**International Journal of Artificial Intelligence, Data Science, and Machine Learning**
Grace Horizon Publication | Volume 6, Issue 4, 9-13, 2025
ISSN: 3050-9262 | https://doi.org/10.63282/3050-9262.IJAIDSML-V6I4P102

*Original Article*

# BAAs in the Cloud: Securing HIPAA-Compliant EMR Hosting

Devika Jagarlamudi[1], Harshith Kumar Pedarla[2]
[1] Product Manager, CurerTech, Chicago, USA.
[2] Software Developer, Amazon, Seattle, USA.

***Received On: 13/08/2025*** ***Revised On: 17/09/2025*** ***Accepted On: 25/09/2025*** ***Published On: 13/10/2025***

***Abstract*** *- The wide use of the cloud in the healthcare field has brought about the redesigning of EMR (Electronic Medical Records) storage, accessibility and managing. While standing out as the best option, the cloud majorly offers the following among others: ability to scale, cost savings, and Interoperability. It also carries with it some downsides: particularly with the legal aspects, regulatory and the overall security which becomes increasingly complex as HIPAA legislation comes into play. For cloud-based healthcare systems to follow the HIPAA there is a need to forerun with the formalization of a Business Associate Agreements (BAAs) between cloud service providers (CSPs) and those large healthcare systems. Based on whether they are established, this thesis will evaluate the legal consequences of BAAs, analysing if they are enforceable contracts under the federal common law or if there is an easier way to ensure they exist (forcing the parties to really read and understand them). This work further investigates the impact of or roles played by BAAs in assigning liability, defining responsibilities, and reinforcing policies with regards the health's record safety in the cloud infrastructure. It also solves the burden of delivering and maintaining the same infrastructure platforms required by entities, heightening the automation or efficiency, whether economies of convergence and scope.*

***Keywords*** *- Business Associate Agreements (BAAs), HIPAA, Cloud Computing, Electronic Medical Records (EMR), Data Security, Compliance.*

## 1. Introduction

### *1.1. Background*

There is a gigantic digitization of the healthcare sector that has been influenced by cloud computing and big data technologies. EMRs are the core of such transformation because physicians can store, retrieve, and share patient information using them efficiently. Nevertheless, the virtue of EMRs hosted by the cloud poses significant security and compliance difficulties because protected health information (PHI) is sensitive data. The HIPAA law provides stringent privacy protections on PHI, under which the covered entities (healthcare providers) and their business partners (vendors) should guarantee the protection of health data by ensuring confidentiality, integrity and accessibility of health information.

Under the HIPAA, Cloud Service Providers (CSPs) dealing with PHI join business partners and thus are required to sign Business Associate Agreements (BAAs) with covered parties. BAAs are legally oriented contracts, which specify the performance of every party involved with respect to the PHI protection, use, disclosure and breach of notification. In the absence of a legitimate BAA, even the storage of PHI through a cloud platform will be a HIPAA violation. Therefore, both CSPs and healthcare organizations need to be aware of the operations of BAAs in gaining the HIPAA compliant EMR hosting.


**Fig 1: Best HIPAA-Compliant Cloud Storage in 2025**

### *1.2. Problem Statement*

Although cloud solutions become more widely utilized, health care organizations can hardly find ways to go through the maze of HIPAA issues in the domain of a cloud-based solution. Lack of understanding the shared responsibility model or implementation of extensive BAAs usually results in data breaches, judicial fines or service interruptions. There is no clarity on the security responsibilities between the covered entities and CSPs, which also serves to increase compliance risks.

### *1.3. Purpose and Objectives*

*This dissertation aims to:*

- Reproach the legal basis and architectural elements of BAAs in cloud-based EMR hosting.
- Conduct the analysis of shared responsibility approach to HIPAA compliance between healthcare organizations and CSPs.
- Assess technical, administrative and physical security that is needed to host EMRs securely.
- Recommend a governance framework comprising of BAAs, cloud security controls as well as continuous compliance monitoring.

