file a complaint if they feel their information has been mishandled.

The Business Associate Agreement

Under HIPAA, a Business Associate Agreement (BAA) is a contract between a HIPAA covered entity and a HIPAA business associate (BA). The contract protects personal health information (PHI) in accordance with HIPAA guidelines. In the context of cloud-based solutions, business associates would include cloud-based software providers, infrastructure providers, cloud managed services providers, data center operators, and other entities. That means they must also comply with HIPAA security and privacy rules.

The fundamental purpose of the BAA is to protect patient rights. To that end, the three major obligations of a BAA are:

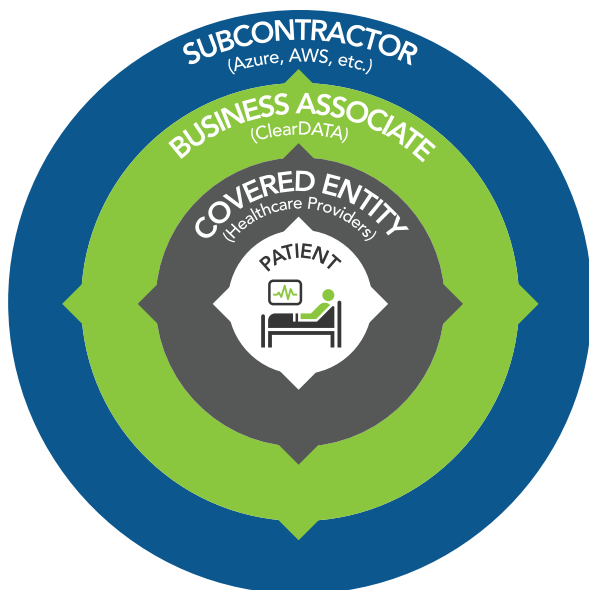
- Conduct a Security Risk Analysis
- Establish Policies & Procedures that help ensure patient rights
- Define security breach liabilities and reporting responsibilities for covered entities, the business associate and any subcontractors.

In 2013, under the Omnibus rule, HIPAA compliance and establishing a BAA became a requirement for cloud providers. However,

many of the BAAs were designed for specific type of cloud deployment model. As new cloud deployment models have emerged and existing models have evolved, these existing BAAs are not necessarily inclusive of what a Covered Entity or Business Associate needs for a proper shared responsibility model.

The BAA has always been a requirement for the Covered Entity. But as healthcare moves to the cloud with new service models, it is also a responsibility to have a BAA with business associate subcontractors.

The Fundamental Purpose of a BAA is to Protect Patient Data



BAA Obligations Flow Outward

- The Covered Entity must enter into a BAA with a Business Associate
 - The Business Associate must have a BAA with Subcontractors
 - Three Major Obligations of a BAA:
 1. Facilitate Patient Rights
 2. Complete Risk Analysis, Policies and Procedures
 3. Report Breaches and Liability
-

Many Clouds, Many Service Models

Cloud Service Models

There are two primary factors that contribute to the confusion around shared responsibility for protecting PHI. First, there are now multiple cloud types, including private, public, hybrid, and community clouds - each with varying levels of security and privacy expertise, and each with benefits and drawbacks.

Private Cloud: A cloud infrastructure that is owned or leased by a single organization.

Community Cloud: A cloud infrastructure that is shared by several organizations within a single community.

Hybrid Cloud: A combination of two or more different cloud models.

Public Cloud: A cloud infrastructure owned by an organization that sells cloud services publicly to other companies. Amazon Web Services is an example of a public cloud.

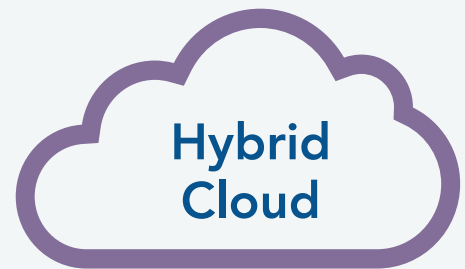
The less control the healthcare organization has over the infrastructure, platform, application, or other elements of the solution, the more HIPAA compliance responsibility is shared with the cloud provider.



