workday®

Supporting Customer Compliance with the Health Insurance Portability and Accountability Act (HIPAA)

Supporting Customer Compliance with the Health Insurance Portability and Accountability Act (HIPAA)

Introduction

Customers who are regulated as Covered Entities under the Health Insurance Portability and Accountability Act ("HIPAA") may face specific requirements and obligations in using Workday Enterprise Cloud Applications to capture, process, or store information regulated by HIPAA. As a Cloud Service Provider ("CSP"), Workday may serve as a Business Associate to our Covered Entity Customers. In this Business Associate role, Workday is committed to maintaining security and privacy controls that support our processing of Protected Health Information in line with HIPAA requirements for Business Associates. Customers can use this paper to understand how Workday meets our obligations as a Business Associate and to get more information on some of the features the Service offers Customers to evaluate and enable alignment with their internal HIPAA policies and procedures.

HIPAA Overview

HIPAA, first enacted in 1996, imposes requirements related to the use and disclosure of Protected Health Information ("PHI"). Specifically, it defines appropriate safeguards to protect PHI, outlines individuals' rights regarding their PHI, and describes the administrative responsibilities for both Covered Entities and Business Associates. Covered Entities may include healthcare providers, health plans, and healthcare clearinghouses, among other businesses. Business Associates are the entities who perform services for Covered Entities that involve capturing, maintaining, transmitting, or storing PHI. Business Associates share many of the same obligations under HIPAA as Covered Entities. For more information on HIPAA, visit hhs.gov/ocr/privacy.

The Workday HIPAA Compliance Program

Workday has policies, procedures, and technological safeguards designed to comply with the HIPAA requirements applicable to us as a Business Associate processing the PHI our Customers have entered into the Workday Enterprise Cloud Applications, as detailed below. We've summarized these safeguards below, categorized in alignment with the structure of the HIPAA Security Rule.

Administrative Safeguards

- Regularly assessing, evaluating, and mitigating as appropriate internal and external risks that could impact the ability for Workday to maintain the confidentiality, integrity, and/or availability of Customer Data, including PHI
- Maintaining and continually enhancing a culture of security and privacy awareness among Workday personnel, especially in regards to policies, procedures, and best practices
- Adequately vetting Workday personnel prior to providing access to Customer Data, including PHI, or the infrastructure that is used to process, store, or transmit Customer Data, including PHI
- Adhering to the "Minimum Necessary" principle of access to Customer Data, including PHI through controlled access requests and approvals, as well as periodic access reviews
- Promptly terminating Workday personnel access to Customer Data, including PHI, when no longer necessary or appropriate
- Identifying, monitoring, and responding when appropriate to known or suspected security incidents

- Maintaining procedures to enable continuation of business processes as well as the confidentiality, integrity, and availability of Customer Data, including PHI, in the event of a disaster
- Obtaining satisfactory assurance from any third parties of their ability to uphold Workday security and privacy commitments prior to granting access to Customer Data, including PHI, and continuing to monitor third-party compliance once access is granted
- Educating Workday personnel on sanctions for violating security and privacy policies, and issuing appropriate sanctions if violations occur
- Formally identifying the individual(s) who is/are responsible for developing and implementing Workday privacy and security policies

Physical Safeguards

- Restricting corporate facility access through badging systems and other physical security processes
- Securing Workday servers in a private, caged area within data centers
- Restricting data center access only to authorized personnel and requiring two-factor biometric authentication
- Enforcing 24/7 monitoring of data center access through on-site security personnel and video monitoring equipment
- Implementing a baseline of workstation security for all Workday personnel, and additional workstation security measures for individuals with access to Customer Data, including PHI
- Controlling the acquisition, allocation, reallocation, and final destruction of hardware used to capture, transmit, or store Customer Data, including PHI

Technical Safeguards

- Provisioning unique user credentials to all Workday personnel
- Requiring two-factor authentication for access to any environment that may contain Customer Data, including PHI
- Enforcing user IDs and passwords that meet minimum length and complexity requirements
- Logging all user interaction with Customer Data, including PHI, within environments that may contain Customer Data
- Enforcing security measures to guard against unauthorized access to Customer Data, including PHI, during transmission
- Encrypting Customer Data, including PHI, at rest
- Configuring data validation on certain fields to validate data input into the Workday Enterprise Cloud Applications based on attribute type
- Reviewing network configurations to prevent and detect potential vulnerabilities
- Monitoring network activity to detect and respond to performance issues

Workday annually engages a third-party independent audit firm to evaluate the effectiveness of the Workday HIPAA Compliance Program in conformity to the applicable requirements of the HIPAA Security, Breach Notification, and Privacy Rules. In accordance with established standards from the American Institute of Certified Public Accountants (AICPA), the auditor gathers evidence from its examination procedures to evaluate Workday's assertion regarding conformity to the applicable requirements of the HIPAA Security, Breach Notification, and Privacy Rules. The auditor's evaluation results in the issuance of an opinion regarding Workday's conformity, which is made available to all Workday Customers for review.