### *1.4. Significance of the Study*

This study will enable healthcare executives, IT managers, and compliance officers to have a good knowledge of the role played by BAAs in HIPAA compliance in cloud-hosted EMR systems. It also provides contribution in policy development and risk management approaches towards secure digital transformation in the healthcare.

## 2. Literature Review

### *2.1. HIPAA and The Relevance in Cloud-Based EMRs*

The HIPAA Privacy, Security, and Breach Notification Rules are the key to data protection of the healthcare sector in the United States. Security Rule demands that covered entities and business associates apply administrative, technical and physical protections in order to protect PHI. As healthcare organizations move the EMRs to CSPs, the compliance requirements are transmitted onto CSPs, which would be responsible for keeping the data safe as a business partner (U.S. Department of Health and Human Services, 2023).

The flexibility of HIPAA premiss to adopt a cloud at the expense of good risk management, encryption, and access control. Compliance is more difficult in the distributed nature of cloud computing which highlights the importance of formalization of contractual and operational controls using BAAs.

### *2.2. Legal Underlying of Business Associate Contracts*

A Business Associate Agreement is a document with contractual arrangements that are necessary according to HIPAA SS164.502(e) and SS164.504(e). It makes certain that the business associates, those entities that produce, receive, store or transfer PHI, adhere to the same protection as covered entities. The BAA should outline the uses and disclosures of PHI that are permitted, require the provision of the breach notification measures, and permit the HHS to inspect the records concerning the implementation.

On the cloud, BAA implements the shared responsibility model by allocating security activities between the healthcare organization and CSP. As an example, the CSP can deal with infrastructure-level security and physical security, whereas the healthcare organization is in charge of identity access management (IAM), and application-layer security.


**Fig 2: HIPAA Business Associate Agreement**

### *2.3. Content and Major Provisions of BAAs*

Typical BAAs contain:

- PHI Use: The scope of PHI use by the CSP provides the allowable and unauthorized use or disclosure of PHI.
- Security Safeguards: Demands adherence to the Security Rule of HIPAA (encryption, audit controls, restrictions of access).
- Breach Notification: Requires timely reporting of data privacy events or unrelated revelations.
- Subcontractor Obligations: Imposes obligations of compliance to any third party contracted by the CSP.
- Termination Clause: specifies an eventuality within which the BAA may be terminated due to non-compliance.
- Liability and indemnification: Provides legal implications of breach or violation.

All these clauses add up to the fact that PHI is safeguarded on its way in the cloud.

### *2.4. HIPAA and Cloud Providers*

HIPAA-eligible services are available with major cloud providers, like Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) who enter into BAAs with covered entities. Nevertheless, signing of an EMR system does not make it compliant, it is important to set it properly, control access, and audit. Misconfigurations like accessible storage buckets on the web still happen as one of the top causes of PHI exposure.

**Fig 3: Cloud Computing in Healthcare**

### *2.5. The Shared Responsibility Model*

Under the model of shared responsibility: The cloud provider captures the point of reference infrastructure (data centres, physical servers, networking, and virtualization sculpture). The healthcare organization or covered entity safeguards the information, applications, user access and settings. Either of the two domains may result in failure that would jeopardize the HIPAA compliance. This division is therefore formalized under the BAA so that there is effective accountability, and uniform application of controls.

### *2.6. Research Done Before and Discovered Gaps*

Although existing research highlights frameworks of security in cloud, limited studies are done to understand the contractual aspect of HIPAA compliance. The encryption, access control or auditing of technology is the subject of most technical research to ignore the way BAAs develop enforceable accountability. That gap is addressed in this dissertation by connecting contractual governance and technical mechanisms of compliance.

## 3. Methodology

The method of analysis applied in this research is qualitative in that it involves legal review, literature review, and an analysis of the cases.

- Legal Analysis: The review of HIPAA laws, HHS regulations, and sample of BAAs of large CSPs.
- Comparison Analysis: BAA Practice Analysis at AWS, Azure, and GCP.
- Case Study: Interpretation of actual cases of data breaches of PHI hosted on the cloud and failures of the BAA.