- Owned or leased by a single organization
- Operated solely for that organization



- Shared by several organizations
- Supports a specific community



- Combination of two or more cloud models



- Owned by an organization selling cloud services
- Sold to the public or large organizations

Cloud Infrastructure Models

There are also several different types of cloud service models, which offer varying levels of control to the customer. The less control the healthcare organization has over the infrastructure, platform, application, or other elements of the solution, the more HIPAA compliance responsibility is shared with the cloud provider. There are three general cloud service models:

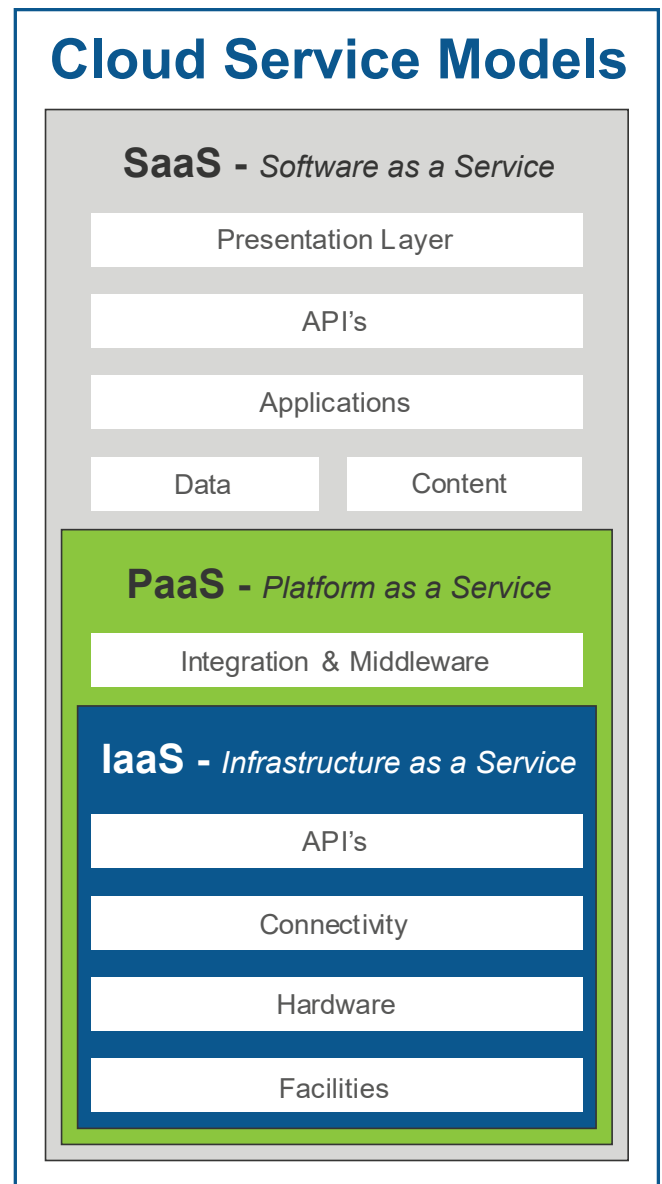
Infrastructure as a Service (IaaS) provides on-demand compute resources, networking and storage capabilities. IaaS includes the full IT foundation, with infrastructure facilities that include hardware, storage, networking, and APIs. IaaS allows self-service provisioning of resources, control of the operating system, and the ability to deploy and run arbitrary software.

Platform as a Service (PaaS) includes integration with other systems, and middleware, but provides less control than IaaS. Users can develop, run, and manage applications on a cloud-based infrastructure.

Software as a Service (SaaS) provides access to a presentation layer for applications and data, but little control over the underlying infrastructure.

Organizations can access applications at less cost than purchasing software outright, but they have no control over the underlying infrastructure (including the network, servers, operating system, storage, etc.).

