Privacy & Security Compliance Standard Operating Procedure (SOP)

Version: 1.0

Created on: June 23, 2025

Privacy Contact:

Simon Salas/CEO

simon.salas@goodsamtx.org

www.goodsamtx.org

Table of Contents

1. Introduction

This policy establishes Good Samaritan Community Services' formal privacy and security measures to protect client and organizational information. These policies apply a trauma-informed lens and comply with applicable federal and state requirements, including:

- HIPAA (Health Insurance Portability and Accountability Act)
- Texas Health and Human Services (HHS) Data Use Agreements (DUAs)
- Texas PII and SPI laws
- Texas Government Code and CJIS (Criminal Justice Information Services) requirements
- City of San Antonio administrative privacy guidelines

This SOP supports secure and ethical handling of sensitive information across all programs provided by Good Samaritan Community Services.

---

2. Scope

These policies apply to all staff, interns, contractors, volunteers, and subcontractors who create, access, transmit, store, or manage:

- Physical or electronic client files
- Personally Identifiable Information (PII)
- Protected Health Information (PHI)
- Texas HHS Confidential Information
- Any other sensitive organizational records

They apply to data handled through:

- Hard copy storage
- Computers, phones, and portable media
- Cloud-based and third-party systems
- Internal databases and secure portals

---

3. Definitions

Texas HHS Confidential Information
Data covered under DUAs with the Texas Health and Human Services system, including PHI, SPI, case information, or program data.

HIPAA
Federal law governing the privacy and security of health data, including rules for storage, access, and disclosure.

CJIS
Criminal Justice Information Services security standards issued by the FBI and Texas DPS, applicable to background checks and justice-involved client records.

PII (Personally Identifiable Information)
Information such as name, DOB, SSN, driver's license, or other identifiers protected under Texas law.

PHI (Protected Health Information)
Any health information that can identify an individual and is protected under HIPAA.

Authorized User
A Employee or subcontractor approved to access Texas HHS Confidential Information for an authorized purpose under a DUA.

Authorized Purpose
Use, disclosure, access, or processing of confidential information as permitted under the Texas HHS DUA.

---

4. Privacy and Security Policies

Good Samaritan Community Services implements administrative, technical, and physical safeguards to protect all information including Texas HHS Confidential Information, HIPPA, CJIS, PII and PHI. These policies are reviewed regularly and enforced through training, monitoring, and accountability procedures.

4.1 Privacy Safeguards

"Privacy Safeguards" include protections required by HIPAA (45 CFR 164.530), the DUA, Medicaid, and applicable law:

- **Administrative Safeguards:** Policies for training, access controls, termination, incident response, and disaster recovery.
- **Technical Safeguards:** Passwords, encryption, secure emailing/faxing, logging, and emergency access protocols.
- **Physical Safeguards:** Locked file cabinets, restricted access, secured devices, and procedures for shredding or disposal.

4.2 Authorized Users and Authorized Purposes

Only designated Authorized Users may access Texas HHS Confidential Information for Authorized Purposes defined in the DUA. Only designated Authorized Users may access HIPPA, CJIS, PII and PHI. All access must be job-related and documented.

4.3 Workforce Compliance with HIPAA and Applicable Laws

All staff must comply with HIPAA, the DUA, and applicable Texas laws. Training is required prior to access and repeated annually. Confidentiality agreements are signed and kept on file.

4.4 Minimum Necessary Use and Disclosure

Use or disclosure of Texas HHS Confidential Information, HIPPA, CJIS, PII and PHI is limited to the minimum necessary to fulfill the Authorized Purpose.

4.5 Breach Response Policies and Procedures

The organization maintains a documented breach response plan that includes:

- Immediate notification to immediate supervisor and CEO
- Immediate notification to Texas HHS and regulators as required under Article 4 of the DUA
- Investigations and corrective action
- Notification of affected individuals as directed by Texas HHS

4.6 Annual Workforce Training and Monitoring

Privacy and security training is mandatory annually. Completion is tracked and enforced. Delinquent training results in restricted access until completed.

4.7 Individual Rights: Access, Amendment, and Correction

Clients may request access to or correction of their Texas HHS Confidential Information to Goos Samaritan's Privacy Officer. Written requests are processed per applicable law and documented.

4.8 Authorization for Access

Only Authorized Users with current training and a demonstrated job-related need may access confidential information. Exceptions require written approval from Good Samaritan Community Services CEO.

4.9 Sanctions for Non-Compliance

Violations of policy, including unauthorized access or disclosure, are subject to sanctions including retraining, suspension of access, termination, or legal action. All sanctions are documented.

