STAFFINGLY, INC.

HIPAA Security & Compliance Overview

How we protect Protected Health Information across our people, systems, and vendors

Version: 2026.5 | **Prepared for:** HIPAA-covered entities and their Business Associates | **Prepared by:** Staffingly IT & Compliance

1. Purpose

This document describes the security controls, vendor relationships, workforce safeguards, and insurance coverage Staffingly, Inc. maintains to protect Protected Health Information (PHI) under the HIPAA Privacy, Security, and Breach Notification Rules (45 CFR Parts 160 and 164).

It is intended for client security reviews, procurement teams, and counsel. It summarizes current controls at a technology-stack level. Policy documents, certification letters, insurance certificates, and BAA executables are available on request.

2. About Staffingly

Staffingly, Inc. is a healthcare outsourcing company supporting U.S. providers with prior authorization, insurance eligibility verification, revenue cycle support, virtual medical assistance, and related back-office services. Our U.S. corporate office is located at 15 Corporate Pl S, Suite 145, Piscataway, NJ 08854.

State licensure

NJ Division of Consumer Affairs - Consulting Firm & Temporary Help Service License CT006693, ACTIVE through June 30, 2027 (verifiable on the NJ DCA public registry). Piscataway premises inspected by the Division during licensure.

Clinical workforce

CLINICAL WORKFORCE HIGHLIGHT

Over 95% of our workforce holds overseas medical graduate qualifications. Our team includes Overseas MDs, Registered Nurses (RNs), Doctors of Pharmacy (PharmDs), and licensed Pharmacists.

In addition, Staffingly maintains **one (1) actively U.S.-licensed Registered Nurse (Illinois) and one (1) actively U.S.-licensed Pharmacist (Florida)**, both serving from our India delivery center. This gives our engagements both scale and direct clinical oversight.

3. Certifications and attestations

Staffingly maintains an integrated compliance program aligned to the frameworks below. Certificate PDFs are available for verification on request.

Framework	Scope	Issuing body	Certificate / reference
SOC 2 Type II	Security and Confidentiality trust services criteria	Jay Maru CPA LLC (Prudence Advisors)	Clean opinion, zero exceptions
HIPAA	Covered Entity / Business Associate program	United International Certifications Ltd. (UICL)	Cert No. 909473/2024/U
HITRUST CSF	Information security management	United International Certifications Ltd. (UICL)	Cert No. 714992/2025/U
ISO/IEC 27001:2022	Information Security Management System	Magnitude Management Services	Cert No. 24MEQTJ05
GDPR	Personal data protection program	United International Certifications Ltd. (UICL)	Cert No. 415009/2025/U

All certificates are maintained in an active status. Surveillance and renewal activities are scheduled in accordance with each framework's requirements.

4. Workforce safeguards

Every Staffingly team member who may access client systems or PHI is onboarded through a documented compliance program before being assigned to any client work.

HIPAA training and annual refresher

- Every employee completes HIPAA Privacy, Security, and Breach Notification training before being granted access to any client system or PHI.
- Each employee completes an annual HIPAA certification refresher. Training records and dated certificates are retained and are available on request.
- Training covers minimum-necessary access, breach identification and reporting, safe PHI handling in remote work, credential hygiene, and prohibited activities (screenshots, downloads, personal storage).

Confidentiality and non-disclosure agreements

- Every employee signs a Non-Disclosure Agreement and a Confidentiality and PHI Handling Agreement as a condition of employment.
- Where a client requires a client-specific NDA, attestation, or user compliance questionnaire, the assigned employees sign that instrument before access is provisioned.
- NDAs survive termination and are backed by employment contract provisions.

Background screening and access discipline

- Background verification is completed for all employees prior to assignment.
- Each employee has a unique login. Credential sharing is strictly prohibited and is grounds for termination.
- Access is provisioned on a minimum-necessary, role-based basis and is revoked immediately on termination or role change.
- User activity on Staffingly-managed systems is logged and auditable.

5. Endpoint and device safeguards

All workstations used to access client systems or PHI are Staffingly-managed and enrolled in Microsoft Intune for continuous policy enforcement. Work activity is additionally isolated inside the Venn Blue Border™ secure enclave (Section 7). The following controls are enforced centrally and verified through compliance monitoring.

