Hubstaff Compliance & Data Governance

January 2026

Hubstaff

Organizations operating in regulated environments often need more than time tracking. They need to protect sensitive data with verifiable, secure, and compliant systems.

This resource will cover Hubstaff's compliance framework, data governance practices, and the configuration options available to help your team stay audit-ready and meet regulatory requirements across various sectors like health care, research, finance, legal, nonprofit, and other high-risk industries.

Table of Contents

Hubstaff

Compliance certifications & regulatory alignment

SOC 2 Type II

Every year, Hubstaff undergoes a **SOC 2 Type II compliance** audit to ensure its customer data management practices and internal controls meet the **American Institute of Certified Public Accountants'** (AICPA) Trust Services Criteria. This independent, third-party assessment validates that Hubstaff consistently maintains high standards for:

- Security
- Availability
- Processing Integrity
- Confidentiality
- Privacy

These principles are upheld over an extended period, not just at a single point in time. Hubstaff's annual SOC 2 Type II audits are an ongoing commitment to safeguarding sensitive data and maintaining reliable, resilient systems.

These controls may include the following in order to ensure customer data remains protected at all times:

- Documented incident response procedures
- Continuous system monitoring
- Strict access controls
- Data encryption

Additionally, Hubstaff operates a **bug bounty** program that rewards qualifying reports of security vulnerabilities that meet the program's criteria.

HIPAA readiness and Business Associate Agreement (BAA)

Hubstaff also maintains **HIPAA-aligned compliance** security and privacy controls. Under the **Health Insurance Portability and Accountability Act** (HIPAA), we:

Provide HIPAA-aligned security controls. Hubstaff undergoes annual third-party HIPAA assessments to validate that its security practices align with HIPAA requirements. These assessments support our customers' compliance efforts but do not replace their own internal risk assessments or compliance programs.

Support PHI compliance readiness. Hubstaff helps organizations handling **Protected Health Information** (PHI) to ensure accuracy and compliance.

Offer a business Associate Agreement (BAA). A BAA is available upon request and serves as an addendum to Hubstaff's **Terms of Service**, superseding any previously applicable BAA between the customer and Hubstaff.

A signed BAA is a key requirement for HIPAA compliance and helps ensure PHI is handled in accordance with regulatory standards. To support customer compliance readiness, Hubstaff provides:

- HIPAA-aligned safeguards, including encryption, role-based access controls, audit logs, secure data handling, and incident response procedures
- Annual third-party HIPAA assessments
- Business Associate Agreement (BAA) upon request

Customer responsibility: Hubstaff is not intended to store medical records or function as a system of record for PHI. Customers are responsible for configuring their use of Hubstaff to limit the exposure of PHI and ensure compliance with their internal HIPAA policies and obligations.

GDPR compliance

At Hubstaff, we recognize the importance of privacy for your business and its clients. We adhere to a rigorous **data privacy framework** that prioritizes compliance with the EU's **General Data Protection Regulation (GDPR)**.

Hubstaff maintains an internal **GDPR compliance** program designed to protect the rights of data subjects and support our customers' regulatory obligations. Here's how it works:

For customers.
Under GDPR, customers act as the Data Controller, determining the purpose and lawful basis for processing personal data.

For Hubstaff.
At the same time, Hubstaff operates as a Data Processor, processing personal data only on documented customer instructions and in accordance with GDPR requirements.

To support lawful data processing and international data transfers, Hubstaff offers a **Data Processing Agreement (DPA)** that includes Standard Contractual Clauses (SCCs), available upon request.

These agreements help ensure that personal data originating from the EU is transferred and processed in a compliant manner. Where applicable, EU customer data is transferred to and processed in AWS US East (N. Virginia) using GDPR-compliant transfer mechanisms and contractual safeguards.

Hubstaff implements appropriate technical and organizational measures to protect personal data, including:

- Encryption
- Role-based access controls
- Audit logging

Defined data retention logic to limit data exposure and support data minimization principles. This shared-responsibility approach enables customers to meet their GDPR obligations while leveraging Hubstaff as a compliant and secure data processor.

Data center and infrastructure security

Hubstaff's infrastructure is hosted in **Amazon Web Services (AWS) US East (N. Virginia)**, one of AWS's most mature and highly available regions.