Key questions to address in the planning stages are which type(s) of clouds to use, and which type of service model is best suited to your organization's business priorities, in-house IT expertise and resource constraints, and privacy and security needs when selecting one or a combination of clouds and service models.



Key Roles in Data Ownership

In the previous section discussing the HIPAA Business Associate Agreement (BAA), we identified the three main parties handling data:

- 1 Healthcare entities** (hospitals and other care providers known as “covered entities” in HIPAA terms).
- 2 Business Associates (BAs)** supply the underlying cloud infrastructure or other services. The best BAs take responsibility for facilitating patient rights, completing risk analysis, safeguarding patient data, and reporting breaches and liabilities. BAs are also responsible for monitoring and working with their own service providers and contractors to do the same.
- 3 Subcontractors** that supply additional infrastructure or services, mostly to BAs, are the third main entity.

Each of these parties have varying responsibilities in the data ownership chain, depending on the specific cloud infrastructure and service model. We define these key data ownership roles as follows:

- **Data subject:** an individual who is the subject of personal data (typically the patient)
- **Data controller:** a person (alone or jointly with other persons) who determines the purpose for which, and the manner in which, any personal data may be processed
- **Data processor:** any person (other than an employee of the data controller) who processes data on behalf of the controller
- **Data stewards:** responsible for data content, context, and business rules
- **Data custodians:** responsible for the safe custody, transport, storage of the data, and implementation of business rules
- **Data owner:** holds legal rights and complete control over a single piece or set of data elements. Data owners also define distribution and policies.



Shared Responsibility

With so many parties, cloud models and roles involved, things can sometimes get confusing for the covered entity. While understandable, it is crucial to understand that the covered entity itself is ultimately responsible for safeguarding patient data. The stakes are high, because data loss—no matter who has caused it along the healthcare continuum or contributor to the cloud infrastructure—can be extreme, including hefty fines and great harm to reputation.

Varying levels of responsibility and liability may be shared among the covered entity, the cloud provider, and their subcontractors. The BAA should reflect the model and responsibilities of the cloud provider. Each type of cloud service has its own benefits and drawbacks, and different levels of control available to the healthcare organization. General examples for each cloud service model would be:

SaaS: The cloud-based software provider would take on the responsibility of safeguarding data, and the BAA would require enough detail to cover that responsibility. The SaaS provider should be responsible for compliance of the compute resources, storage, encryption, and platform.

PaaS: In this case, the PaaS provider would be responsible for the compliance of the underlying infrastructure (including the operating system), while the covered entity bears responsibility for the applications and (possibly) some configuration settings in the application hosting environment.

IaaS: The covered entity has control and responsibility over the operating system, some networking components, and the application software. The IaaS provider would be responsible for compliance of the underlying infrastructure.

A managed cloud services provider, such as ClearDATA, would responsibility for the platform, operating system, network, firewall, client-side data encryption, server-side encryption, network traffic protection, and other elements.

Remember: The covered entity is ultimately accountable (and liable) for protection of the PHI, even if a business associate (such as a cloud services provider) bears the responsibility of executing the processes necessary to ensure that protection.

The stakes are high, because data loss—no matter who has caused it along the healthcare continuum or contributor to the cloud infrastructure—can be extreme, including hefty fines and great harm to reputation.

The RACI Matrix

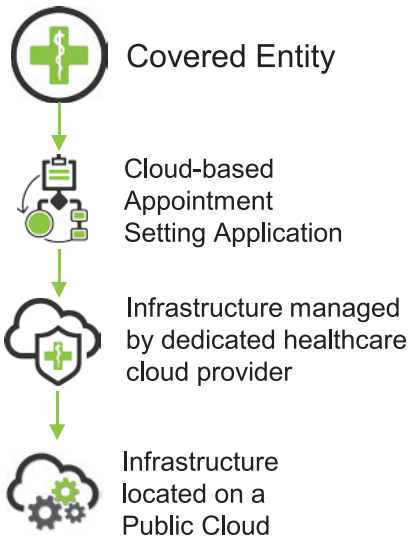
When developing BAAs with cloud providers, an excellent approach is to utilize a responsibility assignment matrix, also known as a RACI matrix to determine which parties are Responsible, Accountable, Consulted, or Informed.

