



Privacy Policy - Effective Date: 01-01-2026

Aloha Copy & Scanning ("Company," "we," "us," or "our") is committed to protecting the confidentiality, integrity, and security of documents and personal information entrusted to us through our document scanning, indexing, storage, handling, and related records management services. We maintain administrative, physical, and technical safeguards designed to protect information from unauthorized access, use, disclosure, alteration, or destruction.

Scope

This Policy applies to information collected, received, maintained, processed, scanned, stored, transmitted, or otherwise handled by the Company in connection with our services, including paper records, electronic records, and digital images created during the scanning process. It also applies to information collected through our website, client communications, service forms, and operational systems used to perform our services.

Information We Handle

In the ordinary course of business, we may receive:

- Client contact information and account details.
- Personal information contained in documents provided by clients.
- Protected Health Information ("PHI") or electronic Protected Health Information ("ePHI") when we act as a service provider to covered entities or other authorized clients under applicable HIPAA arrangements.
- Business records that include, but are not limited to: Invoices and receipts, purchase orders, contracts, signed agreements, tax records, bank statements, insurance records, HR files, legal, correspondence, bio-technology research, manufacturing records and others that are submitted to us for document scanning and archiving.

Use of Information

We use information solely for purposes of providing contracted services, including document intake, preparation, scanning, indexing, quality review, secure storage, secure transmission, retention, destruction, billing, customer support, and related operational activities. We do not use client documents or data for unrelated purposes except as permitted by contract, authorized by the client, or required by law.

Safeguards and Controls

We maintain a security program designed to protect sensitive information through appropriate administrative, physical, and technical safeguards. These safeguards may include:

- Restricted access to facilities, storage areas, scanning stations, and systems.
- Role-based access controls and unique user credentials.
- Workforce confidentiality obligations and security training.
- Logging, monitoring, and audit procedures.
- Secure handling of paper records before, during, and after scanning.
- Quality control checks to confirm image accuracy and completeness before disposition of originals.
- Encryption or other protective measures for electronic data where appropriate.
- Secure transfer methods for data in transit and secure storage protections for data at rest.

Scanning and Quality Review

We follow workflow procedures intended to ensure that scanned documents are complete, legible, properly indexed, and retrievable. Paper originals may be held in secure staging areas during scanning and quality assurance review, and may be retained until verification is complete before any approved destruction or return process is performed. Where original documents are eligible for destruction, they are destroyed using secure methods appropriate to the sensitivity of the records and applicable law or contractual requirements.



HIPAA-Related Services

Where we handle PHI or ePHI on behalf of a covered entity or other authorized client, we act only as permitted by our written agreement and applicable law. We will not use or disclose PHI except as authorized by the applicable agreement, required by law, or otherwise permitted under HIPAA. We also require appropriate safeguards and, where applicable, flow-down obligations to qualified subcontractors consistent with HIPAA requirements.

Team and Premises Security

Each team member is subject to a comprehensive background investigation, consents to random drug testing, and is required, as a condition to work at the company, to execute both a standard non-disclosure agreement and a HIPAA-compliant non-disclosure agreement.

All services are performed exclusively by Aloha Copy & Scanning personnel on an in-house basis; The company does not engage third-party vendors or independent contractors in the performance of such services. The company represents that its operations are conducted in compliance with all applicable federal regulations, including the International Traffic in Arms Regulations (ITAR). In accordance with ITAR requirements and the nature of Aloha's work involving Department of Defense and other government contracts, Aloha employs only U.S. citizens.

We maintain physical security measures designed to safeguard its facilities and information systems, including two layers of secured access doors in accordance with HIPAA standards and continuous, Access to production areas is strictly limited to authorized personnel; visitors, including personal acquaintances, are prohibited from entering these areas or accessing documents at any time. 24/7 video surveillance of both interior and exterior areas. Exterior building entrances and internal office doors remain locked during non-business hours and weekends.

In-House Information and Data

All scanned images are maintained on secure workstations with access restricted to authorized personnel during scanning, indexing, and optical character recognition (OCR) processes. To ensure endpoint monitoring and data protection, all scanning workstations and servers are fully isolated from external internet connectivity and operate elusively within a secured, internal wired Ethernet network.

As an additional safeguard, all workstations require authenticated user login credentials, utilize password-protected screen savers, and are powered down when not in active use. User credentials are updated on a regular basis and immediately revised upon any change in authorized personnel.