To triangulate the data, scholarly articles, industry reports and regulatory advisories were used to collect data.

## 4. Discussion and Findings

### *4.1. The Role of BAAs in Cloud EMR Security*

BAAs provide the legal framework of ensuring safety of PHI in the cloud platform. They establish mutual duties and thus make the compliance a measurable and a contract. A good BAA would make sure that business operations are in sync with HIPAA standards by:

- Organizing takeover of data protection functions. Establishing breach response deadlines.
- Imposing compliance on subcontractors. Lending rights of an audit and oversight to the covered entity.

BAA enables the CSPs to legitimately deal with PHI, whereas it lacks makes even the encrypted cloud store a HIPAA breach. The enforcement involves carrying out the action plan.

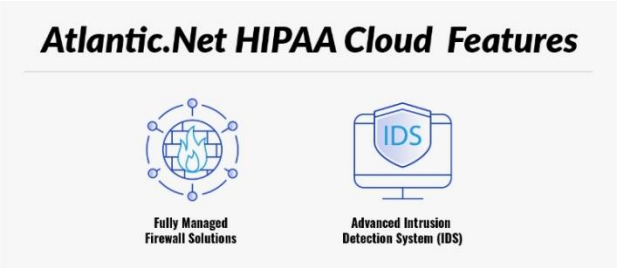


**Fig 4: Understanding HIPAA-Compliant Cloud Computing**

**Table 1: Security Safeguards under BAAs**

| Safeguard Type | Examples |
|---|---|
| Administrative | Security policies, employee training, risk assessments, and access management. |
| Technical | Encryption in transit and at rest, secure API integration, audit logs, and access controls. |
| Physical | Data center security, hardware protection, and redundancy. |

Tools for key management, such as the AWS KMS, Azure Key Vault, and Google Cloud KMS, are offered by a number of CSPs. It is the healthcare organization's responsibility for key rotation and configuration, and therefore it is very important to be very clear about the role of the CSP with respect to the BAA.

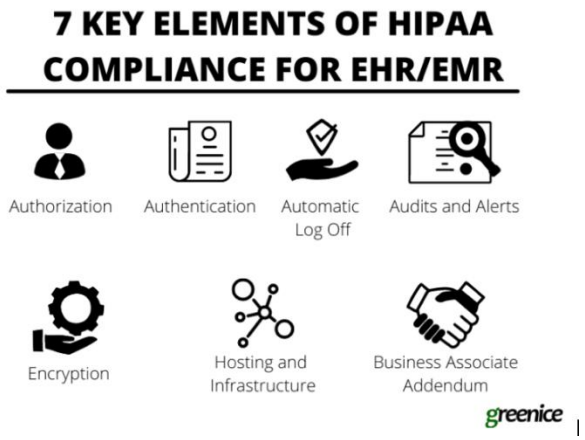


**Fig 5: Compliance Checklist for HIPAA and EMR**

### *4.2. Enforcement and Accountability*

The enforcement refers to the implementation of the action plan. BAAs carry in place accountability enforcers. As an example, they grant covered entities the right to carry out

audit, demand compliance documentation or can end the contract or agreement in case the CSP does not comply with HIPAA standards. The legal necessity of the agreement is supported by the punishment given to various healthcare providers who use cloud or communication tools without BAAs by the U.S. Department of Health and Human Services (HHS).

### *4.3. Shared Responsibility Model Practicum*

Although CSPs have been seen to guarantee infrastructure protection, it is the responsibility of healthcare organizations to:

- User Authentication and Authorization: The use of IAM, MFA, and least-privilege access.
- Data Classification: Determining datasets with PHI.
- Configuration Management: Preventing the exposure of data repositories to the general public.
- Incident Response: Checking and reporting breaches in line with the terms of BAA. Failure in these areas is normally as a result of human mistakes or non-observation as opposed to technical insufficientness.