AWS data centers are designed to meet globally recognized security standards and maintain compliance with **AWS Program certifications**, including:

ISO 27001	SOC 1	SOC 2	SOC 3	PCI	DSS

At the infrastructure level, data is protected through encryption in transit and at rest, network segmentation, Zero Trust security principles, and continuous monitoring, which significantly reduces the risk of data breaches or unauthorized access.

Together, these measures ensure Hubstaff customer data remains secure, available, and protected against evolving cyber threats.

This approach allows Hubstaff to deliver **enterprise-grade security** while maintaining performance, scalability, and reliability for customers worldwide.

Data collection controls & monitoring configuration

Hubstaff provides a centralized system that allows organizations to configure data collection during time tracking. Furthermore, Hubstaff's **Data Processing Agreement (DPA)** helps meet GDPR and other privacy-related legal compliance requirements.

Additionally, all monitoring features are **configurable by the organization**, and data is collected only when a user actively starts tracking time using the Hubstaff app.

Organizations are responsible for selecting which features to enable and for clearly communicating these expectations to their teams. Hubstaff does not collect data outside of active time tracking sessions.

Below, we explain how **Hubstaff's time tracking features work** and outline their capabilities and limitations.

What Hubstaff does and does not collect

Hubstaff does not:

Log keystrokes	Capture or store typed content
Analyze or interpret the contents of screenshots	Record audio from microphones
Record video from webcams	Collect biometric data

Hubstaff's tracking is activity and context-based, not content-based. For more details, check out our full guide covering **how tracking works**.

Screenshot controls

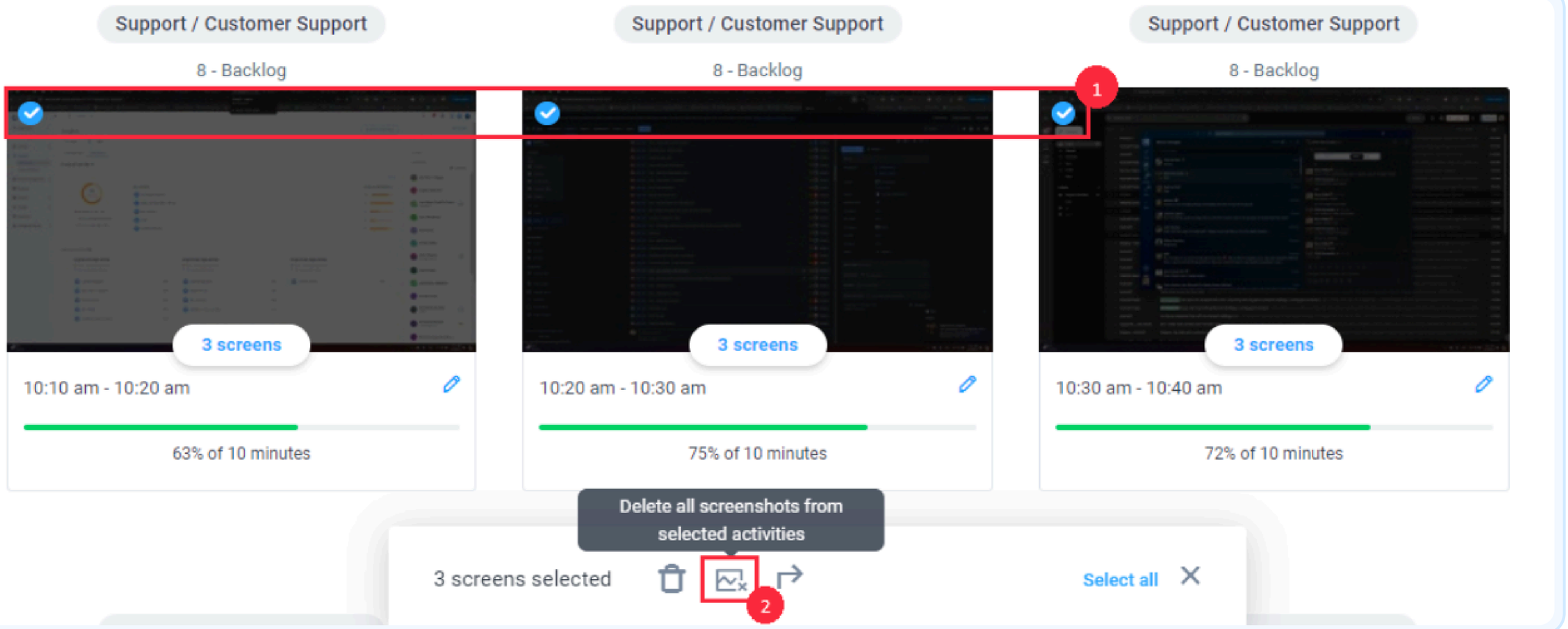
Screenshot tracking is optional and fully controlled at the organization level.

