MedPro Systems, LLC

System and Organization Controls (SOC) 3

Report on MedPro Systems, LLC's Assertion Related to Its Healthcare Provider Data Management Software Services System Relevant to Security

Throughout the Period
January 1, 2025 to June 30, 2025

Contents

I. Independent Service Auditor's Report on a SOC 3 Examination

Tel: 212-885-8000
Fax: 212-697-1299
www.bdo.com

200 Park Avenue, 38th Floor
New York, NY 10166

Independent Service Auditor's Report on a SOC 3 Examination

To the Management of
MedPro Systems, LLC
Mt. Arlington, New Jersey

Scope

We have examined MedPro Systems, LLC's (MedPro or service organization) accompanying assertion titled *Assertion of MedPro Systems, LLC Management* (assertion) that the controls within MedPro's Healthcare Provider Data Management Software Services System (the System) were effective throughout the period January 1, 2025 to June 30, 2025 to provide reasonable assurance that MedPro's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) *se*t forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*.

MedPro uses subservice organizations to provide certain services. The subservice organizations and the services provided are listed in Attachment A. The assertion indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at MedPro, to achieve MedPro's service commitments and system requirements based on the applicable trust services criteria. MedPro's description of the boundaries of the System in Attachment A presents the types of complementary subservice organization controls assumed in the design of MedPro's controls but does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

MedPro is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the System to provide reasonable assurance that MedPro's service commitments and system requirements were achieved. MedPro has also provided the accompanying assertion about the effectiveness of controls within the System. When preparing its assertion, MedPro 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 controls within the System.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the System were effective throughout the period January 1, 2025 to June 30, 2025 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 AICPA. 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 the service organization'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 MedPro'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.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

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 are 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 risks that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Other Matter

As noted in MedPro Systems, LLC's Description of Its Healthcare Provider Data Management Software Services System, control CC3.1.1 related to the annual risk assessment, CC4.1.1 related to the annual internal control assessment, and CC4.1.2 related to the annual penetration test and vulnerability scan within CC3.3, CC4.1, and CC4.2 did not operate during the period of January 1, 2025 to June 30, 2024. Therefore, we did not test the operating effectiveness of these controls and the related criteria CC3.3, The entity considers the potential for fraud in assessing risks to the achievement of objectives; CC4.1, The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning; and CC4.2 The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

Opinion

In our opinion, management's assertion that the controls within MedPro's system were effective throughout the period January 1, 2025 to June 30, 2025 to provide reasonable assurance that MedPro's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Restricted Use

This report is intended solely for the information and use of MedPro, user entities of MedPro's system during some or all of the period January 1, 2025 to June 30, 2025, business partners of MedPro subject to risks arising from interactions with the System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties.
- Internal control and its limitations.
- Complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements, and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

BDO USA, P.C.

October 01, 2025

II. Assertion of MedPro Systems, LLC Management

Assertion of MedPro Systems, LLC Management

We are responsible for designing, implementing, operating, and maintaining effective controls within MedPro Systems, LLC's (MedPro or the service organization) Healthcare Provider Data Management Software Services System (the System) throughout the period January 1, 2025 to June 30, 2025, to provide reasonable assurance that MedPro's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in *TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*. Our description of the boundaries of the System is presented in Attachment A, *MedPro Systems, LLC's Description of the Boundaries of Its Healthcare Provider Data Management Software Services System* and identifies the aspects of the System covered by our assertion.

MedPro uses subservice organizations to provide certain services. The subservice organizations and the services provided are listed in Attachment A. The description of the boundaries of the System in Attachment A indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at MedPro, to achieve MedPro's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the System presents the types of complementary subservice organization controls assumed in the design of MedPro's controls. The description of the boundaries of the System does not disclose the actual controls at the subservice organizations.

We have performed an evaluation of the effectiveness of the controls within the System throughout the period January 1, 2025 to June 30, 2025 to provide reasonable assurance that MedPro's service commitments and system requirements were achieved based on the applicable trust services criteria. MedPro'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 Attachment 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.

As noted in MedPro Systems, LLC's Description of Its Healthcare Provider Data Management Software Services System, control CC3.1.1 related to the annual risk assessment, CC4.1.1 related to the annual internal control assessment, and CC4.1.2 related to the annual penetration test and vulnerability scan within CC3.3, CC4.1, and CC4.2 did not operate during the period of January 1, 2025 to June 30, 2024, because the circumstances that warrant the operation of these controls did not occur during the examination period.

