*

System and Organization Controls (SOC) 3 Report

Management's Report of Its Assertions on SYNERGEN Health LLC & SYNERGEN Health (Pvt) Ltd.'s Revenue Cycle Management (RCM) Services and Technology Solutions Based on the Trust Services Criteria for Security, Availability, and Confidentiality

For the Period November 1, 2022 to September 30, 2023

TABLE OF CONTENTS

SECTION ONE: REPORT OF INDEPENDENT ACCOUNTANTS

To: Management of SYNERGEN Health LLC & SYNERGEN Health (Pvt) Ltd.

Scope

We have examined management's assertion, contained within the accompanying "Management's Report of Its Assertions on the Effectiveness of Its Controls over SYNERGEN Health LLC & SYNERGEN Health (Pvt) Ltd.'s Revenue Cycle Management (RCM) Services and Technology Solutions Based on the Trust Services Criteria for Security, Availability, and Confidentiality" (Assertion) that SYNERGEN Health LLC & SYNERGEN Health (Pvt) Ltd.'s controls over the Revenue Cycle Management (RCM) Services and Technology Solutions (System) were effective throughout the period November 1, 2022 to September 30, 2023, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, 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*).

The Assertion also indicates that SYNERGEN Health LLC & SYNERGEN Health (Pvt) Ltd. 's ("Service Organization" or "SYNERGEN" or "SYNERGEN Health") controls can provide reasonable assurance that certain service commitments and system requirements can be achieved only if complementary user entity controls assumed in the design of SYNERGEN's infrastructure's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

SYNERGEN uses subservice organizations to supplement its services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at SYNERGEN to achieve SYNERGEN's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitable design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

SYNERGEN management is responsible for its assertion, selecting the trust services categories and associated criteria on which its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the Revenue Cycle Management (RCM) Services and Technology Solutions and describing the boundaries of the System;
- Identifying the principal service commitments and system requirements and the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of the System; and
- Identifying, designing, implementing, operating, and monitoring effective controls over the Revenue Cycle Management (RCM) Services and Technology Solutions (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the Assertion, based on our examination. 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. An examination involves performing procedures to obtain evidence about management's assertion, which includes:

- Obtaining an understanding of SYNERGEN's Revenue Cycle Management (RCM) Services and Technology Solutions relevant to Security, Availability, and Confidentiality policies, procedures, and controls;
- Testing and evaluating the operating effectiveness of the controls; and
- Performing such other procedures as we considered necessary in the circumstances.

The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence we obtained during our examination is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating SYNERGEN's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program. We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements related to our examination engagement.

Inherent Limitations

Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design and operating effectiveness of the controls to achieve SYNERGEN's Revenue Cycle Management (RCM) Services and Technology Solutions' principal service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the system or controls, or the failure to make needed changes to the system of controls, may alter the validity of such evaluations.

Opinion

In our opinion, management's assertion that the controls within SYNERGEN's Revenue Cycle Management (RCM) Services and Technology Solutions were effective throughout the period November 1, 2022 to September 30, 2023 to provide reasonable assurance that SYNERGEN's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

CyberGuard Compliance, LLP

November 10, 2023
Las Vegas, Nevada

SECTION TWO: MANAGEMENT'S REPORT OF ITS ASSERTIONS ON THE EFFECTIVENESS OF ITS CONTROLS OVER SYNERGEN HEALTH LLC & SYNERGEN HEALTH (PVT) LTD.'S REVENUE CYCLE MANAGEMENT (RCM) SERVICES AND TECHNOLOGY SOLUTIONS BASED ON THE TRUST SERVICES CRITERIA FOR SECURITY, AVAILABILITY, AND CONFIDENTIALITY

November 10, 2023

Scope

We, as management of SYNERGEN, are responsible for:

- Identifying the SYNERGEN's Revenue Cycle Management (RCM) Services and Technology Solutions (System) and describing the boundaries of the System, which are presented in the section below (Attachment A) titled SYNERGEN Health LLC & SYNERGEN Health (Pvt) Ltd.'s Description of the Revenue Cycle Management (RCM) Services and Technology Solutions (Description);
- Identifying our principal service commitments and system requirements (Attachment B);
- Identifying the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of our system, which are presented in the section below (Attachment B)
- Identifying, designing, implementing, operating, and monitoring effective controls over SYNERGEN's Revenue Cycle Management (RCM) Services and Technology Solutions (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirements; and
- Selecting the trust services categories that are the basis of our assertion.

