Key Personnel

We recognize that a team of skilled and experienced personnel is essential for the successful execution of any project, and as such, we have assembled a highly capable multi-tier team of experts. Our team represents the highest level of knowledge, skills, and expertise required for the digital conversion of documents. All team members including management, team leaders and executive staff are HIPAA certified and have received Chain of Custody training and HIPAA certification.

Additionally, team members assigned to CJIS and sensitive document processing and handling are screened per CJIS requirements documented elsewhere in this proposal. Finally, all SSG team members must complete the SSG "Rules of Conduct" training session and complete a SSG Confidentiality Statement for each individual project. With the exception of Project Managers, no recording devices are allowed to be powered or in use within the facility, including but not limited to, cell phones, digital cameras, laptop computers, etc. All communication to and from team members is conducted through our Project Managers.

The following training and certifications have been obtained for all Executive and Level I & II Managers who are directly involved with all service projects:

1. HIPAA Certification
2. Federal Public Trust Clearance
3. Department of the Army Certificate of Training/Information Assurance Security Officer Certification Course (40 Hours)
4. Investigation for ARNG Supporting DoD Missions
5. Public Trust Security Clearance
6. United States Information Technology Agency (AAIT-DC)
7. CJIS Compliant

Quality Control Plan

Our reputation as a quality provider of healthcare solutions is based on us consistently exceeding our client's expectations.

We achieve this by having a **comprehensive Quality Control Plan and strict adherence to rigorous quality standards**.

Standards of process and procedure have been developed and are included in all our records and information management projects. Standardization enables high quality production of goods and services on a reliable, predictable, and sustainable basis. Standardization assures us that important elements of a process are performed consistently and in the most effective manner.
Changes are made only when data shows that a new alternative is better. Use of standard practices allows us to:

- Reduce variation among individuals or groups and make process output more predictable
- Provide "know-why" for operators and managers
- Provide a basis for training new people
- Provide a trail for tracing problems
- Provide a means to capture and retain knowledge
- Give direction in the case of unusual conditions

Our standard process incorporates a "single task" function that enables team members to conduct Quality Control (QC) of the previous task before conducting their assigned task. These controls allow for a 4-point QC system that has been developed over 20 years to address expected errors. Each error is always documented and tracked to identify the root and process changes are made accordingly. We have developed studies and compiled data that validates a file requires a 4- point check to ensure the maximum accuracy and accountability.

The utilization of technology and internal controls also allows us maximum control of the stages, tasks and final audit of every project.

Standard Operating Process

Our processes are what we refer to as "location neutral." Whether we are executing within one of our secure facilities or at our clients' location, the baseline process and methodology are the same. Our processes are built three primary criteria: security, control, and quality. Additional steps based on the specific cope of this project are outlined within the scope of work.

Stage I: Intake/ QC1

Files received shall go directly to the intake team. Files shall be counted and a "count per box" recorded for additional reconciliation. Each BOX and FILE shall be assigned a unique barcode number and entered into our document management tracking system.

Utilization of barcode technology provides a chain of custody trail and audit history as the

record moves through the various stages for reconstruction, scanning and reconstruction. Each task performed begins with the team member logging the beginning and end of the designated task using unique login credentials. This provides us with a complete audit trail for all transactions and tasks. Compiling and maintaining a chain of custody also allows us the ability to conduct daily QC performance measurement for all personnel.

A log is kept identifying any discrepancies between the client manifest and the intake verification. The POC is notified of any discrepancies each day via an issue report outlining the specific item. The POC validates back to us and the issue is noted in our tracking system. You can be assured that we expect it to be our job to keep track and reconcile all items through each process.

 Stage II: Document Prep

The document prep team is responsible for ensuring that all the documents are free from staples, paper clips, etc. They also are identifying and preparing documents that may need special settings (i.e., light documents or colored forms) as well as small notes, etc.

The prep team is also inserting barcode cover sheets at this time to identify the section and the form number and/or any index information required. Folders remain with the documents within their original box and are transferred to the scan station with the appropriate barcode cover sheets and ancillary document identification sheets. This box is the records' "forever home" until it returns to the client or is destroyed on site. It is also identified as a batch within our system and allows us to track any file and/or document back to the box to address any issues, discrepancies, etc. that may be found during any one of the QC stages.