We assert that the controls within the System were effective throughout the period January 1, 2025 to June 30, 2025 to provide reasonable assurance that MedPro's service commitments and system requirements were achieved based on the applicable trust services criteria.

MedPro Systems, LLC

October 01, 2025

Attachment A — MedPro Systems, LLC's Description of the Boundaries of Its Healthcare Provider Data Management Software Services System

Attachment A — MedPro Systems, LLC's Description of the Boundaries of Its Healthcare Provider Data Management Software Services System

Scope and Description of the Boundaries of the System

This is a SOC 3 report and includes a description of the boundaries of MedPro Systems, LLC's (MedPro, service organization, or Company) Healthcare Provider Data Management Software Services System and the controls in place to meet the applicable trust services criteria of security set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*, throughout the period January 1, 2025 to June 30, 2025 which may be relevant to the users of the System. It does not encompass all aspects of the services provided or procedures followed for other activities performed by MedPro.

MedPro uses subservice organizations to provide certain services. The subservice organizations and the services provided are listed in the following table. The description of the boundaries of the System does not disclose the actual controls at the subservice organizations.

Subservice Organization	Services Provided
Cologix Inc. (Cologix)	Production colocation
CyFlare Security Inc. (CyFlare)	SOC as a Service
ProShred Security	Shredding services
Netrix LLC (Netrix)	Disaster recovery colocation
Sophos Ltd. (Sophos)	Detection and prevention services

Company Background

The company was founded in 1989 as Hilltown Systems to design, build, implement, and support custom software applications to solve business needs with technology. In 2001, Hilltown started consulting work in the Life Sciences industry to help companies meet the newly enacted Prescription Drug Marketing Act (PDMA) requirements. Seeing a clear and growing need in the industry to support pharmaceutical manufacturers with ongoing healthcare license validation to meet federal and state regulations, MedPro Systems was established in Mount Arlington, New Jersey. In 2011, MedPro expanded beyond core healthcare license validation solutions to support Life Sciences customers with capture and reporting of healthcare provider data to meet U.S. federal, state, and local reporting requirements. Beginning in 2021, MedPro continued its growth by providing international reporting services.

At the heart of MedPro's corporate philosophy are six core values: Mutuality, Empowerment, Determination, Partnership, Reliability, and Ownership.

Services Provided

MedPro's software and services consists of acquiring and managing healthcare practitioner (HCP) and healthcare organization (HCO) data from authoritative sources (government agencies, including federal, state, and other jurisdictions; as well as other third-party sources of information from which MedPro acquires data). Users of MedPro's services provide MedPro with their HCP and HCO

data in an agreed-upon format and delivery methodology for the purpose of data verification, enrichment, and/or reporting to comply with regulatory obligations and business objectives.

MedPro provides U.S. and Canadian HCP and HCO license and other identification data directly from authoritative sources. This data, combined with MedPro's software applications and analytical and consulting services, is designed to optimize technology and minimize costly manual activities. MedPro additionally provides services for life sciences companies to report payments and transfers of value to healthcare providers and healthcare organizations to meet international and U.S. federal, state, and local requirements.

System Incidents

A system incident is an incident that leads to the loss of, or disruption to, operations, services, or functions and results in MedPro's failure to achieve its service commitments or system requirements. Such an occurrence may arise from a security event, security incident, failure to comply with applicable laws and regulations, error, or other means. In determining whether a system incident occurred resulting in MedPro's failure to achieve one or more of its service commitments or system requirements, considerations may include, but are not limited to, the following:

- Whether the occurrence resulted from one or more controls that were not suitably designed or operating effectively.
- Whether public disclosure of the occurrence was required (or is likely to be required) by cybersecurity laws or regulations.
- Whether the occurrence had a material effect on the service organization's financial position or results of operations and required disclosure in a financial statement filing.
- Whether the occurrence resulted in sanctions by any legal or regulatory agency.
- Whether the occurrence resulted in the service organization's withdrawal from material markets or cancellation of material contracts.