### *4.4. Multi-Cloud and Hybrid Cloud*

The growing trend in healthcare organizations is to adopt hybrid and multi-cloud architecture in order to obtain resiliency and vendor diversification. This however makes it difficult to manage compliance since there may be several CSPs working on PHI at the same time. All providers should have their own BAA, and the healthcare organization should have standards of control in environments. The incompatibility of various BAAs may result in duplications and conflicting duties, and the risk of legal and operational hazards.

### *4.5. Case Study: BAA Gaps and Cloud Misconfiguration*

Another action that caused a PHI breach was registered in 2022, when a healthcare analytics company in the U.S. had to tackle a cloud storage service by severely misconfiguring it. The covered entity had not implemented encryption and access controls as outlined in the shared responsibility framework even though it had signed a BAA, despite the stipulated requirements. It is pointed out by the incident that a BAA is as efficient as it is enforced. Continuous Compliance Monitoring. The compliance in HIPAA of the cloud is dynamic rather than point in time. Continuous risk assessment, use of automated compliance tools, and frequent security audits should be used to complement BAA. CSPs offer compliance dashboards (e.g., AWS Artifact, Azure Compliance Manager) which help in writing down compliance with the requirements of the BAA. The frequent review shows that both the parties uphold their responsibilities throughout the lifecycle of the system.

## 5. Challenges and Limitations

### *5.1. Legal Ambiguity Although the HIPAA Requirements of Cloud Interpretation Are Still Complicated*

BAAs are usually inconsistent in their scope and language that leads to inconsistency in implementation. Smaller healthcare establishments might not be able to negotiate broad contracts because of the lack of legal expertise.

### *5.2. Lock-In by Vendors and Transparency*

CSPs might provide inflexible BAAs that are standardized. Such a take-it-or-leave-it strategy limits customization and can be unable to cover all applications. Also, healthcare entities rarely have an insight into the inner workings of the CSP and can be restricted in its capacity to ensure compliance on top of the contractual guarantees.

### *5.3. Technological Complexity*

The use of encryption, identity management, and access control that spans through various cloud setups is not an easy task. Healthcare organizations have to invest in the automation of security and personnel training to ensure compliance. Unless there is strong governance, chances of human error are too high.

### *5.4. Resource and Cost Constraints*

Constant surveillance, third party audit, and litigations are expensive to maintain operations. Without either cheap managed services or shared responsibility tools, smaller providers can struggle to remain compliant.

## 6. Recommendations

### *6.1. Strengthening BAAs*

*Healthcare organizations are supposed to:*

Establish responsibilities of data owner, deadline to notify breach and limit liability. Add on-demand specifications regarding subcontractor compliance and right-to-audit. Ordinarily, assess BAAs to correspond to changing HIPAA and state regulations.

### *6.2. Installing a Governance Framework*

*The fundamental governance system must include:*

- Legal: This is done by ensuring that there are valid BAAs with all CSPs and vendors.
- Technical Controls: Adoption of encryption, access management as well as monitoring tools.
- Administrative Control: Policy, training and documentation.
- Continuous Compliance: Performing detection of violations through automated tools to ensure the tracking of configurations.

### *6.3. Improving Cooperation in Vendors*

Covered entities are supposed to form a strategy partnership with CSPs as opposed to being transactional vendors. A trusting culture and proactive compliance The trust and compliance management is achieved through joint risk assessment, sharing of the audit outcomes, and open communication.

### *6.4. Adopting Automation and AI*

Security analytics and automated compliance solutions can be used to help improve breach detection and compliance monitoring. These tools will be able to continually compare system settings to HIPAA-specified requirements and alert whenever deviations occur before

they cause a violation. This term distinguishes two groups, namely, promoting interoperability and standardization. The structure of standardized BAAs and reports of compliance in the industry can somewhat eliminate ambiguity and administrative workload. There must be co-operation between regulators, CSPs and healthcare providers to develop the best practices.

## 7. Conclusion

### *7.1. Summary of Key Insights*

The present dissertation has discussed the invaluable contribution of Business Associate Agreement to the achievement of HIPAA-compliant EMR hosting in cloud environment. BAAs do not only create legal responsibility between covered entities and cloud service vendors but also outline the basis of adopting joint security responsibility. It can be seen that BAAs institutionalize compliance requirements, but it requires regular implementation of operational safeguards using technical and administrative tools to be effective.

