Tower MSA Partners, LLC

System and Organization Controls Report (SOC 3)

Independent Report of the Controls to meet the criteria for the Security and Confidentiality categories for the period of March 16, 2021 through March 15, 2022.

KirkpatrickPrice

TABLE OF CONTENTS

ASSERTION OF TOWER MSA PARTNERS, LLC MANAGEMENT

ASSERTION OF TOWER MSA PARTNERS, LLC MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within Tower MSA Partners, LLC's Medicare secondary payer services and mandatory section 111 reporting services system (system) throughout the period March 16, 2021, to March 15, 2022, to provide reasonable assurance that Tower MSA Partners, LLC's service commitments and system requirements relevant to Security and Confidentiality were achieved. Our description of the boundaries of the system is presented in section A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period March 16, 2021, to March 15, 2022, to provide reasonable assurance that Tower MSA Partners, LLC's service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). Tower MSA Partners, LLC's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in section B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period March 16, 2021, to March 15, 2022, to provide reasonable assurance that Tower MSA Partners, LLC's service commitments and system requirements were achieved based on the applicable trust services criteria.

INDEPENDENT SERVICE AUDITOR'S REPORT

Rita Wilson
CEO
Tower MSA Partners, LLC
223 NE 5th Avenue, Suite 101
Delray Beach, FL 33483

Scope
We have examined Tower MSA Partners, LLC's accompanying assertion titled "Assertion of Tower MSA Partners, LLC Management" (assertion) that the controls within Tower MSA Partners, LLC's Medicare secondary payer services and mandatory section 111 reporting services system (system) were effective throughout the period March 16, 2021, to March 15, 2022, to provide reasonable assurance that Tower MSA Partners, LLC's service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Service Organization's Responsibilities
Tower MSA Partners, LLC is responsible for its service commitment and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Tower MSA Partners, LLC's service commitments and system requirements were achieved. Tower MSA Partners, LLC has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Tower MSA Partners, LLC is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities
Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:
- Obtaining an understanding of the system and the service organization's service commitments and system requirements

- Assessing the risks that controls were not effective to achieve Tower MSA Partners, LLC's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Tower MSA Partners, LLC's service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Tower MSA Partners, LLC's Medicare Secondary Payer Services and Mandatory Section 111 Reporting Services system were effective throughout the period March 16, 2021, to March 15, 2022, to provide reasonable assurance that Tower MSA Partners, LLC's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Joseph Kirkpatrick
CPA, CISSP, CGEIT, CISA, CRISC, QSA
4235 Hillsboro Pike, Suite 300
Nashville, TN 37215

April 11, 2022

TOWER MSA PARTNERS, LLC'S DESCRIPTION OF ITS MEDICARE SECONDARY PAYER SERVICES AND MANDATORY SECTION 111 REPORTING SERVICES SYSTEM

SECTION A:
TOWER MSA PARTNERS, LLC'S DESCRIPTION OF THE BOUNDARIES OF ITS MEDICARE SECONDARY PAYER SERVICES AND MANDATORY SECTION 111 REPORTING SERVICES SYSTEM

Services Provided

Tower MSA Partners, LLC (Tower), established in 2011, provides Medicare Secondary Payer (MSP) services through its proprietary MSP Automation Technology Suite, which provides end-to-end visibility of claim activity from Section 111 Query and Centers for Medicare & Medicaid Services (CMS) reporting module through conditional payment search initiation and negotiation, Pre-MSA Triage Assessment, and cost driver intervention through final Medicare Set-Aside (MSA) and CMS submission.

Services Offered

Pre-MSA Triage Assessment

- Projected preliminary exposure based on current medical and pharmacy treatment regimen
- Snapshot view of MSA exposure in a non-discoverable (not an MSA) format
- Overview of inappropriate, unnecessary treatment and cost drivers that may impact MSA/settlement
- Case-specific recommendations based on jurisdictional issues and opportunities
- Action plan and next steps to optimize settlement outcomes before the MSA is prepared

