**Guidance on HIPAA and Resellers of Cloud Computing Services**

**Introduction**

State departments are seeking Cloud Computing Service Providers (CSPs) to complement their technology solutions. U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR) “[Guidance on HIPAA and Cloud Computing](https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html)” defines the specific guidance for CSPs and must be considered for managing all contracts/relationships with CSPs.

One area not covered in the HHS/OCR guidance is working with a “reseller” who has a direct relationship with the CSP. In this scenario, the state department contracts with the reseller for the cloud computing services of a CSP company.

For state departments that are Health Insurance Portability and Accountability Act (HIPAA) covered entities (CE) or business associates (BA), HIPAA obligations must be addressed to ensure the privacy and security of electronic Protected Health Information (ePHI) – specifically, which entity or entities in the CSP contracting relationship should sign the Business Associate Agreement (BAA).

**Guidance**

The California Office of Health Information Integrity (CalOHII) provides the following guidance on how to navigate the contracting arrangements with a reseller of CSP services, focusing specifically who signs the BAA.

There are three parties in this CSP arrangement:

* ***HIPAA CE/BA state entity*** initiating the contract for CSP services
* ***Reseller*** signing the contract/purchase order agreement with the state entity – acting as an intermediary for billing and customer support with the CSP
* ***CSP*** delivering the cloud computing solution for the state entity

Who signs the BAA?

***In all cases, the CSP must sign the BAA*** – since they are creating, receiving, maintaining, or transmitting the ePHI, whether encrypted or not, for the CE/BA state entity.

To determine whether the reseller should sign a BAA, consider the following:

1. Does the reseller ONLY provide the state entity with CSP relationship support, such as the point of contact for payment and contracting?

YES, no BAA is needed.

NO, see next question.

1. Does the reseller provide or support any Treatment, Payment or Operation (TPO) services between the state entity and CSP? Specifically, does the reseller have any access to ePHI, whether encrypted or not? Note: for more information regarding TPO services, refer to HHS/OCR guidance on “[Uses and Disclosures for Treatment, Payment, and Health Care Operations](https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/disclosures-treatment-payment-health-care-operations/index.html).”

NO, no BAA needed.

YES, a BAA with the reseller is needed.