Organizations can:

- Turn screenshots on or off entirely
- Set the number of screenshots taken per 10-minute interval (e.g., 1–3 per 10 minutes)

Apply screenshot blurring globally

Configure screenshot settings per user or per project (depending on plan)



Additional notes:

Screenshots are taken only while time is actively tracked

Screenshots are captured at random intervals within the configured time block

Screenshot retention is governed by the organization's account and data retention policy

Hubstaff does not provide real-time "deny-list" or conditional blocking of screenshots based on on-screen content

App & URL tracking controls

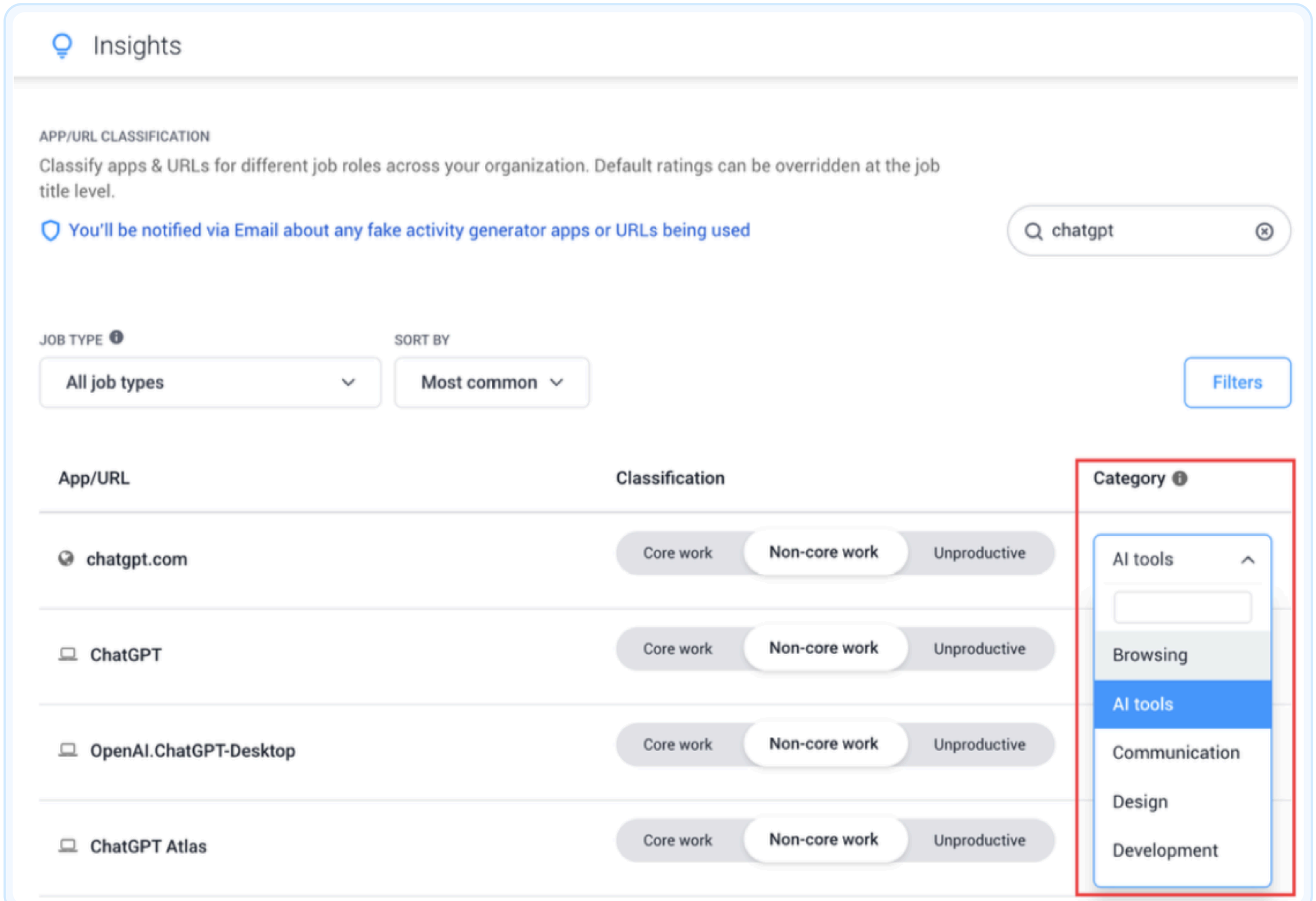
Application and URL tracking is also optional and configurable.