Medicare Set-Aside Arrangement –Workers' Compensation & Liability

- Prepared by licensed, certified medical, legal and pharmacy professionals
- Medicare Set-Aside cost projection of Medicare covered services and future care
- No additional charge for complex cases
- Social Security Status and determination
- Automatic conditional payment search (with corporate Authorization to Represent)
- Structured settlement recommendation if appropriate
- RUSH cases at no additional charge
- Option to prepare per Non-Submit MSA criteria

Physician Follow-Up (Includes Direct Contact with Treating Physician)
- Completed at no charge in conjunction with MSA/CMS submission
- Contact with treating physician to obtain written confirmation of specific treatment patterns
- Confirm discontinuation of inappropriate medications
- Request transfer from brand to generic drug formulation
- Confirmation last treatment date and active, injury related drug regimen

MSA 2nd Opinion (2nd Opinion Review at No Charge)

- No charge review of another company's MSA to identify cost mitigation opportunities
- Confirm Medicare coverage based on accepted body parts and ICD10
- Identify interventions that could mitigate exposure, i.e., surgeries, and medications
- Obtain physician letters can be obtained to document Rx treatment changes
- Capture Rx price changes

Prescription Drug Treatment Review & Intervention

- Physician Peer Review including treating physician contact
- Completed by physicians licensed in occupational and physical medicine
- Recommendations evidentiary based on best practices in medical treatment
- Peer to peer contact and dialogue with treating physician (per jurisdiction)
- Obtain written confirmation of agreement to treatment changes

Clinical Oversight (Following Physician Peer Review)

- Oversight by a registered nurse in follow-up to Physician Peer Review
- Continued contact with treating physician before and after each office visit
- Ongoing reinforcement of changes in treating physician's written agreement
- Communication to client after each office visit to confirm continued progressor issues
- Identification of drugs that should be blocked with Pharmacy Benefit Manager as weaning and agreed changes occur
- Re-engagement of reviewing physician as needed to enforce approved drug regimen
- Update of MSA when CMS-approved evidence of optimized treatment is secured

CMS Submission

- Submission of MSA cost projection to CMS for approval
- Follow up with CMS until final decision received
- Submission of Re-Review, if needed

Medical Cost Projection

- Cost projection of Medicare/non-Medicare covered services and future care
- No additional charge for complex cases
- Social Security Status and determination
- Conditional lien search upon request
- Structured settlement recommendation if appropriate

Life Care Plan

- Estimates both medical and non-medical needs of patient with catastrophic injury

Social Security Determination & Medicare Beneficiary Check

- Verification of Social Security eligibility
- Verification of Medicare beneficiary entitlement and status determination

Conditional Payment Search (Completed at No Charge If Requested as Part of MSA Service)

- Obtain carrier's Letter of Authority or beneficiary's Proof of Representation
- Upload of authorization to Medicare Secondary Payer Recovery Portal (MSPRP) to establish case
- Contact with Benefits Coordination and Recovery Center (BCRC) to obtain Lead ID# and track through assignment of Case ID#
- Request conditional payment letter from BCRC/CRC – follow up until received

Conditional Payment Dispute/Negotiation

- Analysis of conditional lien information from BCRC/CRC
- Research all ICD10 codes per state jurisdictional statutes
- Prepare legal argument citing rationale for removal of unrelated charges
- Submit to BCRC/CRC via MSPRP
- Negotiate with BCRC/CRC to secure approval of disputed charges

Medicare, Medicaid, and SCHIP Extension Act (MMSEA) Section 111 Mandatory Insurance Reporting

- Establish claims eligibility electronic data interchange between Tower MSA Partners and Claims System
- Execute monthly query function via Centers for Medicare and Medicaid Services' (CMS's) Health Insurance Portability and Accessibility Act (HIPAA) Eligibility Wrapper (HEW) Query software
- Execute quarterly (or more frequent) CMS submission of new, updated, and deleted records
- Exchange of data between Responsible Reporting Entity (RRE) and Tower MSA Partners
  - Electronic eligibility upload and automated updates
  - Manual entry via secure Web portal
- Dedicated Reporting Manager (RM) specifically assigned to RRE
  - Prepares and tracks 30-day implementation timeline for new RRE clients
  - Ensures timely data transfer between all parties
  - Informs RRE of reporting updates and changes from CMS
  - Provides response file analysis and direct communication with RM
  - Evaluates CMS's disposition, error, and compliance flag code
- Data storage for 10 years per the MMSEANGHP user guide

