Policy
Sensitive Information

Janco Associates, Inc.

2025

Table of Contents

Sensitive Information Policy - Credit Card, Social Security, Employee, and Customer Data

Overview

Sensitive information is defined as information that is protected against unwarranted disclosure. Access to sensitive information is to be safeguarded. Protection of sensitive information may be required for legal or ethical reasons, for issues on personal privacy, or proprietary considerations.

Information sensitivity is the control of access to information or knowledge that might result in the loss of an advantage or level of security if disclosed to others.

Loss, misuse, modification, or unauthorized access to sensitive information can adversely affect the privacy or welfare of an individual, trade secrets of a business, or even the security, internal and foreign affairs of a nation depending on the level of sensitivity and nature of the information. If an individual or an organization violates this policy, its standards, or procedures, they are subject to immediate termination or contract revocation without recourse.

Policy

The Chief Security Officer or delegate must approve all processing activities at ENTERPRISE associated with sensitive information. This information includes but is not limited to social security numbers, credit card numbers, credit card expiration dates, security codes, passwords, customer names, customer numbers, ENTERPRISE proprietary data, and any other data (i.e. California Personal ID number) that is deemed to be confidential by ENTERPRISE, its external auditors, any governmental agency, or other body that has jurisdiction over ENTERPRISE or its industry.

This policy applies to the entire enterprise, its vendors, its suppliers (including outsourcers), and co-location providers and facilities regardless of the methods used to store and retrieve sensitive information (e.g. online processing, outsourced to a third party, Internet, Intranet, or swipe terminals).

All processing, storage, and retrieval activities for sensitive information must maintain strict access control standards and the Chief Security Officer mandates these specific policies be followed.

PCI

The sensitive information policy of ENTERPRISE applies to all system components, which are defined as any network component, server, or application that is included in or connected to the cardholder data environment. The sensitive information PCI DSS policy is that all cardholder data is protected, and cardholder data that is not allowed (see PCI DSS requirements) to be stored is removed from the system once the card has been authorized.

The primary account number, cardholder name, service code, and expiration date can be stored if that data is sufficiently protected as specified in the PCI DSS standard.

	Data Element	*Storage Permitted*	*Protection Required*	*PCI DSS Requirement 3.4*
Cardholder Data	Primary Account Number (PAN)	Yes	Yes	Yes
	Cardholder Name*	Yes	Yes*	No
	Service Code*	Yes	Yes*	No
	Expiration Date	Yes	Yes*	No
Sensitive Authentication Data**	Full Magnetic Stripe	No	N/A	N/A
	CVC2/CVV2/CID	No	N/A	N/A
	Pin / Pin Block	No	N/A	N/A

* These data elements must be protected if stored in conjunction with the PAN (Primary Account Number). This protection must be consistent with PCI DSS requirements for the general protection of the cardholder environment. Additionally, other legislation (for example, related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data or proper disclosure of a company's practices if consumer-related personal data is being collected during the business. PCI DSS, however, does not apply if PANs are not stored, processed, or transmitted.

** Sensitive authentication data must not be stored after authorization (even if encrypted).

Regulations and Industry Impact

Regulation	Industry Impacted	Retention Implications	Penalties
Sarbanes-Oxley	All publically-traded companies	Audit records must be maintained for 7 years AFTER the audit	Fines up to $5,000,000 & imprisonment up to 20 years
Section 17a-4	Financial Services	Email records must be kept for 3 years, trading records through the end of the account plus 6 years	Case by case
HIPAA	Healthcare	Hospital records must be kept for 5 years, medical records for the life of the patient plus 2 years	Fines up to $250,000 & imprisonment up to 10 years

Regulations and Industry Impact Table

Keys to Email Archiving Compliance

Four objectives must be met. They are:

- **Discovery** - Information must be easy to access and consistently available to meet legal discovery challenges from regulatory committees.
- **Legibility** - Information must have the ability to be read today and in the future, regardless of technology. When selecting archiving technology, companies should look for solutions that are based on open systems, if their Email application should change. For example, if a company migrates from Microsoft Exchange to Lotus Notes, it must still be able to quickly access and read archived Emails.
- **Auditability** - An Email archiving solution must have the ability to allow third parties to review the information and validate that it is authentic.
- **Authenticity** - Information must meet all security requirements, account for alteration, and provide an audit trail from origin to disposition. An audit trail can track any changes made to an Email.

Job Descriptions

The job descriptions listed below come as separate files in their directory

- Chief Compliance Officer (CCO)
- Chief Security Officer (CSO)
- Manager Data Security
- Security Architect

Forms

The forms listed below come as separate files in their directory

- Sensitive Information Policy Compliance Agreement
- Work From Home IT Checklist

HIPAA Audit Program Guide

Background

All providers of medical services were required to comply with the Health Information Portability and Accountability Act (HIPAA). HIPAA was created to improve the efficiency and effectiveness of the healthcare system through the development of national standards for electronic healthcare transactions.

HIPAA mandates that the organizations:

- Provide information to patients about their privacy rights and how their information can be used.
- Train employees so that they understand the privacy procedures.
- Designate an individual to be responsible for seeing that the privacy procedures are adopted and followed.
- Perform a privacy risk assessment.
- Adopt clear privacy procedures for practice, hospital, or plan.
- Secure patient records containing individually identifiable health information, so that they are not readily available to those who do not need them.

The focus of the HIPAA audit is:

- Review of written policies and practices on security
- Review of written policies and practices on privacy
- Review of processes in practice vs. privacy policies and procedures
- Review of processes in practice vs. security policies and procedures
- Review of business associates to ensure that each has a valid contract or agreement, especially new associates or partners

Ensuring HIPAA Compliance

With the passing of the Health Insurance Portability and Accountability Act, maintaining standards in administrative and communication of healthcare-related information has become mandatory.

HIPAA Requires

- Electronic healthcare transactions and code sets
- Health information privacy
- Unique identifier for employers
- Security requirements
- Unique identifier for providers
- Unique identifier for health plans and
- Enforcement procedures

What's New

2025

- Updated all included forms
- Updated all included job descriptions

2024

- Added 1 job description
  - Chief Compliance Officer
- Updated to meet ISO Supply Chain compliance requirements
- Updated all included forms
- Updated all included job descriptions

2023

- Added 3 job descriptions
  - Chief Security Officer (CSO)
  - Manager Data Security
  - Security Architect
- Updated to meet ISO compliance requirements
- Updated all included forms

2022

- Major re-edit of the entire policy
- Updated to meet ISO compliance requirements
- Updated all included forms

2021

- Updated all included forms
- Updated to reflect WFH impact
- Add Work From Home IT Checklist