Organizations can:

Turn apps and URLs used on or off entirely

Disable tracking for specific users

Apply blurring to only view categories instead of raw application titles or URLs



Important considerations:

Application titles and URLs may sometimes contain sensitive information (PII or PHI), depending on how third-party tools label windows or pages

Hubstaff records application names and URLs only, not the data entered into those applications or websites

Best practice recommendations:

Disable app/URL tracking for roles that routinely handle sensitive data

Use category-based visibility instead of raw titles when privacy risk is higher

Clearly document internal policies for capturing app and URL data

Activity measurement

Hubstaff **measures activity** using a mouse and keyboard activity percentage.

Key clarifications:

Activity levels indicate whether input occurred, not what was entered	Hubstaff does not record keystrokes or mouse clicks
No text, commands, or content are captured or stored	Activity data is used to show general engagement trends, not detailed behavior

Activity levels should be interpreted as a contextual signal, not a direct measure of productivity or work quality.

Privacy, PHI protection & "No-PHI" configurations

Hubstaff is designed to support privacy-conscious deployments through transparent data practices, configurable monitoring controls, and role-based access. However, Hubstaff **does not automatically detect or classify PHI**.

Instead, it provides configuration options that allow organizations (particularly those in health care and regulated industries) to minimize or prevent PHI exposure during time tracking.

Data is collected only while users actively track time, and all monitoring features are optional and controlled by the organization. Customers are responsible for configuring Hubstaff in a way that aligns with their internal compliance obligations, including HIPAA, where applicable.

Configuring a PHI-Safe deployment

Organizations can reduce or prevent PHI exposure by configuring Hubstaff as follows:

- Disable screenshots entirely
- Enable **screenshot blurring** (partial or complete, depending on account settings)
- Hide raw application names and URLs (show categories only)
- Disable app and URL tracking
- Apply role or user-specific tracking configurations
- Enforce internal device, application, and workflow policies to limit exposure at the operating-system or application level

These controls allow Hubstaff to be used for time tracking and productivity context without collecting visual or contextual data that may contain PHI.

PHI considerations

Important limitations and responsibilities to understand:

Hubstaff does not automatically detect or redact PHI

PHI exposure risk depends on:

- The applications used by the customer
- How those applications display data (e.g., window titles, URLs)
- Internal workflows and device usage policies

Recommendations for PHI-sensitive environments:

Avoid tools or systems that display patient names or identifiers in application titles

Avoid URLs that contain patient identifiers or record numbers

Apply stricter monitoring controls (or turn off monitoring entirely) for:

- Clinical staff
- Billing and finance teams
- Legal or compliance roles

Hubstaff provides the controls, while businesses determine how and where they are applied.

Role-based access, permissions, and governance

Hubstaff uses **role-based access control and configurable permissions** to give organizations control over:

Who can access tracked data	What they can see	How data is governed across teams

Beyond basic permissions, Hubstaff's **guiding principles** are rooted in transparency, autonomy, and trust. These controls are designed to support operational oversight while limiting unnecessary exposure of employee data.

The organization defines access rules and visibility settings, which can be adjusted as roles, teams, or compliance needs change. Employees have access to their own time tracking data, which helps with getting **team buy-in for Hubstaff**.

Permissions model

Hubstaff's permissions system is based on granular, role-based authorization.

Organizations can:

- Assign predefined roles (such as owner, manager, or member) with different access levels
- Maintain auditability through account activity logs and permission histories
- Apply a least-privilege approach, ensuring users only see data required for their role
- Control visibility of:
  - Activity levels
  - Screenshots
  - Application and URL data
  - Time entries and reports

This model helps reduce unnecessary access to sensitive data while still enabling operational oversight.

Transparency & TAC principles

Hubstaff adheres to the **Transparency, Access, and Control (TAC) principles**, which emphasize the responsible use of monitoring technology.