Incidents and events relevant to MedPro's service commitments and system requirements based on the applicable trust services criteria are important in monitoring, identifying, and evaluating if a system incident has occurred; however, incidents and events relevant to MedPro's service commitments and system requirements based on the applicable trust services criteria do not always rise to the level of a system incident. The evaluation of an incident or event relevant to MedPro's service commitments and system requirements based on the applicable trust services criteria will make that determination.

MedPro did not identify any system incidents that occurred during the period January 1, 2025 to June 30, 2025 resulting in MedPro's failure to achieve one or more of its service commitments or system requirements based on these considerations.

Components of the System Used to Provide the Services

Infrastructure

MedPro utilizes multiple private colocation data centers to host its production and disaster recovery environments, in addition to leveraging Oracle Cloud Infrastructure for Oracle Analytics Cloud (OAC)

reporting and Auth0 for Identity Provider (IDP). Hardware used to host MedPro applications and services is fully owned and managed by the company.

The in-scope infrastructure supporting MedPro's applications and services consists of multiple applications, operating systems, and databases as shown in the table below:

Production Application	Business Function Description	Physical Location
Virtual Private Network (VPN)	Secure remote access to production and disaster recovery environments	Cologix, Netrix
Firewall	Access control and prevention of unauthorized traffic	Cologix, Netrix
Load Balancer	Distributed application/network traffic	Cologix, Netrix
VMware ESXi	Virtualized computing	Cologix, Netrix
Operating Systems	Windows Server, Oracle Linux	Cologix, Netrix
IIS	Web server software	Cologix, Netrix
Oracle DB	Database management system (DBMS)	Cologix, Netrix
Elastic	Search and analytics engine	Cologix, Netrix
Redis Cache	In-memory data store	Cologix, Netrix
Pure Storage	Data storage	Cologix, Netrix
Auth0	Identity management	Auth0 Cloud (US-4)
Oracle Analytics Cloud	Analytics and business intelligence tools for data visualization, reporting, and advanced analytics	OCI (US East – Ashburn)

Physical Locations

MedPro's office is located in Mount Arlington, New Jersey. MedPro's production data center is hosted by Cologix in Cedar Knolls, New Jersey. MedPro's disaster recovery data center is hosted by Netrix in Wyomissing, Pennsylvania.

Software

Primary software used to support MedPro's systems includes the following:

Software	Purpose
Jira	Collaboration tool to plan, track, and manage work and issues
Jira Service Management	IT service management (ITSM) platform for customer support
Confluence	Collaboration tool for documentation
Slack	Company IM communications
Sophos	Next-generation antivirus, endpoint detection and response (EDR) security application

Software	Purpose
Stellar Cyber	Security information and event management (SIEM)
Duo	Multifactor authentication (MFA)
InvGate	IT asset repository
MangeEngine Endpoint Central	Patch management and software deployment
Octopus Deploy	Deployment and release management
Azure DevOps	Git-based repositories for source control

The applications covered within the scope of this report are as follows:

Application Name	Purpose
MedProID	Software and services that assist life sciences companies manage, validate, and enrich healthcare provider and healthcare organization attributes to meet business needs and regulatory requirements.
MedPro Compliance Reporting ID (MCR)	Software and services that assist life sciences companies collect, enrich, remediate, and report transfers of value, interactions, and prescription drug samples provided to healthcare providers, healthcare organizations, and affiliated entities to comply with regulatory requirements.

People

MedPro employees provide support for the above services in each of the following functional areas:

- *Senior Leadership Team* — Responsible for providing general oversight and strategic planning of operations.
- *Infrastructure* — Responsible for security, monitoring, and administration of access controls and the provisioning, installation/configuration, operation, and maintenance of systems hardware and software relevant to the System.
- *Product Development* — Responsible for creating requirements for products and services.
- *Development* — Responsible for delivering products in accordance with the functional specification.
- *Data Operations* — Responsible for delivering data to meet the requirements of the products and services.
- *Customer Success* — Responsible for serving customers by providing product and service information and resolving product and service issues.
- *Quality Management* — Responsible for performing regularly scheduled assessments relative to defined standards, providing continuous improvement initiatives, and assessing legal and regulatory requirements.

