TinyDocx CAIQ / SIG Lite Security & Privacy Questionnaire

Version: 1.0
Date: May 20, 2026
Organization: TinyDocx
Prepared by: Jennifer Feldman, CISO of Record

Overview

This document provides a lightweight combined CAIQ / SIG Lite style response package for TinyDocx customers, partners, auditors, and prospective clients.

Products in Scope

MemoryBook, Mermaid Sea, Senior Tree (pre-launch), and Hash Browns.

Security & Privacy Alignment

TinyDocx maintains a security and privacy program aligned with HIPAA, SOC 2, ISO/IEC 27001, ISO/IEC 27701, GDPR principles, and CCPA/CPRA principles.

Security Governance

TinyDocx maintains formal security leadership, annual policy reviews, workforce training requirements, documented corrective action procedures, and documented risk management processes.

Compliance & Audit

TinyDocx maintains audit logging, periodic compliance reviews, vulnerability management processes, and independent assessment planning.

Identity & Access Management

TinyDocx supports MFA, SSO, role-based access controls, least-privilege access principles, periodic access reviews, and restricted privileged accounts.

Infrastructure & Cloud Security

Primary infrastructure is hosted on AWS in us-east-1. Encryption is enforced in transit and at rest. Production systems are access controlled and monitored.

Privacy & Data Protection

TinyDocx restricts PHI access by role, segregates customer data from marketing systems, and prohibits unauthorized advertising use of customer data.

Data Subject Rights

TinyDocx supports DSAR requests including access, deletion, correction, and erasure requests through documented procedures.

Vendor & Subprocessor Management

TinyDocx performs third-party privacy assessments, requires DPAs where applicable, and provides advance notice of subprocessor changes.

Incident Response & Business Continuity

TinyDocx maintains documented incident response and corrective action procedures and monitors critical systems for availability risks.

Secure Development Practices

TinyDocx uses source control, environment separation, production change controls, and tracked configuration management practices.

AI Usage Controls

TinyDocx prohibits unauthorized PHI exposure to non-approved AI providers and does not position AI-generated output as deterministic source-of-truth decisions.

Customer Assurance Statements

TinyDocx does not sell customer data, does not use customer PHI for advertising, maintains encryption and audit logging controls, and enforces least-privilege access principles.

Contact Information

Security & Privacy Contact: security@tinydocx.com
Website: https://tinydocx.com

Current Key Subprocessors

Vendor	Function
AWS	Cloud hosting & infrastructure
Auth0	Identity provider
Vanta	Compliance monitoring
GitHub	Source code hosting
Anthropic	Internal engineering assistance (no PHI permitted)

Disclaimer

This document is provided for informational and customer due diligence purposes only. Responses reflect TinyDocx operational controls and governance practices as of the effective date listed above.