Service Delivery

New clients (adjusters) are sought directly by the organization via marketing materials and word of mouth. Service agreements are executed with large clients, and service descriptions are communicated via email to remaining clients. Clients must request access to Tower portals, and a Tower manager creates a unique account for the client. User account information is sent to the client for access to the portal. Clients upload claim data to the Tower Client Portal (Tower OS) or provide data via email, fax, hardcopy, or thumb drive for Tower personnel to upload to the portal. Tower personnel sort, triage, and clean records for the report, and nurses review the report and summarize project out medical needs. Upon completion, the report goes through three or four rounds of quality assurance (QA) to ensure accuracy and completeness, then the report is provided

to the client for review. The report may also be uploaded to the CMS portal for approval. Adjusters have limited views of data within the portal, and adjuster accounts are never removed. User accounts can be reused if adjusters have additional claims to be reviewed and submitted.

Infrastructure

Tower maintains network diagrams, pictured below, to depict network connectivity. The Chief Technology Officer (CTO) is responsible for reviewing and updating network diagrams annually or upon significant changes. The organization also manually maintains an inventory of its systems in use. The systems inventory, which includes virtual systems, includes the following information for each listing:

- Name
- ID
- IP address
- Location
- Device type
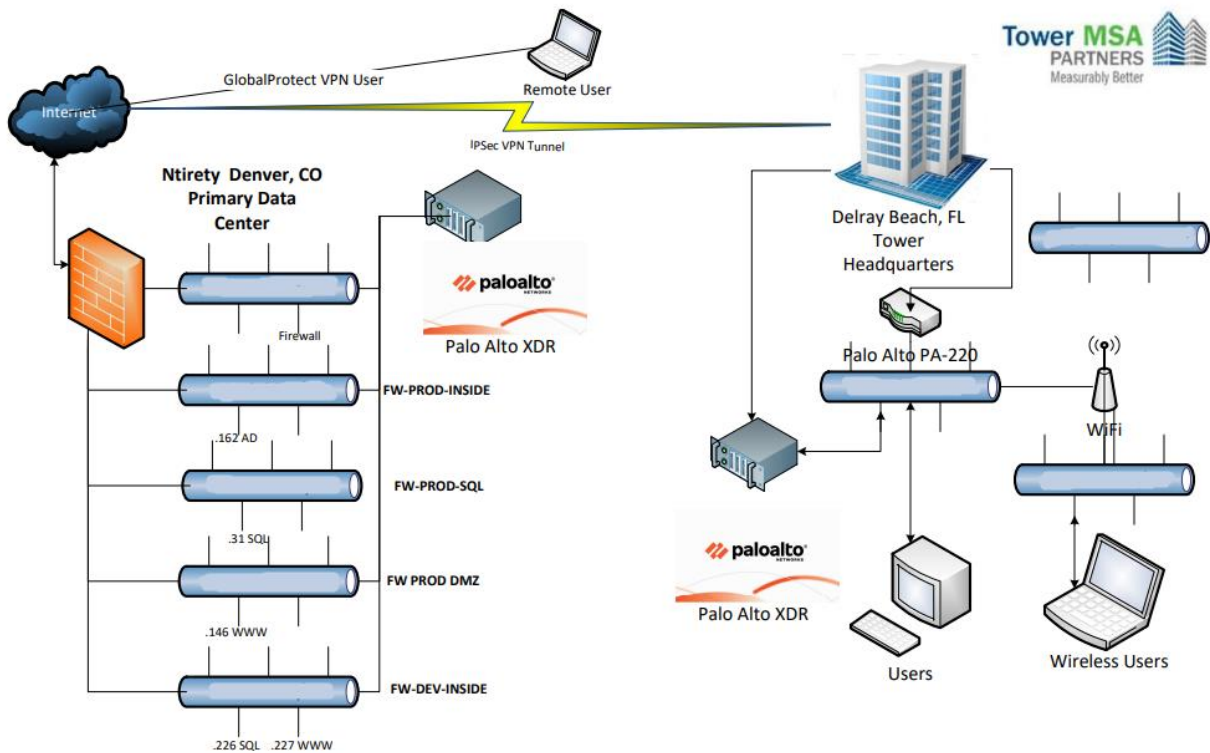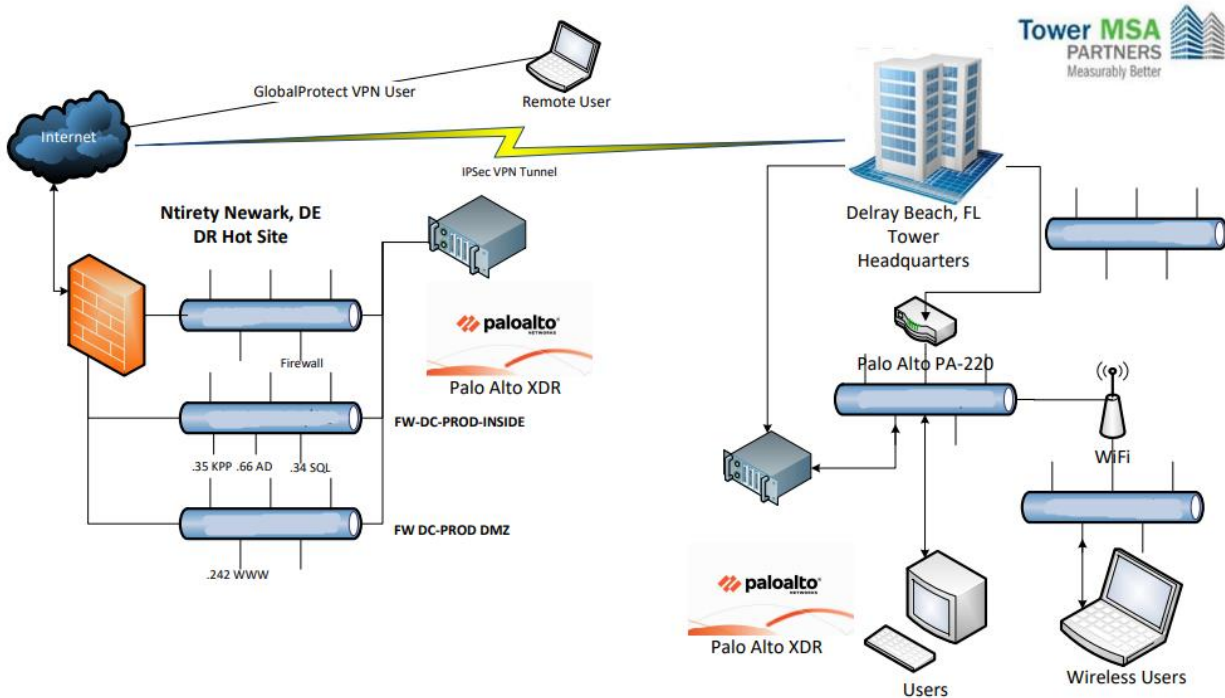
Software