 Stage III: Scanning

The scan operators are now ready to process the documents. The box (batch) is scanned first to identify the batch and also used as reconciliation all the way back to intake. During the scan process, operators are making adjustments as needed based on document types and formats. Our experience with these documents indicates that some require special settings and the condition of the paper can sometimes require special attention. Once a batch/box has been completed, the box is transferred to the reassembly team.

 Stage IV: Image QC4

Scanned images are saved to a QC workflow process where QC operators will begin the 100% image QC process by viewing each document scanned to ensure legibility, skewed documents, etc. After the QC operators are complete, the batch is released for final

processing to remove blank documents and barcode cover sheets.

Deficiency Controls/Exceptions

Deficiencies in the quality of service performed are monitored on a daily basis through a 4-point quality control check at each stage of the record rebuild and data entry. Identification of staff per task is tracked and audited to identify specific personnel and/or stages whereby an excessive margin of error is identified. This enables us to target the point of error, adjust the process and/or personnel and continue evaluation.

Deficiencies identified (also referred to as exceptions and/or errors) are isolated from the process and reassigned to an "exception" team. We know there will be exceptions throughout this project that will need to be addressed. Some items are addressed by communication with the POC to identify a new process that needs to be implemented. For example, we have fund that some files have forms without form numbers. Other examples include form numbers that have changed over time but are representative of the same form. These types of items are not unusual and the Project Manager will work with the POC to identify the preferred process for thesesituations.
Once a decision is made, our templates and process documents are amended and all team members are notified.

"Exception" team members' sole function is to verify the error, make corrections and readmit the record into the process. "Exception" team members also document the staff ID, error classification, date and batch.

Information collected to identify and analyze deficiencies shall be shared with the POC in a format agreeable to both parties. Typically this is documented in matrix format identifying the specific deficiency and outlining the change in process to correct the deficiency.

Secure Production Facilities

This facility was designed to ensure that our customers receive not only the latest in capture technologies but the confidence of knowing that every precaution has been taken to maintain the integrity and security of both your physical and digital information while it is in their possession. Our facilities are capable of operating under a 24 hour – 7 days per week production model when necessary. The data and documents that are housed at our location are secure in individual locked down storage pods, where individual client files are not intermingled with files from other clients. Each pod is secure in that only authorized personnel have access to it.

Southwest Solutions Group complies with the most stringent industry requirements for security and privacy of the documents and information that we process. We provide our employees with rigorous and thorough training regarding the handling and processing of confidential information. Southwest Solutions Group assesses potential risks and vulnerabilities to all data, images and documents in our possession. We have developed, implemented and continue to maintain appropriate security measures, which are incorporated throughout our process controls as listed below:

- Selection and Execution of Security Measures that Protect the Integrity, Confidentiality, and Availability of Data and Images
- Security Privacy Officer
- Security Awareness Training
- Personnel Conduct and Background Verification
- Keypad Entry
- Computer System and Network Design
- Audit Controls
- Security Authorization Control
- Data Authentication
- Event Reporting and Monitoring

All access permissions are based on "need to know, least privilege" for the facility and data. Unauthorized access to our facility is prevented through the following: closed circuit television, electronic badge systems, proximity badge readers for all doors, surveillance cameras, visitor access procedures, visitor escorting, emergency doors are alarmed, hard key locks, burglar and motion sensing alarms and monitoring services. No cell phones or cameras of any type are allowed by production staff in the operations area.

Facility Security Details

- Restricted access
- Cameras and motion detectors
- Server and telecommunications room – restricted card key access

SSG closely monitors both the inside as well as the outside of the facility. The conversion facility is outfitted with an access control system for the building. The card readers allow access only to those authorized individuals programmed into the system by the Security Supervisor. Additionally, all doors are equipped with sensors that detect and register an alarm with any unauthorized entry or exit. The system will also alarm for any door props or doors remaining open longer than the routine amount of time to allow normal entry or exit.

The monitoring company monitors alarms on a 24-hour basis. When necessary, the monitoring company will contact the Security Coordinator or one of the designated alternatives. The individual contacted will respond to the alarm. Whenever the facility is not open, the local police will be called to respond and secure the building until the Security Manager, or the designated alternative, arrives at the facility. The facility is equipped with cameras and recording equipment to cover entrances and other key locations at the site.

All personnel are issued an access control card. The access control system at the facility records date, time, cardholder, and reader location for each badge swipe. It records accesses granted and denied. Reports can be generated on site for the previous 30 days' activity.