In addition to the safeguards listed above, Workday also offers a standard Business Associate Addendum ("BAA") for Covered Entity Customers who wish to process, transmit, or store PHI using certain Workday Enterprise Cloud Applications. As outlined within the BAA, Workday maintains formally documented breach response procedures to guide organizational response to a known or suspected breach of PHI in accordance with HIPAA requirements.

Customer-Enabled Safeguards

In addition to the safeguards Workday maintains in support of its HIPAA obligations as a Business Associate, Workday also offers Customers many product features in Workday Enterprise Cloud Applications to enable them to achieve their own HIPAA objectives. Some of these key product features and functionalities, which are accessible and/or managed directly by the customer in their Workday tenant, are described below.

- Configurable Security: The Workday Enterprise Cloud Applications allow customers to define access rules based on security groups by individual. Customers can restrict users' access to sensitive data or business processes, and modify user privileges upon role change or termination. Additionally, Customers can configure passwords to accommodate multifactor authentication, enhanced password complexity requirements, and adjusted frequency of session time-out rules.
- Integration Security: By default, integrations from other services into Workday must be configured using standard encryption technologies unless explicitly allowed by the Customer's Security Administrator.
- Audit Logging: Workday Enterprise Cloud Applications track all changes to business data at an application level, including data creation, modification, and deletion. Workday Customers can leverage on-demand reports to satisfy ad hoc or recurring end-user activity review, as well as activity log retention requirements.
- View User Activity: Through enabling User Activity Logging, Customers can download and analyze users' activity in Workday, including access to tasks and instances where users viewed but did not modify data.
- Data Purge: A purge functionality allows Customers to purge certain personally identifiable information for terminated workers, active workers, candidates, and prospects from their Workday tenant.
- Workday Learning: Customers can enhance existing HIPAA training and awareness programs by leveraging the capabilities of Workday Learning to make HIPAA awareness materials broadly available to employees.

Additional information on topics listed above, as well as other key product features, can be found on Workday Community or in the product documentation.

Frequently Asked Questions

Listed below are answers to a few FAQs to provide additional insight into Workday Enterprise Cloud Applications.

Will Workday sign a Business Associate Agreement ("BAA") with Customers?

Yes, Workday has a standard BAA that we make available to Customers who plan to leverage Workday to capture, transmit, or store PHI.

I have a signed BAA with Workday. That means I can put any PHI that my company has into any Workday product or offering, right?

No. Before entering any PHI into a Workday product, it is critical that you, our Customer, ensure that you are permitted to use PHI for the desired purpose, are authorized to disclose PHI to a third party (Workday), and are entering PHI into a Workday product or offering that supports your HIPAA policies and procedures. Customers should always review their product Documentation and Order Form to determine if a particular product meets the needs of their HIPAA requirements, and/or has an explicit limitation on the processing of PHI.

Where should I go to better understand HIPAA, my obligations as a Covered Entity or Business Associate, and my subcontractor's obligations?

We believe in getting information directly from the source. While there are many resources available based on individual interpretations of HIPAA, we always recommend referring to hhs.gov/ocr/privacy or consulting with your privacy or legal team for guidance.

I found a company that will provide a HIPAA certification if you pass their assessment. Does Workday have a HIPAA certification? Is Workday HIPAA compliant?

The Department of Health and Human Services ("HHS")—the government body that enforces HIPAA—has not acknowledged a standard audit, evaluation protocol, or seal to signify "HIPAA Compliance." We have designed our HIPAA Compliance Program to meet the requirements of the HIPAA Security and Privacy Rules that are applicable to our processing of Customer PHI in our role as a Business Associate, and our HIPAA Compliance Program is audited against applicable HIPAA requirements by an independent third-party auditor. However, we have no plans to pursue privatized certifications unless such a process or program is recommended by HHS.

I have a specific question about HIPAA or the PHI that I am storing in Workday. Who can I contact to get my question answered?

We encourage you to communicate via your Named Support Contact and submit your question through the standard Workday Support Case process. Just keep in mind—we cannot advise you in matters related to your obligations under HIPAA. For questions specific to your internal practices, we encourage you to reach out to your privacy or compliance team, or seek external counsel