The organization manually maintains a software inventory that includes the name, product, version, and license quantity. Tower uses the following critical software:

- Adobe DC Pro
- Cisco AnyConnect virtual private network (VPN)
- Cortex XDR
- Egnyte
- GoTo Connect
- Java
- Office 365
- Plantronics Hub
- Section 111
- Tower OS

People

Tower is structured into distinct functional departments that are headed by members of a C-level executive team with direct reporting lines to the CEO. This executive team consists of the following roles:

- CEO – Oversight over all strategic initiatives, business development, sales, marketing and operational activities, and IT systems development. The CEO seeks business partnerships that bring innovation solutions in support of MSP compliance. The executive team that oversees all of Tower's business initiatives include the following leadership positions.

- Chief Operations Officer (COO) – Oversight over all day-to-day administrative and operational functions of Tower's business. As second in the chain of command reporting

to the CEO, the COO creates, manages and maintains all policies and procedures associated with the company' operational and clinical departments. Direct responsibilities include all recruiting, hiring and management of departmental staff, as well as full responsibility for the quality of Tower's work product and maintaining performance metrics as established by the CEO. The COO must maintain and enforce currency in industry certifications including, but not limited to MSP Consultant Certified, Registered Nurse, Certified Pharmacy Technician, Adjuster Certification, and Legal.