Data Transfer and Company Information Storage

We utilize third-party file transfer services in circumstances where a secure file-sharing portal has not been established by the client to connect directly to a designated customer server.

The third-party services currently utilized include:

- SMASH: <https://www.smash.org/privacy-policy/>
- WeTransfer: https://wetransfer.com/documents/WeTransfer_Privacy_Policy_20250715.pdf

These services are used solely for the temporary transfer of image files and related data. They are not used for ongoing or long-term image hosting. Files transmitted via these platforms are subject to automatic and permanent deletion from the provider's servers after a period of seven (7) days. Upon request, a shorter retention period may be arranged. Additionally, Aloha Copy & Scanning will delete transferred data upon the client's request once successful download has been confirmed.

When images and data are delivered via flash or USB storage devices, all such devices are new, and are reformatted, verified, and confirmed to be free of viruses or malicious software prior to the transfer of any data to the customer.

- MEGAsync: cloud storage is used exclusively by management for the limited purpose of storing customer invoicing, quotes, contact information, and related correspondence. No scanned images or client-provided materials are stored on this platform. MEGA's Privacy Policy is available at: <https://mega.io/privacy>



Incident Response

We maintain procedures for identifying, reporting, investigating, and responding to suspected security incidents, unauthorized disclosures, and other events affecting sensitive information. If we determine that a reportable security incident or breach has occurred, we will follow applicable legal, contractual, and regulatory notification obligations.

Retention and Disposal

We retain records only for as long as needed to fulfill service obligations, legal requirements, and contractual commitments. When records or media are no longer needed, we dispose of them securely in a manner designed to prevent reconstruction or unauthorized recovery. The Company implements strict controls governing the secure destruction and deletion of scanned image data residing on workstations, servers, and associated storage systems. All such data shall be retained only for the minimum period necessary to fulfill its intended business or legal purpose and shall thereafter be irreversibly deleted using industry-recognized secure deletion methods designed to prevent unauthorized access, reconstruction, or recovery. This includes, but is not limited to, the use of data wiping standards, secure overwriting protocols, and, where applicable, physical destruction of storage media. Access to deletion processes is restricted to authorized personnel, and all destruction activities are subject to audit and verification procedures to ensure compliance with applicable data protection laws, regulatory requirements, and internal information security policies. All document and physical file destruction is handled by a third party partner that is ISO compliant and has all the proper procedure in place.

Client Responsibilities

Clients are responsible for ensuring they have the legal right to provide documents to us for scanning, processing, retention, and disposal. Clients should also confirm that their instructions regarding retention, return, access, destruction, and access permissions are accurate and complete.

Banking Use of Information

We accept payments via direct customer checks or through an approved purchase order. For ongoing contractual engagements, Automated Clearing House (ACH) direct deposit payments may be established by the client's organization.

Credit card payments are accepted exclusively through PayPal's secure online payment platform. In such cases, a payment link will be provided to the client for completion of the transaction. We do not request, collect, store, or have access to any credit card information submitted through PayPal.

All credit card transactions are processed in accordance with PayPal's privacy and security policies, which are available at: <https://www.paypal.com/us/legalhub/paypal/privacy-full>

Website Use

Our website may collect limited technical and contact information such as form submissions, email addresses, and device or usage data used to operate the site, respond to inquiries, and improve services. We do not intentionally collect more information through the website than is reasonably necessary for these purposes. We use Google Analytics to understand how visitors use our website and to measure website traffic, understand page performance, identify popular content, detect navigation issues and measure campaign performance all to improve user experience to improve website performance. To know more about how Aloha Copy & Scanning uses Google Analytics, visit <https://policies.google.com/technologies/partner-sites> More about our On-line Privacy Policy can be found on our website: <https://www.alohacopy.com/LegalNotice.htm> and our website and email servers are hosted by JCI John Companies, Inc and their privacy policy is here: <https://www.jcihosting.com/privacy.html>

Changes to This Policy

We may update this Policy from time to time to reflect changes in our practices, operational requirements, or applicable law. The updated version will be posted on our website with a revised effective date.

This Policy is intended to describe our general document security and privacy practices and is not a substitute for a specific contract, business associate agreement, or legal advice. In the event of a conflict between this Policy and a signed service agreement, the signed agreement controls.