

HIPAA and HITECH ACT Compliance Statement

Overview

Akamai enables covered entities to utilize the Akamai services in a manner that allows them to meet their obligations under the U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH). While there currently is no official certification for HIPAA or HITECH compliance, Akamai undergoes annual audits conducted by accredited independent auditors to ensure ongoing HIPAA and HITECH compliance for those services identified as appropriate (“Covered Services”) for use with protected health information (“PHI”).

Akamai operates largely as a conduit for personal data, which may include PHI, about visitors to web properties included within the content that is cached or stored on Akamai’s servers for purposes of optimization and transport, is provided by a customer for storage on Akamai servers for delivery to its end users, or that otherwise transits the Akamai servers as part of an end user’s session with the customer’s web property (“End User Personal Data”). To the extent that any End User Personal Data includes PHI, Akamai’s customer determines what PHI is collected or otherwise used by its web property. Akamai does not store or otherwise process End User Personal Data other than as required to provide the services purchased by the customer, and in those cases, any access to PHI by Akamai is largely, with the exception of the Akamai Identity Cloud service (discussed below), automated and random or infrequent in nature.

Business Associate Agreements (BAA)

While Akamai arguably operates as a conduit for the Covered Services, to the extent that it creates, receives, maintains or transmits PHI while providing services to its covered entity customers such that it is functioning as a “business associate”, Akamai will enter into the required BAA. A copy of Akamai’s standard BAA is available upon request.

Covered Services

Akamai provides its customers with tools and services designed to ensure secure distribution of its content to its end users. Only certain of its services are deemed appropriate for the transmission of PHI. Therefore, any BAA entered into between Akamai and a customer shall apply only to these Covered Services. The Covered Services Offered by Akamai at this time are:

- the Akamai Secure CDN with Enhanced TLS;
- Web performance services running on the Secure CDN with Enhanced TLS;
- the Akamai Kona Security Services, when running on the Secure CDN with Enhanced TLS;
- Enterprise Application Access;
- the Akamai Control Center (formerly Luna); and
- Akamai Identity Cloud

Akamai Identity Cloud

The Akamai Identity Cloud (AIC) is a suite of Customer Identity and Access Management (CIAM) solutions designed to provide enterprise clients with deep customer access and insights while maintaining the security and privacy of those customers. Unlike the other Akamai services, the AIC provides customers with the ability to define a data registration, storage and access schema that is hosted by Akamai. Such data could include PHI and Akamai, therefore, operates in the traditional BA role for these services. Any BA entered into between covered entity customers and Akamai applies to all products and services, development, operations, and professional services of the AIC solution. The AIC undergoes a full annual HIPAA/HITECH audit, the results of which are available to customers upon request.

Hosting for the AIC is currently designed to use only AWS HIPAA-eligible services for storing PHI. AWS follows a standards-based risk management program to ensure that the HIPAA-eligible services specifically support the security, control, and administrative processes required under HIPAA. Using these services to store and process PHI allows Akamai to address the HIPAA requirements applicable to AWS's utility-based operating model.