Under these principles:

- Users can see when time tracking is active
- Tracked data (such as screenshots or activity levels) is visible to authorized roles
- Organizations decide what data is collected, retained, and reviewed

Teams are encouraged to:

- Clearly inform employees about which tracking features are enabled
- Document internal monitoring policies
- Align Hubstaff configurations with local laws, contracts, and employee agreements

Hubstaff provides the tooling to support transparency and control; policy definition and enforcement remain the customer's responsibility.

Department or role-specific policies

Hubstaff allows tracking and visibility rules to be applied per user or per role, enabling differentiated policies across departments.

Examples:

- Applying stricter controls or reduced visibility for teams handling sensitive data
- Disabling screenshots or app/URL tracking for specific roles
- Limiting which managers can view screenshots or detailed activity data

For company-owned environments, Hubstaff also supports preconfigured or "silent" tracker deployments on corporate devices, allowing organizations to standardize tracking settings while maintaining centralized governance.

Data retention, deletion, and export

Hubstaff offers a **data retention policy** that allows for the configuration of deletion and export options, supporting operational, legal, and compliance requirements. Customers act as the data controller for employee data collected through the platform.

Retention policies

Hubstaff applies default retention periods to tracked data, such as screenshots and activity information. You can use the **Hubstaff data retention add-on** to extend the lifecycle of specific data.

Key points:

- Retention periods are defined by Hubstaff's product and plan configuration
- Data is automatically deleted once it exceeds the applicable retention window
- Retention periods are not configurable below the system-defined minimums
- Different data types may have different retention behaviors (e.g., time entries vs. screenshots)

General notes:

- Time entries and reports are retained longer for payroll, invoicing, and audit purposes
- Screenshots and activity context data follow shorter retention windows

Member	Role	Teams	Projects	Payment	Limits	Time tracking status	
Anne Beasley	Organization manager	E	10	Pay rate: $55.00 Bill rate: No bill rate Hourly / Monthly / Timesheet approvals	No weekly limit No daily limit	Enabled	Actions
Ben Scott	User	T	5	Pay rate: $50.00 Bill rate: No bill rate Hourly / Monthly	No weekly limit No daily limit	Enabled	Actions
Chris Malone	Project viewer	None	2	Pay rate: No pay rate Bill rate: No bill rate	No weekly limit No daily limit	Disabled	Actions
Danny Tester	User	T	4	Pay rate: $40.00 Bill rate: No bill rate Hourly / Weekly / Timesheet approvals	No weekly limit No daily limit	Enabled	Actions
Michael Manager	Organization owner	E	5	Pay rate: No pay rate Bill rate: No bill rate	No weekly limit No daily limit	Enabled	Actions

Customer-Driven deletion

Customers remain the data controller and can manually delete certain data types from within the Hubstaff interface, subject to permissions.

Organizations can delete:	Time entries	Screenshots	Application and URL tracking logs

For non-standard or bulk deletion requests that are not available through self-service tools, customers can work with Hubstaff Support. Where applicable, Engineering, to process deletion requests in accordance with policy and technical constraints.

Export options

Available options include:

Self-service exports via the Hubstaff UI (reports, time tracking data, activity data)	API access for programmatic data extraction and integrations	Custom export support for specific use cases, subject to feasibility and plan limitations

These options allow organizations to maintain independent records and integrate Hubstaff data into downstream systems.

(**Note:** Third-party vendors may access data as necessary to provide, operate, and improve the services offered to customers.)

Security: Encryption, storage & transfer

Security and reliability are maintained through encryption of time tracking data (including screenshots) during transmission and while stored.

Encryption standards

Encryption in transit:
Data is transmitted over secure connections using TLS 1.2+.

Encryption at rest:
Screenshots captured by Hubstaff timer apps are encrypted at rest using AES-256.

SOC 2 Type II:
Hubstaff maintains SOC 2 Type II compliance, a third-party attestation that demonstrates its operational controls are sufficiently designed and consistently operated over time.

Operational security practices:
Hubstaff implements additional security measures, including access controls, audit/system logs, and backups, as part of its security and reliability practices.

(**Note:** Hubstaff has zero tolerance for spam. Users may refrain from sending bulk or unsolicited messages using Hubstaff tools. We monitor all activity very closely for violations and will remove any accounts if breaches are detected.)

Data transfer mechanisms

EU cross-border transfer basis:
Hubstaff utilizes the EU Standard Contractual Clauses (SCCs) as an alternative transfer basis in certain instances, and its Data Processing Addendum (DPA) incorporates these SCCs.