- Chief Compliance Officer (CCO) – Oversight over all aspects of regulatory compliance associated with the MSP status and local, state, and federal laws. Specific responsibilities include ensuring the integrity and quality of Tower's services and products, including its MSA program. The CCO is directly responsible for Tower's performance and approval metrics with the Centers for Medicare and Medicaid (CMS), and for the policies and procedures associated with Medicare Set-Aside preparation and QA. The CCO provides education and consultation to Tower's clients on all aspects of MSP compliance, presents at industry conferences, and writes articles and posts for Tower's MSP compliance blog on MSAs and compliance issues.

- Chief Financial Officer (CFO) – Oversight and management over all financial actions of the company. Responsibilities include tracking cash flow and financial planning as well as analyzing the company's financial strengths and weaknesses and proposing corrective actions. Additional duties include managing finance and accounting, for ensuring that the company's financial reports are accurate and completed in a timely manner, and for oversight over both federal and state taxation issues. At Tower, the CFO plays a vital role in the company's strategic initiatives and has significant input in the company's investments, capital structure and how the company manages its income and expenses.

- Executive Vice President (EVP), Strategic Services – Oversight over all sales initiatives, including but not limited to sales presentations, RFP preparation, conference participation and sponsorship, marketing, client education marketing, as well as account management for all of Tower's existing clients. This position works directly with the VP, IT to provide sales and marketing support for Tower's Section 111 Reporting platform and reporting dashboard. This position is also responsible to the CEO to identify and develop innovative offerings and to improve existing services.

- CTO – Oversight over all aspects of Tower's technology offerings and infrastructure, including, but not limited to systems architecture and disaster recovery/business continuity, and the maintenance and enhancement of its internal systems for all aspects of MSP compliance and Section 111 Mandatory Insurer Reporting. In addition to daily oversight over all development, this position has management oversight over the company's Information Security Program, including all policies and procedures associated with security, password and data access, confidentiality, third-party security, system configuration management and personnel security management and incident reporting.

As a Florida LLC, Tower is not required to have a formal board of directors. The CEO and COO are the sole equity partners with ownership in Tower, and the CEO and COO have management oversight that encompasses the full scope of Tower's financial, operational, and sales and marketing business operations.

The following organization chart depicts Tower's organizational structure.

Tower MSA Partners
Management Organizational Chart
01/01/2022
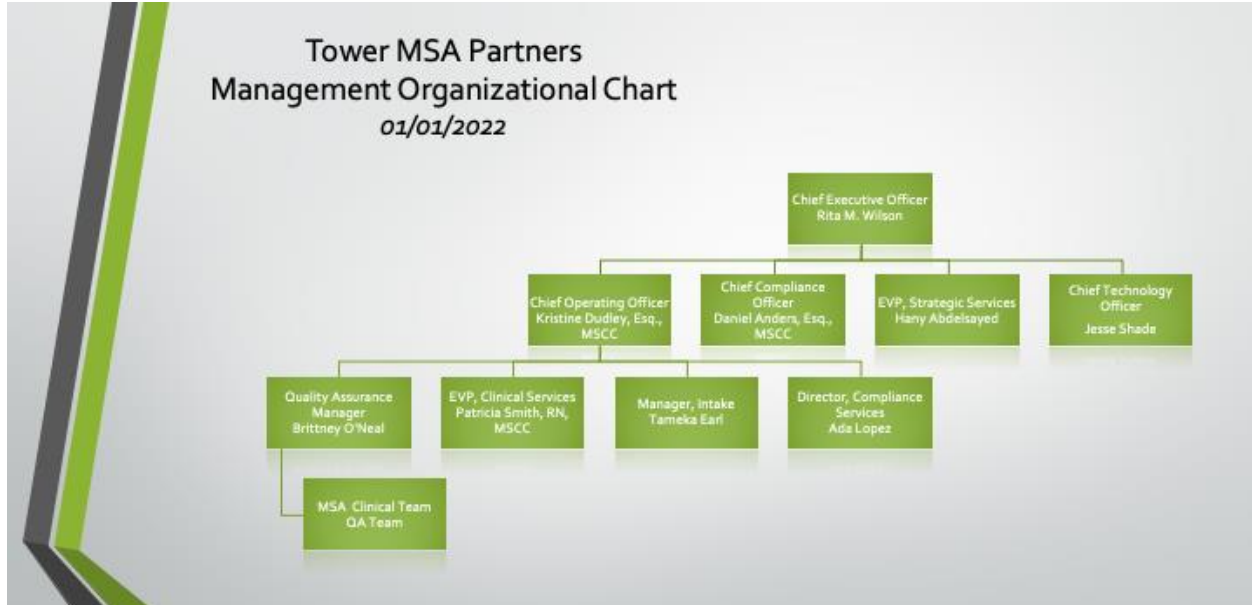
Data