Processes and Procedures

In order to consistently meet customer requirements and facilitate continuous improvement processes, MedPro's quality management system (QMS) uses ACE Essentials, a preconfigured electronic quality management system (eQMS), for QMS documentation: policies, standard operating procedures (SOPs), companywide work instructions (WIs), QMS reports, QMS training, corrective and preventative action (CAPA), and QMS report management, and documentation workflow. Non-companywide departmental work instructions are maintained in Confluence, a knowledge and collaboration tool from Atlassian used to control reference documentation.

QMS documentation is reviewed and updated as necessary as part of the annual quality review process. The Quality Management Team works with business process owners to edit and approve documentation; all documentation, regardless of whether it has changed, is then assigned to MedPro employees based on their role.

Information Security Training is conducted through Paylocity, MedPro's payroll and human capital management software.

MedPro utilizes Jira, a software application used for issue tracking and project management from Atlassian, to manage change control of systems and documentation. MedPro's Quality Management Team manages a help desk portal in Jira, where employees can open a ticket to suggest a new document or edits to an existing document. When a ticket is opened, the Quality Management Team works with business process owners to review and, if necessary, draft, edit, and approve new or updated documentation and assign training. The ticket is closed at the end of the review process.

The policies and procedures supporting control activities are as follows:

Document ID	Document Title	Document Purpose
GLB-FRM-0003	Information Security Incident Response Report	The purpose of this form is to document confirmed information security incidents and provide a record of all findings, actions, and approvals.
GLB-FRM-0004	Tabletop Exercise Summary Report	The purpose of this form is to document Tabletop Exercise Summary Reports.
GLB-FRM-0005	Disaster Recovery Failover Test Summary Report	The purpose of this form is to document Disaster Recovery Failover Test Summary Reports.
GLB-FRM-0006	MedPro Systems Risk Assessment Report	The purpose of this Risk Assessment Report is to document the identified risks and proposed treatments affecting the Company's products and services in order to take proactive steps to mitigate harm, prioritize areas of concern, and implement appropriate control measures, to meet business obligations and fulfill legal and compliance requirements.
GLB-POL-0001	Quality Manual	The purpose of this policy is to define MedPro's quality objectives.
GLB-POL-0002	System Security Maintenance	The purpose of this policy is to document MedPro's system security maintenance standards for information systems.

Document ID	Document Title	Document Purpose
GLB-POL-0003	Software Development Life Cycle	The purpose of this policy is to describe the standards used by MedPro Systems in developing and/or implementing software per the stated requirements for functionality, budget, and security.
GLB-POL-0005	Information Security Classification	The purpose of this policy is to document how MedPro classifies data and information to meet the organization's security needs based on confidentiality, integrity, availability, and relevant interested party requirements.
GLB-POL-0007	Business Continuity Plan	The purpose of MedPro's Business Continuity Plan (BCP) policy is to help ensure the uninterrupted delivery of critical services, maintain data integrity, and minimize downtime in the event of unforeseen disruptions or disasters. This policy aims to safeguard the organization's reputation, customer trust, and overall operational resilience.
GLB-POL-0008	Information Security Management System Manual	The purpose of this policy is to document MedPro's aims and objectives for the management of information security.
GLB-POL-0010	Business Continuity and Information Security Objective Statements	The purpose of this policy is to document the objective statements for MedPro's policies and procedures related to business continuity, information security incident response, and IT disaster recovery. These specific policies and procedures are designed to protect critical business functions and IT systems by creating resilience against disruptions and compliance with quality and business objectives.
GLB-POL-0011	Segregation of Duties	The purpose of this policy is to establish guidelines for the segregation of duties (SOD) to ensure that MedPro's critical tasks are controlled to reduce the risk of errors, fraud, and unauthorized access to information and systems.
GLB-POL-0013	Acceptable Use of Laptop Administrative Access	The purpose of this policy is to establish requirements for the acceptable use of laptop administrative access when it is granted to a MedPro Systems employee in Microsoft Active Directory.
GLB-REF-0002	IT Disaster Recovery (DR) Playbook	The purpose of this reference document is to define the recovery processes for all computerized systems implemented and used by MedPro's IT-hosted solutions.
GLB-REF-0005	Information Security Incident Response Playbook	The purpose of this reference document is to describe how MedPro detects, analyzes, contains, eradicates, recovers from, and reports on information security incidents.
GLB-REF-0007	MedPro Systems Board of Directors Biographies	The purpose of this document is to provide biographical information on the MedPro Systems Board of Directors.