In designing the controls over the System, we determined that certain trust services criteria can be met only if complementary user entity controls are suitably designed and operating effectively for the period November 1, 2022 to September 30, 2023.

SYNERGEN uses subservice organizations to supplement its services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at SYNERGEN, to achieve SYNERGEN's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system does not disclose the actual controls at the subservice organization.

We assert that the controls within the system were effective throughout the period November 1, 2022 to September 30, 2023, to provide reasonable assurance that the principal service commitments and system requirements were achieved based on the criteria relevant to Security, Availability, and Confidentiality set forth in the AICPA's TSP section 100, 2017 Trust Services Criteria for Security, Availability, Confidentiality, Processing Integrity, and Privacy, if subservice organizations and user entities applied the complementary controls assumed in the design of SYNERGEN's Revenue Cycle Management (RCM) Services and Technology Solutions controls throughout the period November 1, 2022 to September 30, 2023.

SYNERGEN Health LLC & SYNERGEN Health (Pvt) Ltd.

ATTACHMENT A: SYNERGEN HEALTH LLC & SYNERGEN HEALTH (PVT) LTD.'S DESCRIPTION OF THE REVENUE CYCLE MANAGEMENT (RCM) SERVICES AND TECHNOLOGY SOLUTIONS

System Overview

The System is comprised of the following components:

- ***Infrastructure*** **-** The physical and hardware components of a system (facilities, equipment, and networks)
- ***Software*** **-** The programs and operating software of a system (systems, applications, and utilities)
- ***Data*** **-** The information used and supported by a system (transaction streams, files, databases, and tables)
- ***People*** **-** The personnel involved in the operation and use of a system (developers, operators, users, and managers)
- ***Procedures*** **-** The automated and manual procedures involved in the operation of a system.

Infrastructure

The operations and corporate facilities are located in Location 1: 249, Stanley Thilakarathne Mawatha, Nugegoda, Sri Lanka, Location 2: 2nd**,** 3rd, 4th, 5th Floor, 209 Wijayaba Mawatha, Nawala Road, Nugegoda, Sri Lanka and the headquarters/corporate office in 2626 Cole Avenue, Suite 429, Dallas, Texas 75204. SYNERGEN Health utilizes a combination local area network ("LAN") and wide area network ("WAN") to share data among its employees. The Virtual Data Center is hosted in Amazon Web Services (AWS) US regions and managed by the IT team located in Sri Lankan Operations Centers. The Virtual Data Center is remotely accessible 24 hours a day, 7 days a week, and 365 days a year to authorized SYNERGEN Health personnel. SYNERGEN Health uses internal IT expertise and follows internal business and IT policies and procedures to support its daily IT administration and service operation.

The SYNERGEN Health's Systems are hosted in Amazon Web Services (AWS) across multiple Availability Zones for redundancy and disaster recovery purposes. SYNERGEN Health does not own or maintain any hardware in the AWS data centers. Services operate within a shared security responsibility model, where AWS is responsible for the security of the underlying cloud infrastructure, and SYNERGEN Health is responsible for securing the SYNERGEN Health's Systems that are deployed in AWS (e.g., IAM, S3 bucket policies, Operating System and application security, Security Group configuration, network traffic monitoring).

Three Virtual Private Clouds (VPC) separate the containerized production, staging, and development environments. Access to AWS production instances is allowed only through an encrypted VPN from SYNERGEN Health's corporate network to ensure the privacy and integrity of data transmitted over the public network. VPN connections are whitelisted to

SYNERGEN Health's IPs and are secured using AES-128 bit or greater encryption. Access is restricted to authorized administrators, who must authenticate via a bastion host through a secure SSH key, AWS IAM roles, and multi-factor authentication.

Production instances at AWS are logically and physically separate from SYNERGEN Health's internal corporate network. All container hosts and database servers run on EC2 instances within Auto Scaling groups. AWS CloudFormation provides auto-scaling management of the production systems based on a defined template, which allows Integrate to deploy and configure consistently hardened instances.