4.10 Policy Updates

Privacy and security policies are updated within 60 days of identifying the need due to operational, legal, or technical changes impacting data use.

4.11 Cooperation with Regulatory Authorities

Good Samaritan Community Services cooperates fully with Texas HHS, OCR, or other authorized inspections, audits, or investigations related to data handling under the DUA or applicable laws.

4.12 Secure Disposal

All physical and electronic Texas HHS Confidential Information must be destroyed so it is unreadable or undecipherable, regardless of retention schedules. This includes shredding paper and securely wiping electronic media.

4.13 Prohibition on Unauthorized Disclosure of Work Product

Work products or deliverables developed under the DUA may not be disclosed or published without prior written approval from Texas HHS.

4.14 Subcontractor Access Restrictions

Subcontractors (e.g., cloud vendors) may not access or process Texas HHS Confidential Information unless their agreement has been reviewed and approved by Texas HHS, with all compliance and liability clauses in place.

4.15 System Security Log Review

Systems accessing or storing Texas HHS Confidential Information must have logs reviewed regularly to detect unauthorized activity or breaches. Logs are retained and reviewed by the designated Privacy Officer.

4.16 Online and Mobile App Security

Public-facing websites and mobile apps handling Texas HHS Confidential Information must comply with TGC §2054.516, including vulnerability and penetration testing. All identified risks must be remediated promptly.

---

5. Privacy Notice Posting

To meet HIPAA and Texas HHS transparency requirements, Good Samaritan Community Services maintains a publicly accessible Privacy Notice:

- **Online:** Posted prominently at www.goodsamtx.org/privacy
- **In Person:** Hard copies available at public-facing service areas (e.g., front desk, intake)

The Privacy Notice informs individuals about their rights, the organization's use of data, and available safeguards.

---

6. Data Processing and Offboarding Compliance

When any Employee, intern, or contractor separates from the organization:

- All Texas HHS Confidential Information access is **terminated immediately**.
- Organizational devices must be **returned and wiped** using tools that comply with **NIST 800-88 Rev. 1** sanitization standards.
- Final checklists include recovery of keys, ID badges, and digital credentials.
- The departing individual must sign a **Confidentiality & Non-Retention Form** affirming no data has been kept or shared.

Documentation of offboarding and device sanitization is retained by the Privacy Officer.

---

7. Encryption Requirements

All Texas HHS Confidential Information must be encrypted as required by HIPAA, Texas law, and DUA provisions.

At Rest:

- Files stored on servers, devices, or portable drives must use **AES-256** or equivalent encryption.
- Personal or unapproved devices may not store confidential data.

In Transit:

- Email or file transmission must use **TLS 1.2+** or encrypted file portals.
- No sensitive data may be sent via unencrypted email or SMS.

This applies to desktops, laptops, phones, backup systems, and cloud platforms.

---

8. Training Documentation and Compliance Logs

To ensure accountability and audit-readiness, Good Samaritan Community Services maintains the following documentation:

- **DUA Training Log:** Tracks completion of all required privacy, HIPAA, and DUA-specific trainings.
- **Signed Acknowledgement Forms:** Confirm each Employee has reviewed and agreed to all relevant policies.
- **Annual Refresher Tracking:** Training logs are updated annually and reviewed quarterly by the Privacy Officer.
- **Training Delinquency Correction:** Individuals with expired or incomplete training will have access revoked until requirements are met.

Training records are retained for a minimum of **six (6) years** and made available upon request to Texas HHS or federal regulatory bodies.

---

9. Attachments and Appendices

The following forms, templates, and checklists are included at the end of this policy and used for documentation and operational compliance:

A. Acknowledgement Form Template

Signed by Employees confirming receipt and understanding of privacy/security policies.

B. Data Use Agreement (DUA) Training Log

Tracks names, dates, and completion of required training.

C. Data Security Plan Template (Web & Mobile Applications)

Outlines risk management for public-facing systems per Texas Gov't Code §2054.516.

D. Vulnerability and Penetration Testing Procedure

Explains how security testing is conducted and documented.

E. Breach Response Plan

Step-by-step response for suspected or actual data breaches.

F. Authorized User Access Request / Termination Form

Used to request, approve, and revoke access to Texas HHS Confidential Information.

G. Device Disposal/Wiping Checklist

Documents the secure wipe or destruction of devices upon separation or device retirement.

H. Privacy Notice Template

A customizable public-facing notice that meets HIPAA/Texas HHS transparency requirements.

I. Incident Report Form

Used internally to report suspected security incidents or data misuse.

