
Square 9 Highlights 5 Essential Security Practices for Safeguarding Extracted Document Data

As organizations expand their use of AI-powered document processing, Square 9 outlines key practices for protecting sensitive information throughout the automation process.

New Haven, CT, September 22, 2026 – As document data is being used to empower new automation initiatives, many organizations are turning to intelligent document processing to capture, classify, and extract this unstructured information. While intelligent document processing offers tremendous benefits, organizations must implement these systems with care.

Many documents contain sensitive information, and regulatory non-compliance can carry severe consequences, including reputational damage, legal liability, and fines from agencies like the FTC and HIPAA.

To protect sensitive information from cyber threats and unauthorized disclosure, Square 9 recommends five essential security practices:

1. **End-to-End Data Encryption:** Safeguard extracted content by encrypting data both in transit across networks and at rest within repositories. This encryption includes scanned documents traveling to capture servers, data moving between integrated systems, and information stored in cloud-based repositories.
2. **Granular Access Controls:** Apply role-based access control (RBAC) and multi-factor authentication (MFA) to all accounts. This means restricting access to sensitive documents to only the staff handling this information and strengthening login security to prevent unauthorized access.
3. **Comprehensive Audit Trails:** Maintain access logs and continuous system monitoring to quickly spot suspicious activity and trace document histories. A comprehensive log of all document changes, views, and access revisions ensures accountability and a swift response in the event of a breach.

PR Contact:

Sam Young, Marketing Communications Specialist
203-789-0889, option 1 | samyoung@square-9.com

4. **Automated Data Redaction and Masking:** Obfuscate sensitive fields, such as Social Security numbers or financial details, before sharing files across broader teams. By redacting this information, you reduce exposure risk and make tracing easier in the event of a breach.
5. **Strict Compliance Frameworks:** Align document processes with industry standards such as SOC 2 and HIPAA to ensure informed, transparent data handling. SOC 2 and HIPAA compliance requires strict processes and policies for handling information. Ensuring both system providers and internal teams are audited and certified keeps information handled according to best practices

Square 9 Softworks remains dedicated to delivering regimented, compliant, and best-practice-informed data security across its entire AI-powered document processing platform. Find out more about how Square 9 is helping businesses securely manage information at: www.square-9.com/compliance-document-management-software/

About Square 9 Softworks®

[Square 9](#) Softworks is a generative AI-powered platform that removes the frustration of extracting data from documents, forms, and all external sources, so you can harness the full power of your information. Release your team from repetitive tasks while your work flows freely in areas like accounts payable, order processing, onboarding, contract management, and more. The Square 9 platform captures your unstructured content, transforms it into clean, searchable data, and securely shares it across your organization to accelerate your decisions and actions.

PR Contact:

Sam Young, Marketing Communications Specialist
203-789-0889, option 1 | samyoung@square-9.com