As a part of its MSP services and mandatory Section 111 reporting services system, the company maintains emails and faxes to and from clients, adjusters, attorneys, and medical providers, as well as legal documents and legal records. These documents are stored on an encrypted storage area network (SAN) in the Rackspace cloud. In addition, many of the medical records and other documents are also stored and encrypted on Egnyte.

Dataflows are documented in the following diagrams to track how data enters, flows within the network, and is stored within the Tower environment.

Section 111 Data Flow Diagram

Data is sent to Tower via Secure FTP or it is manually typed into our Secure Portal

CMS Secure FTP Server

Data Acquisition

Secure-ftp.towermsa.com

Section 111 Data is obtained via:
- File Upload
- Online Data Entry

Data is made electronic if not received electronically

Data is acquired weekly, run thru a number of data checks and a Response file is returned to the customer vis Secure FTP if they are a Feed client.

Monthly, a query file is sent to CMS for each RRE. A response file is made available for download by Tower about a week later. We process that and a response file is produced for each RRE.

Quarterly we report claim data to CMS for each RRE. A response file is made available for download by Tower about a week later. We process that and a response file is produced for each RRE.

Step 1 – Aquire data

Step 2 – Create / Import data

Step 3 – Query & Respond

Data Storage & Document Destruction

Section111_ProcV2 SQL Database

Document Storage on encrypted secure-files folder

We do not archive data unless expressly asked to do so by the customer.
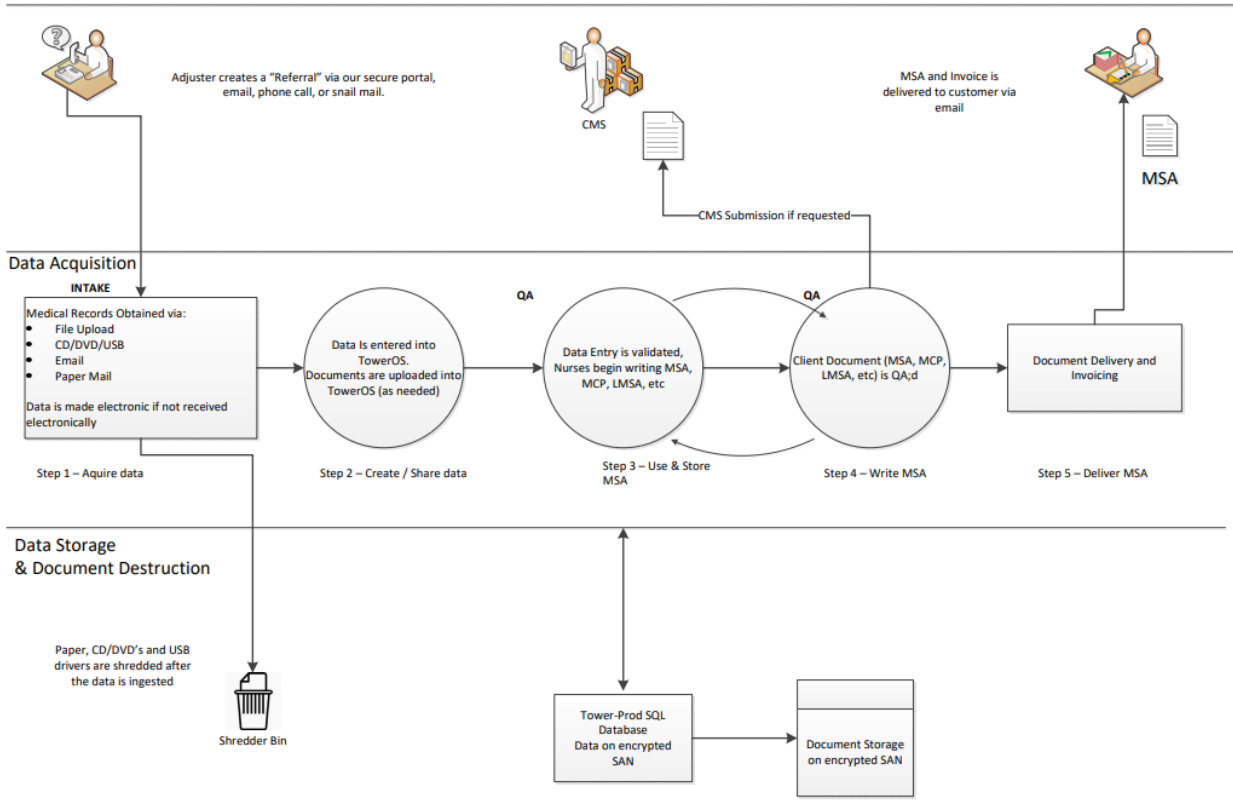