Storage environment for screenshots:
Hubstaff states screenshots are stored on Amazon S3 (AWS). Hubstaff Support

Firewall/allowlisting context:
Hubstaff guides customers requiring AWS region/IP information (relevant for networks that require allowlisting).

Integrations, API & low-bandwidth operation

Hubstaff's powerful integration capabilities utilize pre-built connectors and a robust API to sync data with other tools. The low-bandwidth feature, on the other hand, is a core feature of the Hubstaff desktop application that allows time and activity to be tracked offline.

General integration governance: Hubstaff documents the general "authenticate integration / connect projects / connect users" flow across integrations.

Offline time tracking (desktop app)

Hubstaff's Help Center notes that the desktop timer app is designed to track time and capture activity while offline, and then upload/sync that locally stored data once a stable connection is available.

Key factual points from the troubleshooting doc:

- The app can display "Offline" / "Last Update Failed" when it is unable to sync.
- VPN/proxy environments may require domain allowlisting for reliable connectivity.
- Time/activity may appear missing during connectivity issues, and then appear after the connection is restored and the app reconnects.

Recommended configurations for regulated industries

These are configuration patterns that align with what Hubstaff documents as available controls, including (screenshots optional, screenshot blurring, app/URL controls, permissions, and silent app on managed devices). The exact choices are customer policy decisions.

Health care & clinical research

Common "no-PHI" oriented configuration patterns include:

Disable screenshots entirely or enable screenshot blurring.	Apply role-based restrictions on who can view sensitive tracking artifacts (screenshots/activity).
Reduce exposure from app/URL data by limiting what's captured or who can view it (privacy-forward configuration approach is discussed in Hubstaff's privacy mission content).	For company-owned clinical devices, consider the Hubstaff Silent app (background operation on managed devices; available on Enterprise and some Team plans with the add-on).

Legal

Disable screenshots for sensitive teams where on-screen privileged or confidential material is a standard practice. (Screenshots are optional and can be configured by the org.)	Limit who can access detailed activity artifacts using role-based access controls and audit/log practices described in Hubstaff's security materials.

Finance & donor-funded organizations

Utilize time tracking and reporting while limiting content exposure by turning off screenshots for finance roles.	Export time data for audit/recordkeeping (CSV/PDF exports; screenshot export available if needed before retention expires).

Hubstaff's desktop time tracker supports offline time tracking, allowing for synchronization later when the device is online — a feature convenient for remote or field work environments.

NGOs & multinational teams

Document cross-border transfer posture using Hubstaff's DPA/SCC and data transfer compliance pages.	Plan for low-bandwidth/offline use cases using the desktop app's offline tracking and later sync behavior.

Compliance FAQ

1. Does Hubstaff automatically block screenshots of sensitive apps?

No. Hubstaff does not automatically detect or block screenshots based on the application or content shown. Organizations can turn off screenshots or enable blurring, but content-based blocking is not available.

2. Does Hubstaff perform keystroke logging?

No. Hubstaff does not log keystrokes, record typed content, or capture text input.

3. Can monitoring and tracking policies vary by role or user?

Yes. Tracking and visibility settings can be configured per user or role, allowing different policies to be applied across teams or departments.

4. Can monitoring be disabled for specific teams or users?

Yes. Features such as screenshots and app/URL tracking are optional and can be disabled entirely or limited to specific users, depending on organizational settings and plan.

5. Can access to activity data be restricted?

Yes. Hubstaff utilizes role-based access controls to restrict access to activity levels, screenshots, app/URL data, and reports. Organizations can apply least-privilege access models.

6. Can Hubstaff automatically detect PHI or sensitive data?

No. Hubstaff does not analyze screen contents, application data, or text to identify PHI or other sensitive information. Preventing PHI exposure depends on customer configuration and internal policies.

7. Can data retention periods be customized?

No. Hubstaff applies system-defined retention periods for specific data types (such as screenshots). Retention windows cannot be shortened below platform-defined limits, though customers can manually delete data where supported.

8. Is Hubstaff HIPAA compliant?

Yes, with customer configuration and a Business Associate Agreement (BAA). Hubstaff can be used in HIPAA-regulated environments when configured appropriately and when a BAA is in place.

Hubstaff does not automatically enforce HIPAA compliance; customers are responsible for configuring "no-PHI" setups and operational safeguards in line with HIPAA requirements.

To learn more, visit https://hubstaff.com/terms