Document ID	Document Title	Document Purpose
GLB-SOP-0001	Formation of Standard Operating Procedures	The purpose of this procedure is to outline the procedures and policies for the formation of a Standard Operating Procedure (SOP). This process includes content, format, creation, and revision of an SOP.
GLB-SOP-0003	Electronic Document and Privacy Standards	The purpose of this procedure is for compliance with the electronic document and information privacy standards of the United States, European Union, and other jurisdictions.
GLB-SOP-0005	Physical Security	The purpose of this procedure is to define the MedPro policies and procedures for the management, control, monitoring, and removal of physical access to MedPro Systems office, colocation, and disaster recovery data center facilities.
GLB-SOP-0007	Corrective and Preventative Action	The purpose of this procedure is to define the policies and procedures for completing and documenting CAPA.
GLB-SOP-0008	Change Control	The purpose of this procedure is for controlling and implementing changes to MedPro Systems' products and services, system security, and QMS.
GLB-SOP-0009	Issue Tracking	The purpose of this procedure is to document and track issues related to an application, any part of an application, or supporting infrastructure that is not performing in compliance with stated system specifications.
GLB-SOP-0010	Customer Data Management	The purpose of this procedure is to outline the processes associated with the management of customer data. These policies and procedures include data maintenance, use, retention, and removal.
GLB-SOP-0011	Backup, Restore, and Disaster Recovery for Computerized Systems in IT Hosted Solutions	The purpose of this procedure is to define the recovery processes for all computerized systems implemented and used by MedPro Systems' IT-hosted solutions. These processes include the backup, restore, and disaster recovery for all computerized systems.
GLB-SOP-0013	Selection and Evaluation of Suppliers	The purpose of this procedure is to help ensure effective management and control of suppliers providing products and services, and the selection of products and services from approved suppliers associated with QMS.
GLB-SOP-0017	Training	The purpose of this procedure is to define policies and procedures for ensuring the competence of personnel performing work associated with the QMS. These policies and procedures define how requirements are established, fulfilled, recorded, and evaluated for effectiveness for MedPro Systems.
GLB-SOP-0018	Software Development Project Management	The purpose of this procedure is to define the Software Development Project Management (SDPM) lifecycle to help ensure the successful completion of all software projects developed and/or managed by MedPro Systems.