Appendix A:

Acknowledgement of Privacy and Security Policies

Good Samaritan Community Services
Acknowledgement Form – Privacy & Security Policies and Procedures

❑ **Employee Name:** _____

❑ **Position/Department:** _____

❑ **Date:** _____

I acknowledge that:

1. I have received, read, and understand the **Privacy and Security Standard Operating Procedures (SOP)** provided by Good Samaritan Community Services.
2. I understand that the SOP contains policies and procedures required to comply with HIPAA, the Texas Health and Human Services Data Use Agreement (DUA), CJIS standards, and all applicable privacy/security laws.
3. I agree to comply with these procedures at all times, including safeguarding confidential information and reporting any suspected breaches immediately.
4. I understand that failure to follow these policies may result in disciplinary action, including termination or legal consequences.
5. I will complete all required annual privacy and security training as assigned by the Privacy Officer.

Signature: _____

Date: _____

Supervisor Signature: _____

Date: _____

Compliance Use Only:

☐ Logged in training record

☐ Copy provided to Employee

☐ Original retained in personnel/training file

Appendix B:

Data Use Agreement (DUA) Training Log Template

Good Samaritan Community Services

Data Use Agreement (DUA) Training Log

This log documents workforce training on HIPAA, Texas HHS Confidential Information, and applicable privacy/security procedures under the DUA.

Name	Position	Training Date	Trainer/Facilitator	Training Type (Initial/Annual)	Completion Verified (Y/N)	Notes

Instructions:

- Maintain one centralized log per calendar year or grant cycle.
- Use this log during audits, monitoring visits, or internal reviews.
- Verify training completion with a signed Acknowledgement Form or LMS record.

Appendix C

Data Security Plan Template (Web & Mobile Applications)

(In accordance with Texas Government Code §2054.516)

Good Samaritan Community Services

Data Security Plan for Public-Facing Websites and Mobile Applications

This plan outlines the security measures implemented for all applications that access, process, or transmit Texas HHS Confidential Information via online platforms.

---

1. System/Application Name:

---

2. Description & Purpose:

Briefly describe the app or site and how it interacts with confidential information.

---

3. Data Classification:

☐ Public
☐ Internal Use
☐ **Confidential (Texas HHS Confidential Information)**
☐ PHI/PII

---

4. Responsible Parties:

- **Data Custodian:** _____
- **IT Security Contact:** _____

---

5. Vulnerability Testing Schedule:

Testing must occur:
☐ Quarterly
☐ Semi-Annually
☐ Annually
☐ After major code/deployment changes

Date of Last Test: _____
Testing Vendor/Tool: _____

---

6. Identified Vulnerabilities & Resolutions:

Date Identified	Description	Risk Level	Resolution Date	Resolution Method

---

7. Data Encryption Controls:

- At Rest: _____
- In Transit: _____

---

8. User Access Controls:

- Authentication Method:
  ☐ Username/Password
  ☐ MFA
  ☐ Other: _____
- Role-Based Access Implemented: ☐ Yes ☐ No

---

9. Backup & Recovery Protocols:

Location of Backups: _____
Frequency: ☐ Daily ☐ Weekly ☐ Monthly

Disaster Recovery Tested: ☐ Yes ☐ No
Last Test Date: _____

---

10. Approval & Review

Prepared By: _____ Date: _____

Reviewed By: _____ Date: _____

Approved By: _____ Date: _____

Appendix D

Vulnerability and Penetration Testing Procedure

Good Samaritan Community Services
Security Testing Procedure for Public-Facing Websites and Mobile Applications
(In compliance with Texas Government Code §2054.516)

---

1. Purpose

To identify and remediate security vulnerabilities in public-facing web and mobile applications that store, process, or transmit Texas HHS Confidential Information.

---

2. Scope

Applies to all systems that:

- Are accessible via the internet
- Store or interact with PHI, PII, or other Texas HHS Confidential Information
- Are owned, hosted, or contracted by Good Samaritan Community Services

---

3. Testing Frequency

Vulnerability and penetration testing will be conducted:

- Prior to launching any new application
- After major updates or configuration changes
- On a recurring basis: ☐ Quarterly ☐ Semi-Annually ☐ Annually

---

4. Testing Process

Step	Activity
1.	Identify assets and applications in scope for testing
2.	Use approved tools or vendors to conduct tests (e.g., Nessus, OpenVAS, third-party)
3.	Simulate attacks to uncover exploitable weaknesses (e.g., SQL injection, XSS, brute-force)

Step Activity

4. Document all vulnerabilities with risk levels (Low/Medium/High/Critical)
5. Provide testing report to IT/Compliance/Management
6. Track and document resolution of each finding
7. Retest after mitigation efforts to verify closure

