Okta Support for HIPAA Compliance

Okta Inc.
301 Brannan Street
San Francisco, CA 94107

Okta Cell Architecture

Okta created identity as a service (IDaaS) and from the start has firmly believed in building a best-in-class enterprise-grade service. Infrastructure investments have been a priority at Okta from the beginning.

Today, Okta continues to invest in one of the most resilient, secure and "Always On" cloud architectures in the world. Overall, the Okta architecture uses a concept we call a "cell" as the largest unit of scale in the service. Each Okta "cell" encapsulates a full multi-tenant cloud service with extremely high availability. For more details on the architecture overall, see these papers:

Not all Cloud Services are Built Alike
Scaling Okta to 10 Billion Users
Okta Security: Technical Whitepaper

HIPAA Scoping

The most difficult component of operating in a regulated environment is the definition of the scope boundaries. Organizations want to ensure that only required systems are included in any regulatory audit, as the expansion of scope incurs additional setup, maintenance, and cost. Whereas with other industry regulations such as PCI, the Identity layer can be kept mostly out of scope, Okta believes that the current wording of HIPAA places Identity within scope. This drives the selection of an Identity vendor that can operate as a Business Associate.

HIPAA scoping also includes determining if the data being protected by your Information System is classified as Protected Health Information (PHI). PHI can be defined as information that "relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual, …and directly identifies the individual or there is a reasonable basis to believe …can be used to identify the individual."[1] At Okta, we take a very broad view of PHI. Not only do we include any Healthcare data that may be loaded into the system, but also the combination of Personally Identifiable Information (PII) and any application assignment. Because a user may be assigned to an application that infers a physical or mental health condition (consider an app that assists users with tracking frequency of migranes), this brings Okta usage and log data into HIPAA scope.

Cell for HIPAA

To support the ability to sign a BAA for customers, and enable them to use Okta while continuing to be HIPAA compliant, Okta has developed a solution designed to meet these unique compliance requirements. The cell for HIPAA customers went live on Feb. 15th 2016 and is currently available to customers. There are two main aspects where the HIPAA solution differs from a standard Okta implementation.

[1] Paraphrased from HIPAA section 1171

Reporting requirements

HIPAA contains specific regulations regarding communication of data breaches, access to Protected Health Information, and financial reporting to the US Department of Health and Human Services. These regulations require Okta, upon request by any user, to provide a report of any time that user's PHI was viewed by an Okta employee. Due to Okta's broad definition of PHI, this may include any customer support assistance tickets, technical operations troubleshooting tickets, or other activities required for the maintenance of the Okta service. These reports must be maintained for 6 years, placing a significant burden on Okta on behalf of our customers.

Trickle-down requirements

As a Cloud Service Provider, Okta relies on external vendors to provide critical support for the Okta IDaaS product. This includes Amazon Web Services for Infrastructure, Splunk for log data management, and third-party Customer Support providers. In order for Okta to handle PHI, we must also have agreements with our vendors who may be exposed to PHI as a result. These agreements typically come with additional costs or implementation requirements.

At an infrastructure level, within each cell Okta uses strict internal traffic segmentation via Amazon Security Groups to ensure that data in between production services cannot be viewed by unauthorized parties. This provides a high level of protection while maintaining fast network performance. Amazon's interpretation of the HIPAA regulations requires us to add IPSEC encryption in between services as well. Okta has deployed this technology in the HIPAA cell, and is in process to roll it out to all customers. Amazon also requires the use of dedicated server instances for any system that is handling PHI. Dedicated server instances force Okta to be the only AWS customer with a workload on a physical machine in the AWS datacenter. This would protect against an attack at the virtualization level. Okta uses multiple levels of encryption within our product to provide equal protection, however this trickle-down requirement adds additional cost and complexity.

Benefits of the Okta Cell for HIPAA Compliance

Okta has made significant special investments to provide a HIPAA compliant environment for its customers who need to comply with HIPAA. The Okta service on the HIPAA cell meets the obligations required by HIPAA, HITECH, and the final HIPAA Omnibus ruling.

Okta offers to sign a BAA with its customers who purchase the Okta HIPAA cell prior to allowing the customer to store any Protected Health Information (PHI) within Okta.

Okta has reviewed the HIPAA regulations and updated its product, policies and procedures to support customers around their need to be HIPAA compliant. Okta has also been evaluated by an independent, third party auditor who has issued an evaluation report (HIPAA AUP) that details the controls Okta has in place to meet HIPAA requirements in regards to data privacy and security.

In addition to being able to sign HIPAA BAA, Okta offers the following features in its product and organizational policies to every customer regardless of cell location:

- Data encryption in transit and at rest
- Restricted physical access to production servers
- Strict logical system access controls
- Configurable administrative controls available to the customer to:

- Monitor access
- Reporting and audit trail of account activities on users and content
- Formally defined and tested breach notification policy
- Training of employees on security policies and controls
- Employee access to customer data files are highly restricted
- Mirrored, active-active data center facilities to mitigate disaster situations
- 99.9% uptime SLA
- Annual SOC2 Type II Reports and 3rd party penetration testing
- ISO 27001:2013 and 27018:2014 certification

The main benefit to a customer of using Okta's HIPAA compliant infrastructure is that it enables a customer to take advantage of IDaaS while maintaining compliance with the law. This is a unique capability that Okta offers to customers.