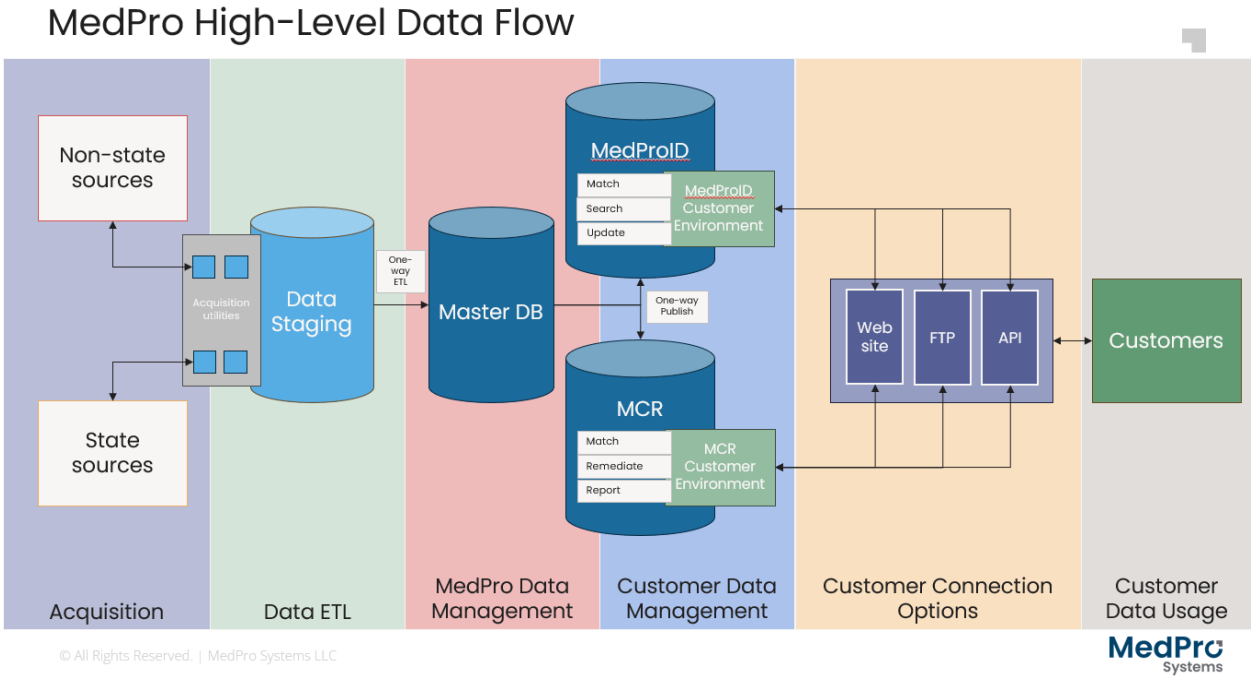
Document ID	Document Title	Document Purpose
GLB-SOP-0019	Internal Audit of Internal and External User Access	The purpose of this procedure is to ensure that access to customer-accessible MedPro Systems-owned and MedPro Systems-maintained production applications are granted, maintained, and revoked based on user roles.
GLB-SOP-0020	Employee Departmental Training	The purpose of this procedure is to outline the process of training employees on department-specific topics and tasks.
GLB-SOP-0021	Testing Automation System	The purpose of this procedure is to outline MedPro's Testing Automation System (TAS) for its core products: MedProID and MCR.
GLB-SOP-0022	Formation of Work Instructions	The purpose of this procedure is to outline the procedures and policies for the formation of Work Instruction documents. This includes content, format, creation, and revision of work instructions.
GLB-SOP-0023	Documented Information Management	The purpose of this procedure is to outline the processes associated with the management of documented information. These policies and procedures include documented information maintenance, use, retention, and removal.
GLB-SOP-0024	MedPro Data Management	The purpose of this procedure is to outline the processes associated with the management of MedPro data. These policies and procedures include data maintenance, use, retention, and removal.
GLB-SOP-0025	Logical Security	The purpose of this procedure is to outline the policies for the management, control, monitoring, and removal of logical access to assets owned and maintained by MedPro Systems.
GLB-SOP-0026	Information Security Incident Response	The purpose of this procedure is to define the information security (IS) response process. This process includes preparing for, responding to, and recovering from information security incidents.

Document ID	Document Title	Document Purpose
GLB-SOP-0027	MedPro Security Control Framework	The purpose of this procedure is to outline MedPro Systems' implementation of and continuing compliance with internal MedPro Security Controls. These Controls were established as a best practice for quality, information security, and business operations process reviews, as part of MedPro's continuous efforts to maintain security and operational excellence. Additionally, these Controls map to certain criteria of the following standards; the execution of these internal controls demonstrates compliance with aspects of these standards: • The National Institute of Standards and Technology Cybersecurity Framework (NSIT CSF) • The International Organization for Standardization (ISO) 27001 and 9001 certifications • The American Institute for Certified Public Accountants Systems and Organization Controls 2 (AICPA SOC 2)
GLB-SOP-0028	Recruiting, Onboarding, Role Change, Leave of Absence, and Off-Boarding	The purpose of this procedure is to document the processes MedPro follows for recruiting, onboarding, managing role changes, leaves of absence, and off-boarding employees and contractors.
GLB-SOP-0030	Risk Assessment and Mitigation	The purpose of this procedure is to describe how MedPro assesses and mitigates risks affecting the company's products and services.
GLB-WI-0005	Monitor and Manage MedPro Security Controls	The purpose of this Work Instruction is to provide documentation and guidance regarding adding, changing, removing, and monitoring and managing the quarterly, semiannual, and annual executions of MedPro's Security Controls. This Work Instruction also covers the annual review and approval of the MedPro Security Controls prior to their execution for the year.
GLB-WI-0006	Summarizing Board, Executive Committee, and Senior Leadership Team (SLT) Meetings	The purpose of this Work Instruction is to describe the process to summarize meeting minutes from the Board, Executive Committee, and Senior Leadership Team as content relates to the quality and information security management systems (QMS and ISMS). These summaries serve as evidence for MedPro Security Control #1012: Senior Leadership Team and Board Oversight and can be utilized for other purposes, including responding to customer questions/audits. Distribution of these summary reports beyond the stated purpose of complying with MedPro Security Control #1012: Senior Leadership Team and Board Oversight must be approved by a member of the Quality Management Team.