---

5. Roles and Responsibilities

- **IT/Security Lead:** Coordinates and performs tests
- **System Owners:** Review results and oversee remediation
- **Privacy Officer:** Ensures documentation meets regulatory expectations

---

6. Documentation and Recordkeeping

All tests, findings, remediation actions, and approvals must be:

- Logged and retained for **6 years**
- Available upon request to Texas HHS or auditors

---

7. Approval

Prepared By: _____ Date: _____

Reviewed By: _____ Date: _____

Approved By: _____ Date: _____

Appendix E

Breach Response Plan

Good Samaritan Community Services
HIPAA & Texas HHS Breach Response Procedure

---

1. Purpose

To provide a clear, documented process for identifying, responding to, reporting, and mitigating actual or suspected breaches involving Texas HHS Confidential Information, HIPPA, CJIS, PII and PHI.

---

2. Definition of a Breach

A breach is any unauthorized acquisition, access, use, or disclosure of PHI, PII, or other confidential information that compromises its security or privacy, including but not limited to:

- Lost/stolen devices containing sensitive data
- Improper access by Employees
- Accidental or intentional disclosure of client information
- Malware, ransomware, or phishing attacks

---

3. Immediate Actions (Within 24 Hours)

- **Step 1:** Isolate the threat (e.g., disconnect affected systems, revoke access)
- **Step 2:** Notify the **Privacy Officer** and/or **IT Security Officer**
- **Step 3:** Begin internal investigation
- **Step 4:** Document key facts, including:
    - Date/time discovered
    - Nature of data involved
    - Number of individuals affected
    - Systems/users involved
    -

---

4. Notification Requirements

- **Notify Texas HHS** as required by Article 4 of the DUA (usually within 24 hours)
- **Notify individuals** if PHI/PII was accessed, per HIPAA Breach Notification Rule
- **Notify other regulatory agencies** as applicable (e.g., OCR, AG's Office)

---

5. Investigation & Mitigation

- Conduct root cause analysis
- Apply technical/administrative corrections (e.g., patches, retraining, policy changes)
- Track all corrective actions and responsible parties
- Retest systems to confirm resolution

---

6. Documentation

Maintain breach files including:

- Incident reports
- Notification letters
- Logs of corrective actions
- Communication with Texas HHS or regulators

Retention period: **6 years**

---

7. Approval

Prepared By: _____ Date: _____

Reviewed By: _____ Date: _____

Approved By: _____ Date: _____

APPENDIX F

Authorized User Access Request / Termination Form

Good Samaritan Community Services
Texas HHS Confidential Information Access Authorization

SECTION 1: USER INFORMATION

- **Name:** _____
- **Position/Department:** _____
- **Email:** _____
- **Phone:** _____
- **Date of Request:** _____

SECTION 2: TYPE OF ACCESS

☐ New Access Request
☐ Modification of Access
☐ Termination of Access

Effective Date: _____

Systems/Applications to Access:
☐ PIERS
☐ State/Federal Portal
☐ Secure File Transfer
☐ Encrypted Email
☐ Other: _____

☐ Other: _____

☐ Other: _____

SECTION 3: AUTHORIZED PURPOSE

Justify business need for accessing Texas HHS Confidential Information:

SECTION 4: TRAINING & AGREEMENTS (REQUIRED)

Requirement	Completed	Date	Verified By
HIPAA Training	☐ Yes ☐ No		
DUA Training	☐ Yes ☐ No		
Confidentiality Acknowledgement	☐ Yes ☐ No		

SECTION 5: APPROVALS

- **Supervisor Signature:** _____ Date: _____
- **Privacy Officer:** _____ Date: _____
- **IT/Security Officer (if applicable):** _____ Date: _____

NOTE: All access must be terminated within 24 hours of a role change or departure from the organization.

Device Disposal/Wiping Checklist

Good Samaritan Community Services
Secure Disposal & Data Wiping Verification Form

SECTION 1: DEVICE INFORMATION

- **Device Type:** ☐ Laptop ☐ Desktop ☐ Mobile ☐ External Drive ☐ Other: _____
- **Serial Number:** _____
- **Assigned User:** _____
- **Department/Program:** _____
- **Date of Decommission:** _____

SECTION 2: DATA SANITIZATION METHOD

Sanitization must follow NIST 800-88 Rev. 1 guidelines:

Sanitization Method	Performed	Tool/Process Used	Verified By
☐ Secure Erase	☐ Yes	_____	
☐ Overwrite (3-pass minimum)	☐ Yes	_____	
☐ Degaussing	☐ Yes	_____	
☐ Physical Destruction (if HDD)	☐ Yes	_____	