TowerOS Data Flow Diagram v1.1

Adjuster creates a "Referral" via our secure portal, email, phone call, or snail mail.

CMS

MSA and Invoice is delivered to customer via email

MSA

CMS Submission if requested

Data Acquisition

INTAKE

Medical Records Obtained via:
- File Upload
- CD/DVD/USB
- Email
- Paper Mail

Data is made electronic if not received electronically

Data Is entered into TowerOS. Documents are uploaded into TowerOS (as needed)

QA

Data Entry is validated, Nurses begin writing MSA, MCP, LMSA, etc

QA

Client Document (MSA, MCP, LMSA, etc) is QA;d

Document Delivery and Invoicing

Step 1 – Aquire data

Step 2 – Create / Share data

Step 3 – Use & Store MSA

Step 4 – Write MSA

Step 5 – Deliver MSA

Data Storage & Document Destruction

Paper, CD/DVD's and USB drivers are shredded after the data is ingested

Shredder Bin

Tower-Prod SQL Database Data on encrypted SAN

Document Storage on encrypted SAN

Client and internal transactions processed through Tower OS and Section 111 are protected from incomplete transmission, misrouting, message alteration, disclosure, and message duplication

using Federal Information Processing Standard (FIPS)-approved encryption algorithms. The company maintains the following procedures for securing data via encryption and authentication:

- RSA (2048) Secure Sockets Layer (SSL) certificates are in place on each entry point to our systems
- TLS 1.2 is used to secure communications
- A Palo Alto GlobalProtect VPN is in place to access Tower systems remotely
- Most data transmission is via direct uploads to Tower portals or via Secure File Transfer Protocol (SFTP)
- External tools from Palo Alto and Ntirety are used to manage and secure the environment

Processes and Procedures

Management has developed and communicated procedures to guide the provision of the organization's services. Changes to procedures are performed annually and authorized by management. These procedures cover the following key security life cycle areas:

- Data classification
- Categorization of information
- Assessment of the business impact resulting from proposed security approaches
- Selection, documentation, and implementation of security controls
- Performance of annual management self-assessments to assess security controls
- Authorization, changes to, and termination of information system access
- Monitoring security controls
- Management of access and roles
- Maintenance and support of the security system and necessary backup and offline storage
- Incident response
- Maintenance of restricted access to system configurations, user functionality, master passwords, powerful utilities, and security devices

Contractual Commitments

Tower executes Master Services Agreements with clients to communicate agreed upon services, obligations, and terms. For third-party vendors and/or business partners, service-level agreements (SLAs) are used. Non-disclosure agreements (NDAs) are also used with third parties prior to sharing sensitive information.

System Design

Tower designs its Medicare secondary payer services and mandatory Section 111 reporting services system to meet its regulatory and contractual commitments. These commitments are based on the services that Tower provides to its clients, the laws and regulations that govern the provision of those services, and the financial, operational, and compliance requirements that Tower has established for its services. Tower establishes operational requirements in its system design that support the achievement of its regulatory and contractual commitments. These requirements are communicated in Tower's system policies and procedures, system design documentation, and contracts with clients.