SSG has established highly vigilant and effective security and safety awareness programs at the all of our facilities to keep employees focused on the need for sound security and safety practices. Through these programs, we disseminate new information or directives andre-enforce existing policies through bulletin boards, flyers, newsletters, and briefings.
The IT Security Manager, as well as other managers, also conduct random checks to ensure our workforce is carrying out appropriate security and safety measures to protect the integrity, confidentiality, and availability of PII/PHI information during collection, storage, transmission, and disposal.

Disaster Recovery

Disaster recovery procedures are in place. Critical support facilities are available for continuing operations in the event of an emergency. Southwest Solutions Group will mirror all processes and services at their other service centers, which will be available for continuing operations in the event of an emergency. Contingency plans are developed, implemented and maintained for responding to system emergencies. Backup of data and images is performed according to schedules established in the contingency plan, which includes:

- Data Backup
- Emergency Mode Operations
- Information Access Control
- Applications and Data Critical Analysis
- Personnel Security-Incident Procedures
- Image Back-up
- Testing and Revisions
- Media Controls

Enhanced Processing for CJIS and Highly Sensitive Materials

A national fingerprint-based criminal history record check will be performed upon assignment of personnel to a facility with access to FBI CJIS systems. Documentation of said shall be provided to client and updated as required each year.

The purpose of this security plan is to validate the requirements for the physical storage of and safeguarding of archive boxes containing CJIS information. This plan references specific relevant portions of the **Criminal Justice Information Services (CJIS) Security Policy,** Version 5.2 dated 8/9/2013 (CJISD-ITS-DOC-08140-5.2)

5.9 Policy Area 9: Physical Protection

Physical protection policy and procedures shall be documented and implemented to ensure CJI and information system hardware, software, and media are physically protected through access control measures.

Details regarding the storage of boxes are outlined in the following paragraphs. Southwest Solutions Group further submits the following safeguards at the entry and during intake:

- ***Boxes shall be delivered to dock, either loose and/or on pallets***
- ***During delivery and intake, only authorized personnel shall be present***
- ***Box barcodes shall be scanned and entered into a database.***
- ***Information captured shall not contain any PII and/or CJIS specific identifiable information.***
- ***Information captured via barcodes shall include "Record Type" (i.e. "Offense Records") and Year (i.e. 1970) only***

Incident Reporting

1. ***Boxes that arrive open or damaged shall be reported in an incident log.***
2. ***Southwest Solutions Group Security Officer and/or authorized personnel shall notify the government agency within 24 hours of reportable incidents***
3. ***Security Officer and/or authorized personnel shall document the incident to include the following information:***
    a. ***Date***
    b. ***Description of incident (i.e., damaged box, open box, loose records, etc.)***
    c. ***Date reported to government agency***
    d. ***Government agency contact name***
    e. ***Resolution***

5.9.1.1 Security Perimeter

The perimeter of physically secure location shall be prominently posted and separated from non- secure locations by physical controls. Security perimeters shall be defined, controlled and secured in a manner acceptable to the CSA or SIB.

Southwest Solutions Group has isolated an area within our facility as follows:

1. ***Boxes to be shrink-wrapped on pallets and stored in high bay shelving***
2. ***High bay shelving section shall be enclosed on all four sides***
3. ***Enclosure shall be secured with a key lock***
4. ***Enclosure shall be clearly marked on all sides as a restricted area allowing only authorized access.***
5. ***Surveillance cameras shall be utilized on a motion sensor to capture each access attempt.***

5.9.1.2 Physical Access Authorizations

The agency shall develop and keep current a list of personnel with authorized access to the physically secure location (except for those areas within the permanent facility officially designated as publicly accessible) or shall issue credentials to authorized personnel.

Southwest Solutions Group shall keep on file a copy of access verification information including:

- ***Name***
- ***Date of birth***
- ***Social security number***
- ***Date fingerprint card(s) submitted***
- ***Date security clearance issued***
- ***Date initially trained, tested, certified or recertified.***

5.9.1.6 Monitoring Physical Access

The agency shall monitor physical access to the information system to detect and respond to physical security incidents.

Motion detector surveillance cameras are in place to capture and record all access activities

5.9.1.7 Visitor Control

The agency shall control physical access by authenticating visitors before authorizing escorted

access to the physically secure location (except for those areas designated as publicly accessible). The agency shall escort visitors at all times and monitor visitor activity.