SECTION 3: FINAL DISPOSITION

- ☐ **Reassigned internally** (sanitized and redeployed)
- ☐ **Donated to third-party** (with confidentiality certification)
- ☐ **Recycled through certified vendor**
- ☐ **Destroyed** (receipt/log attached)

Vendor (if applicable): _____
Certificate or Receipt #: _____

SECTION 4: SIGN-OFF & COMPLIANCE REVIEW

- **Sanitization Completed By: _____**
- **Title: _____**
- **Date: _____**
- **Reviewed and Verified By (IT or Compliance): _____**
- **Title: _____**
- **Date: _____**

Supporting documentation (e.g., logs, photos, vendor receipts) must be attached and retained for 6 years.

Privacy Notice

Good Samaritan Community Services
Client Privacy Notice (HIPAA and Texas HHS Compliance)

Your Privacy Matters to Us

Good Samaritan Community Services is committed to protecting the privacy and security of your personal information. This notice explains how we collect, use, and safeguard your information in accordance with federal and state laws, including the **Health Insurance Portability and Accountability Act (HIPAA)** and our **Texas Health and Human Services (HHS) Data Use Agreement (DUA).**

Information We Collect May Include:

- Name, address, and contact details
- Date of birth, Social Security Number
- Health or behavioral health information
- Services received through our programs
- Background checks (for some programs)

How We Use and Share Your Information:

We use your information only to:

- Provide services and support to you or your family
- Report required data to funding agencies (such as Texas HHS)
- Coordinate referrals or benefits (with your consent)
- Fulfill legal and regulatory obligations

We **do not sell your information** and will not share it without your written consent unless required by law or allowed under HIPAA.

Your Rights Include:

- The right to see or request a copy of your information
- The right to ask for corrections
- The right to request limits on how your information is used or shared
- The right to file a complaint without fear of retaliation

To exercise these rights, please contact our **Privacy Officer** at simon.salas@goodsamtx.org

---

How We Protect Your Information:

- All records are stored securely in locked cabinets or encrypted systems
- Access is limited to authorized staff only
- Our staff receive annual training on HIPAA and privacy laws
- All subcontractors and partners must follow the same rules

Contact Information:

If you have questions or concerns about your privacy, please contact:
Privacy Officer: Simon Salas
Good Samaritan Community Services
simon.salas@goodsamtx.org
1600 Saltillo St. San Antonio, TX 78207
Website: www.goodsamtx.org/privacy

Incident Report Form

Good Samaritan Community Services
Privacy & Security Incident Report

SECTION 1: INCIDENT DETAILS

- **Date of Incident:** _____
- **Time of Incident:** _____
- **Date Reported:** _____
- **Location (physical or system):** _____
- **Type of Incident (check all that apply):**
  ☐ Unauthorized Access
  ☐ Lost/Stolen Device
  ☐ Improper Disclosure
  ☐ Malware or Ransomware
  ☐ Email/SMS Breach
  ☐ Physical Security Breach
  ☐ Other: _____
- **Brief Description of Incident:**

SECTION 2: INFORMATION INVOLVED (check all that apply)

☐ Name(s)
☐ Date of Birth
☐ Social Security Number
☐ Medical or Mental Health Information
☐ Service History
☐ Financial/Eligibility Data
☐ Other Confidential Information: _____

Approximate number of individuals affected: _____

SECTION 3: DISCOVERY & RESPONSE

- **How was the incident discovered?**

- **Immediate actions taken (e.g., access revoked, device isolated):**

- **Reported to Privacy Officer?** ☐ Yes ☐ No
  If Yes, Date: _____ Time: _____ By: _____

SECTION 4: INVESTIGATION & FOLLOW-UP

- **Investigation Summary:**

- **Was a breach confirmed?** ☐ Yes ☐ No ☐ Pending
- **Were notifications issued to individuals?** ☐ Yes ☐ No ☐ Not Applicable
- **Was this reported to Texas HHS or OCR?** ☐ Yes ☐ No
  Date Submitted: _____ Confirmation #: _____
- **Corrective Actions Taken:**
  ☐ Training/Re-training
  ☐ Policy/Procedure Update
  ☐ Technical Fix
  ☐ Other: _____

SECTION 5: SIGN-OFF & RETENTION

- **Completed By:** _____ Date: _____
- **Title:** _____
- **Privacy Officer Review:**
  ☐ Incident Closed ☐ Further Action Required
- **Signature:** _____ Date: _____

All reports must be retained for a minimum of 6 years.