### *7.2. Legal and Technological Compliance Intersection*

The legal documentation, however, is not the only way to consider HIPAA compliance in the cloud: alignment between contractual requirements and technical controls is a required requirement to be performed continuously. The application of encryption, management of identities and audits logging should be in five or six dimensions with the requirements of the BAA and that of the PHI protection. Such a combined solution will make sure that both sides of the case can have a justifiable stand whenever a regulatory board audits its operations or when an investigation into a breach is conducted.

### *7.3. Future Outlook*

With the ongoing digitalization of healthcare, the need to have secure and compliant cloud environments will increase. The research of the future should be dedicated to this automation of the compliance control and the creation of AI-based monitoring mechanisms that will be able to enforce BAA provisions dynamically. Moreover, the policymakers might be required to update HIPAA to cover new technologies like AI-based diagnostics and edge computing, so that the BAAs can be not outdated within the healthcare ecosystem development.

## References

[1] Agarwal, S., & Peta, S. B. (2025). From Notes to Billing: Large Language Models in Revolutionizing Medical Documentation and Healthcare Administration. Sch J App Med Sci, 8, 1558-1566.

[2] Al-Marsy, A., Chaudhary, P., & Rodger, J. A. (2021). A model for examining challenges and opportunities in use of cloud computing for health information systems. Applied System Innovation, 4(1), 15.

[3] Ameyed, D., Jaafar, F., Charette-Migneault, F., & Cheriet, M. (2021, December). Blockchain based model for consent management and data transparency assurance. In 2021 IEEE 21st International Conference on Software Quality, Reliability and Security Companion (QRS-C) (pp. 1050-1059). IEEE.

[4] Arumugam, K. J. (2025). Cloud, Care and Confidentiality: The Healthcare Data Security Dilemma. Available at SSRN 5277766.

[5] Atobatele, O. K., Ajayi, O. O., Hungbo, A. Q., & Adeyemi, C. (2023). Enhancing the Accuracy and Integrity of Immunization Registry Data Using Scalable Cloud-Based Validation Frameworks.

[6] Dong, Y. (2022). Blockchain-enabled Secure and Trusted Personalized Health Record.

[7] Evans, A., Singh, A., & Golbin, A. (2025). Navigating Supply Chain Cyber Risk: A Comprehensive Guide to Managing Third Party Cyber Risk. Taylor & Francis.

[8] Gallifant, J., Kellogg, K. C., Butler, M., Centi, A., Doyle, P. F., Dutta, S., ... & Bitterman, D. S. (2025). Beyond the Algorithm: A Field Guide to Deploying AI Agents in Clinical Practice. arXiv preprint arXiv:2509.26153.

[9] Hemapriya, K. E., & Saraswathi, S. (2024). Deep learning-based cloud computing technique for patient data management. In Deep learning for smart healthcare (pp. 143-164). Auerbach Publications.

[10] Huo, M., Bland, M., & Levchenko, K. (2022, November). All eyes on me: Inside third party trackers' exfiltration of phi from healthcare providers' online systems. In Proceedings of the 21st Workshop on Privacy in the Electronic Society (pp. 197-211).

[11] Kansara, M. (2021). Cloud migration strategies and challenges in highly regulated and data-intensive industries: A technical perspective. International Journal of Applied Machine Learning and Computational Intelligence, 11(12), 78-121.

[12] Olorunlana, T. J. (2024). Securing Healthcare Data in the Cloud under HIPAA and NIST Frameworks.

[13] Onwuzuruike, F. E. (2023). Recommendations on how clinicians and healthcare professionals should secure patient data (Doctoral dissertation, Marymount University).

[14] Samant, P. S. (2024). Secure cloud services for the healthcare industry: Addressing unique challenges and ensuring compliance. International Journal of Research and Application of Science, Engineering and Technology, 12(4), 3095-3101.

[15] Vale, T. (2024). Automated snapshot lifecycle management for health it storage.