Document ID	Document Title	Document Purpose
GLB-WI-0008	Conducting Tabletop Exercises	The purpose of this Work Instruction is to establish a consistent manner in which tabletop exercises are conducted.
GLB-WI-0009	Conducting Disaster Recovery Failover Testing	The purpose of this Work Instruction is to describe how MedPro plans, executes, and debriefs DR failover testing.
GLB-WI-0011	Data Destruction	The purpose of this work instruction is to define the procedure for when data needs to be removed (destroyed) from all of MedPro's systems.

Data

The diagram below describes at a high level how data flows from authoritative sources through MedPro's applications and databases for customer consumption. The section labeled Customer Connection Options demonstrates how customer-provided data is processed and managed.



Complementary Subservice Organization Controls

In some instances, a service organization's controls cannot provide reasonable assurance that its service commitments and system requirements were achieved without the subservice organizations performing certain activities in a defined manner. Such activities are referred to as complementary subservice organization controls (CSOCs). The following CSOCs are those controls that MedPro's management assumed, in the design of the System, would be implemented by a subservice organization and are necessary, in combination with controls at MedPro, to provide reasonable

assurance that the service organization's service commitments and system requirements are achieved.

Number	CSOC	Applicable Criteria
Cologix Inc. and Netrix LLC		
1.	The subservice organization should have controls in place to help ensure secure physical infrastructure for hosting servers and applications.	CC6.4
2.	The subservice organization should have controls in place to help ensure physical security measures, including controlled access points, surveillance, and monitoring systems to protect customer data and IT assets, are operating.	CC6.4
CyFlare Security Inc.		
3.	The subservice organization should have controls in place to help ensure continuous real-time monitoring, detection, and response to potential security incidents across MedPro's environment.	CC7.1, CC7.2, CC7.3, CC7.4
Sophos Ltd.		
4.	The subservice organization should have controls to help ensure timely monitoring, detection, and response to security incidents.	CC7.1, CC7.2, CC7.3, CC7.4
5.	The subservice organization should have controls related to change management of the tool and updates to the signatures/patterns for threat detection.	CC6.8, CC7.1
ProShred Security		
6.	The subservice organization should have controls in place to help ensure the secure destruction of sensitive documents, media, and other physical assets containing confidential information.	CC6.5

User Entity Responsibilities

User entities must perform specific activities in order to benefit from MedPro's services. These activities may affect each user entity's ability to effectively use MedPro's services but do not affect the ability of MedPro to achieve its service commitments and system requirements. These activities may be specified in agreements between user entities and MedPro, user manuals, and/or other communications. These activities are referred to as user entity responsibilities (UERs).

UERs are listed in the following table. They are the responsibility of the user entities of the System and are expected to be in operation at user entities to complement MedPro's controls. The list of UERs does not represent a comprehensive set of all the controls that should be employed by user entities. Other controls may be required at user entities.

Number	UER
1.	User entities must notify MedPro about their users of MedPro services in order for MedPro to add, modify, or remove user access for contracted services.

Number	UER
2.	User entities must identify the business rules, data fields, and methods of data delivery and receipt they will utilize so that they can be configured. Changes to business rules, data fields, and data delivery and receipt methods must be discussed in advance so they can be configured appropriately.
3.	User entities must determine and communicate to MedPro the data access and terms, conditions, and responsibilities, including security requirements, that each party is responsible for in the contract.

Attachment B — Principal Service Commitments and System Requirements

Attachment B — Principal Service Commitments and System Requirements

MedPro believes in transparency with employees, customers, and stakeholders when it comes to information privacy and security processes and protocols. MedPro institutes appropriate technical, administrative, and physical safeguards designed to protect information in its possession from loss, misuse, and unauthorized access, disclosure, alteration, and destruction. MedPro's employees are trained in the importance of data security. Security service commitments, including file transfer methods and restriction of access to customer data to customers are documented and communicated in the master services agreement (MSA) and associated contractual documents.