Two-factor authentication (2FA)

- 2FA is enforced at sign-in to every Staffingly-managed workstation through Microsoft Entra ID / Windows Hello and conditional access.
- 2FA is additionally enforced for Microsoft 365, the Venn secure workspace, and any client remote-access channel that supports it.
- Credential-only (password-only) access is blocked by conditional access policy.

Removable media and data-egress controls

- USB mass storage is blocked at the endpoint level through Intune and Microsoft Defender device control. External drives, SD cards, and MTP devices cannot be mounted or written to.
- Copy / paste and screen capture from client systems are restricted by policy. Inside the Venn Blue Border enclave, copy / paste, screen capture, downloads, and peripheral redirection are governed by DLP policy.
- Personal cloud storage (personal OneDrive, Google Drive, Dropbox, iCloud) is blocked by Microsoft Purview DLP and web filtering.
- Local printing of PHI is disabled. Print-to-PDF of PHI is not permitted.

Web filtering and app control

- Outbound web traffic is filtered through Microsoft Defender for Endpoint network protection and SmartScreen, with policies that block personal webmail, file-sharing sites, social media, streaming, and categories unrelated to work duties.
- Application install rights are restricted. Only IT-approved software may run on Staffingly-managed endpoints.
- Malicious and newly registered domains are blocked automatically by Microsoft Defender threat intelligence feeds.

Baseline endpoint hardening

- Full-disk encryption (BitLocker on Windows) is enforced on every workstation.
- Automatic patching for OS and applications is enforced through Intune.
- Auto-lock activates at or before five minutes of inactivity.
- Microsoft Defender for Endpoint (EDR) runs on every workstation with tamper protection enabled.

6. Access model for client systems

Every Staffingly-managed endpoint runs the Venn Blue Border™ secure enclave (see Section 7). Two access patterns are supported, depending on whether the client provides their own remote environment.

Pattern A — Venn Blue Border™ secure workspace (Staffingly default)

Every Staffingly user works from a Staffingly-issued, Intune-managed workstation running Venn Blue Border™. Work applications, browser sessions, EHR / PM logins, payer portals, client VPN clients, and any temporary PHI are isolated inside a company-controlled, encrypted enclave on the device. Work apps run locally at native performance — no VDI, no streamed desktop, no virtualization layer in the user path. Every byte is governed by the enclave.

- AES-256 encryption of work data at rest inside the Venn Disk on the endpoint.
- TLS-tunneled egress through a static, company-dedicated IP for every byte that leaves the enclave.
- DLP on copy / paste, screen capture, downloads, uploads, peripherals, printing, and browser upload destinations — enforced inside the enclave.
- Single sign-on through Microsoft Entra ID with conditional access and MFA enforced before the enclave will open.
- Full audit log of work activity inside the enclave. Controls auditable for HIPAA, SOC 2, PCI-DSS, FINRA, and CMMC.

Pattern B — Direct access to a client-managed environment

Where a client maintains its own VDI / EHR / practice management environment, Staffingly users connect into that environment through the client's approved remote-access channel (client VPN, VDI, Citrix, AVD, RDS, RDP gateway, or portal), launched from inside the Venn Blue Border™ enclave on the Staffingly endpoint. PHI remains inside the client's environment — it is not copied to, downloaded onto, or stored on Staffingly devices. Access is governed by the client's identity provider and MFA policy.

7. Venn Blue Border™ secure workspace

Venn is a U.S.-based secure-workspace provider. Venn Blue Border™ is a patented, software-defined secure enclave that installs on every Staffingly-managed Windows endpoint and isolates work applications, work data, and work network traffic inside a company-controlled, encrypted perimeter. There is no VDI, no streamed desktop, and no virtualization layer in the user path — work apps run locally at native performance, and every byte is governed by the enclave.

BLUE BORDER™ — HOW IT IS SECURED

Inside the Blue Border (company-controlled secure enclave):
Browser sessions, EHR / PM logins, payer portals, client VPN clients, and any temporary work files live inside an encrypted virtual disk on the endpoint. The enclave is visually marked by a blue line around each work window so users and auditors can see, in real time, which apps are governed.