A cloud services provider and their business associates & subcontractors may share some responsibility and accountability with the covered entity, depending on the cloud model involved. For example, in the chart below you can see what a RACI matrix would

look like for a covered entity that deploys a cloud-based appointment setting application via a business associate (i.e., a developer) that is on infrastructure managed by a dedicated healthcare cloud provider.

Create a RACI with your provider up front to map out these responsibilities. The RACI can even be included in the service level agreement and reviewed on a regular basis to ensure each party is meeting these requirements.

IaaS Deployment RACI

Use Case Scenario	Task	Covered Entity	Business Associate	Services Provider	
 <p>Covered Entity</p> <p>Cloud-based Appointment Setting Application</p> <p>Infrastructure managed by dedicated healthcare cloud provider</p> <p>Infrastructure located on a Public Cloud</p>	IaaS	Provision Storage Account	I	C, I	A, R
		Provision IaaS Networking	I	C, I	A, R
		Firewall Management, Configuration	I	C, I	A, R
		Breach Notification Plan	I	C, I	A, R
		Data Encryption at Rest & In Flight	I	C, I	A, R
		Provision IaaS Virtual Machine	I	C, I	A, R
		OS Deployment & Hardening	I	I	A, R
		OS Security Patch Management	I	C, I	A, R
		Backup	I	C, I	A, R
		Antivirus/Antimalware, Endpoint Protection	I	I	A, R
		App Installation, Configuration	I	C	A, R
		Monitoring (fabric, OS, app platform)	I	C, I	A, R
		Monitoring Alerting / Notification	I	I	A, R
		Desired State Configuration	I	C, I	A, R
Vulnerability Scanning	I	I	A, R		
Apps	Provision Application Services instance	I	A, R	I	
	CMS Install, Setup, and Maintenance	I	A, R	C, I	

Best Practice Tips for Ensuring a Secure & Compliant Cloud

There's little left to debate about the benefits of moving to the cloud; chiefly, alleviating the need to build and maintain an in-house IT infrastructure and take on patient security and privacy alone. But there are cloud providers who are true data security and privacy experts, and share in the responsibility for the safe custody, transport, storage of the data, and implementation of business rules. These companies are also capable of helping covered entities navigate the various cloud models (private, public, community, and private) to help align business models to the covered entity's business needs.

Additional Best Practice Tips

- Hire an in-house auditor to gauge security, privacy, and performance
- Bring on a BA that is HITRUST certified and will intelligently assist with the choices required on the journey to the cloud
- Find a BA capable of conducting comprehensive security risk assessments (SRAs) and implement the recommendations they provide
- Decide on the best level of service orchestration (IaaS, PaaS, and/or SaaS)
- Get solid business support that includes provisioning and configuration, as well as interoperability
- Insist on the highest levels of security and privacy expertise to avoid fines, penalties, and reputation risks

Conclusion

Remember that the covered entity has ultimate responsibility for the confidentiality, integrity, and availability of sensitive patient data. With the move into the cloud, it is essential to select partners who will share in this responsibility. Look for a cloud provider with complete control over the infrastructure, the knowledge of how to work with other infrastructure providers and contractors, and security and privacy expertise that meets or even exceeds your own so they can become a true partner in your journey to the cloud. Remember that this is a journey, and will take time and expertise. In the end, it is well worth the effort.



About Us

ClearDATA is the nation's fastest growing healthcare cloud computing company. More than 310,000 healthcare professionals rely on ClearDATA's HIPAA compliant cloud computing HealthDATA platform and infrastructure to store, manage, protect and share their patient data and critical applications.

For more information

101 West 6th Street, Austin TX



(800) 804-6052



www.cleardata.com