1. *Visitors and unauthorized personnel shall not have access to the secure storage area.*
2. *Access to the secure storage area requires access to fork lift equipment. All personnel with access to said equipment shall be considered authorized personnel and subject to a fingerprint background check.*
3. *Records shall be maintained for all personnel with access to required equipment shall be*

5.9.1.3 Physical Access Control

The agency shall control all physical access points (except for those areas within the facility officially designated as publicly accessible) and shall verify individual access authorizations before granting access.

1. ***A key to the secure area shall be secured by the Security officer and one back-up individual located on site.***
2. ***The security officer and back-up shall have full clearance via a fingerprint background check supplied directly to the government agency***

Personnel

Physical access to CJIS information shall be authorized after completion of the following items:

1. Fingerprint background check
2. Security Awareness training conducted by Southwest Solutions Security Officer. Security training shall include, but not be limited to the Security Awareness Training documentation provided by Alan Ferretti and the Texas Department of PublicSafety.
3. Secure Access Records shall be created and maintained separately from employee files and shall include:
    a. Name
    b. Date of birth
    c. Social security number
    d. Date fingerprint card(s) submitted
    e. Date security clearance issued
    f. Date initially trained, tested, certified or recertified (if applicable).

Access

1. Access to physical records shall be limited to authorized personnel.
2. Access shall not be deemed authorized and/or necessary unless requested by the government agency and or Southwest Solutions Security Officer.
3. Southwest Solutions Security Officer shall be present during receipt and intake of archive boxes.

4. Individuals handling archive boxes during intake and storage placement shall be authorized as having completed fingerprint background check and security awareness training.

Our Equipment

- Ability to effectively scan a wide range of paper thicknesses and sizes
- Document feed has double-feed prevention mechanism
- Vacuum transport mechanism has less physical impact on the paper
- Ultrasonic detection senses air spaces between pages for second double-feed detection
- Software correlates information from the transport sensors to ensure images are present for each page that passes across the transport
- Native document scan at 300 dpi to meet federal regulatory requirements
- Ability to scan front and back, color and black and white, in a single pass
- Superior image quality even for poor quality documents like vision and audiology baselines
- Seven (7) year maintenance cycle with parts and service availability after model end life
- Duplex camera imaging
- Mixed document scanning
- Bi-tonal, grayscale and color scanning
- Ultrasonic doubles detection
- Multi-feed detection
- Mechanical document detection and de-skew
- Single High Capacity Full Page Pocket

All of our scanners have color capability allowing us keep documents in production regardless of setting requirements. Our scanners can be manually set to color and or set to “automatically detect.” Typically, documents to be scanned in color are identified during the document prep stage. They are rotated to alert the operators.

All documents are scanned in duplex. We set our automatic blank page removal at very low thresholds to ensure a small signature or checkmark is not considered a blank page. This is intentional. Although the manual blank page removal done during the QC stage is more laborious, we believe it provides a higher quality validation that all documents containing any information will not be missed.

With the multi-level approach to double-feed detection, the IBML scanners have a very low occurrence of double-feeds vs. roller-transport scanners to ensure paper is not folded, creased, or skewed as it passes through scan, so data is not obscured. SSG scans at native resolution 300 dots per inch (dpi). The scanner captures both the front and back of every page, in both bi-tonal (black and white) and color. SSG scan operators perform a quality review of the images to ensure the following criteria are met:

- The images are delivered in the same orientation as presented in the folder
- Images are complete and not obscured by folds
- Legibility of image approximates that of the source, and is in proper order in the collection

File Requests

As we mentioned earlier, each project has a designated Project Manager, along with team leads in each production stage. One of the most important roles of the PM is to serve you.
You can call or email your PM at any time and make a request. Your PM will tell you where the records is in production. If the file is in process, it will be pulled and expedited.

Inbound Pick-Up

We utilize our own team to prepare and transport items for processing. Our drivers are full time employees required to pass the required fingerprint background, CJIS training, security addendum and drug testing. Our drivers are full time SSG

employees. When transporting CJIS related information, all required security measures are implemented including but not limited to:

- Vehicle containers are always locked
- Vehicles are never left unattended; pick -up and return of materials includes two drivers.
- All boxes are scanned (utilizing our barcode technology) upon pick-up and upon arrival to our location.