Controls enforced at the Blue Border perimeter:
- AES-256 encryption of work data at rest on the device
- TLS-tunneled egress through a static, company-dedicated IP
- DLP on copy / paste, screen capture, downloads, peripherals, printing
- Identity, MFA, conditional access enforced through Microsoft Entra ID
- Full audit log of work activity inside the enclave

Venn controls map to HIPAA Security Rule safeguards

Control	Implementation under Venn Blue Border™
Workspace model	Company-controlled secure enclave on every Staffingly-managed endpoint.
Encryption at rest	AES-256 encryption of work files, browser sessions, and application profiles inside the Venn Disk on the endpoint.
Encryption in transit	TLS-tunneled egress from the enclave through a static, company-dedicated IP. HTTPS / TLS for all web and SaaS access.
Identity and MFA	Single sign-on through Microsoft Entra ID with conditional access and MFA enforced before the enclave will open.
Data Loss Prevention	DLP on copy / paste, screen capture, downloads, uploads, peripherals, printing, and browser upload destinations — enforced inside the enclave.
Audit and logging	Work activity inside the enclave is logged centrally for security monitoring and audit support.
Compliance fit	Controls auditable for HIPAA, SOC 2, PCI-DSS, FINRA, and CMMC, per Venn product documentation.
Business Associate Agreement	BAA with Venn covering Staffingly's use of the platform for PHI handling.

8. Microsoft 365 E5 layer

Staffingly operates on Microsoft 365 E5 under an active HIPAA Business Associate Agreement with Microsoft. The E5 security suite provides our identity, endpoint, email, collaboration, and data-protection stack, and integrates with the Venn Blue Border™ enclave at the identity layer.

Component	What it covers
Microsoft 365 HIPAA BAA	Active BAA with Microsoft covering Microsoft 365 / Azure services used by Staffingly
Entra ID (Azure AD)	Identity, conditional access, device compliance, MFA enforcement on 100% of users
Microsoft Defender for Endpoint	EDR/XDR on all Staffingly-managed workstations and servers
Microsoft Defender for Office 365	Advanced phishing, malware, and business email compromise protection on email and Teams
Microsoft Purview	Data Loss Prevention, sensitivity labels, audit logging, eDiscovery
Microsoft Intune	Mobile device management and compliance policies on all endpoints (encryption, auto-lock, patching, USB lockdown)
Exchange Online and OneDrive / SharePoint	Encrypted mail and storage under the Microsoft BAA; retention and legal hold configured
Teams	Encrypted collaboration; external sharing controlled by policy; meeting recordings governed

9. Physical safeguards

- Staffingly's Piscataway, NJ corporate office has been inspected by the NJ Division of Consumer Affairs as part of state licensure.
- Overseas Delivery operations run from controlled-access facilities with visitor logging, badge access and bio-metric access, and surveillance.
- Workstations are locked when unattended and auto-lock at five minutes. Screens are positioned away from public view, and PHI is only handled in private, secure workspaces.
- PHI may not be printed, photographed, screenshotted, or stored on personal devices or personal storage.

10. Incident response and breach notification

- Documented incident response plan covering detection, containment, eradication, recovery, and post-incident review.
- 24x7 alerting from Microsoft Defender and the Venn admin telemetry into the Staffingly IT and Compliance function.
- Suspected security events are investigated on a same-day basis. Confirmed incidents are classified and documented.
- Clients are notified of any confirmed or suspected breach involving their PHI within the timeframes required by HIPAA and by the Business Associate Agreement, including the updated 2026 breach-notification expectations where applicable.
- Root-cause analysis and corrective actions are shared with affected clients.

11. Insurance coverage

Staffingly maintains active commercial insurance covering the engagement risks typical to a healthcare business associate.

Coverage	Per occurrence	Aggregate
Commercial General Liability	$1,000,000	$2,000,000
Cyber Liability (included with the E&O policy)	$5,000,000	$5,000,000
Errors & Omissions (Professional Liability)	$5,000,000	$5,000,000
Crime / Employee Dishonesty	$250,000	$250,000

Policy numbers, carrier details, and a full Certificate of Insurance (COI) are available on request. We will name the client as an additional insured where the engagement contract requires it.

12. Compliance and security contact

Questions, BAA requests, security reviews, and incident notifications:

Dan Nandan, President & CEO

Staffingly, Inc.

15 Corporate Pl S, Suite 145, Piscataway, NJ 08854

Email: dan@staffingly.com

Compliance inbox: support@staffingly.com

SOC 2 Type II | HIPAA | HITRUST | ISO/IEC 27001:2022 | GDPR | MGMA Corporate Member

This document is provided for informational purposes and does not modify any executed contract or Business Associate Agreement. Controls and vendor arrangements are reviewed and updated as our program evolves.