All container hosts and database servers run on EC2 instances that are secured via Security Groups. Security Groups monitor incoming network traffic by analyzing data packets and filtering traffic based on an Integrate-defined ruleset. Access to manage the Security Groups is restricted to authorized DevOps personnel, and changes to these rulesets are governed by SYNERGEN Health's change management policy, which includes documenting, testing, and approving the change.

SYNERGEN Health Software Solutions
The users facing SYNERGEN Health Software Solutions are predominantly front-end applications for customers to access their services/channel. These applications' content is hosted and run within S3 via the Amazon CloudFront Content Delivery Network (CDN) to provide greater security and increased performance.

Software
SYNERGEN Health Software Solutions run in a containerized environment with Ubuntu Linux as the base image based on a generic Amazon Machine Images (AMI). Monthly, the continuous integration platform runs an automated process to update the image. A configuration management tool is used to configure software applications on individual instances using approved scripts.

SYNERGEN Health uses multiple software and utilities to configure, develop, and support the in-scope infrastructure and applications.

Data
Inbound integrations to the SYNERGEN Health Software Solutions are configured with third parties via SYNERGEN Health Company-developed APIs. Additionally, Clients transfer data to SYNERGEN Health via secure file transfer protocols and/or manual upload via the front-end application.

SYNERGEN Health validates, stores, and processes contact data within the SYNERGEN Health Software Solutions. Data is stored on database servers running on various Database Systems within the production VPC. All data is encrypted at rest, and SSL encrypts data in transit between the container and databases. Data is also encrypted between SYNERGEN Health and

clients' systems, which are interfaced to SYNERGEN Software Solutions as applicable for data processing.

Processed data is provided to customers in various ways:

- Customers can access the processed data via relevant SYNERGEN Health Software Solution.
- Reports of processed data can be accessed by customers using privileged accounts in relevant SYNERGEN Health Software Solution.
- Outbound integrations via APIs send processed data to client's systems.

People

The following functional roles/teams comprise the framework to support effective controls over governance, management, security, and operation:

- *The Board of Directors* establishes business and strategic objectives to meet the interests of stakeholders, and provides oversight of all aspects of the business, including financial and operational performance of the Company. The Board of Directors meets with the members of the executive management team on a regular basis to stay fully informed of all business and operational issues as they arise. The Board of Directors meets on a quarterly basis (or more frequently if required), and all meetings are documented in board minutes. The Board operates in accordance with the written guidelines and roles and responsibilities as set forth in the Company's operating documents (the Company Agreement).
- *The Management Team* conducts regular operational and third-party assessment of the business and presents and discusses the results and findings with the Board of Directors.
- *Executive Management* oversees, and is ultimately responsible for, all aspects of service delivery and security commitments. Among other responsibilities, Executive Management ensures that controls are enforced, risk assessment/management activities are approved and prioritized, people are appropriately trained, and systems and processes are in place to meet security and service requirements.
- *Human Resources* is responsible for managing all functions related to recruiting and hiring, employee relations, performance management, training, and resource management. Human Resources partners proactively with Executive Management and business units to ensure that all initiatives are appropriately aligned with SYNERGEN Health Company's mission, vision, and values.
- *Information Technology (IT)* management has overall responsibility and accountability for the enterprise computing environment.
- *Solutions Support Team and* DevOps personnel administer systems and perform services supporting key business processes, including architecting, and maintaining secure and adequate infrastructure, monitoring network traffic, and deploying approved changes to production. The Solutions Support Team is responsible for help

desk tickets based on customer requests and communicating with customers regarding any issues or outages as well.

- *Solutions Development Team* is responsible for application development, initial testing of changes, and troubleshooting/resolving application issues.
- *Information Security* is responsible for performing assessing and managing risk, defining control objectives, monitoring performance of security controls, addressing and responding to security incidents, maintaining, and communicating updates to security policies, and conducting security awareness training of all users.
- *Client Account Managers / Onboarding Managers* are responsible for initiating the request for creation of new customer instances on SYNERGEN Health Software Solutions based on at what stage a particulate solution is provided to the client.
- *Solutions Product Owners* are responsible for providing user documentation / Product Demos and coordinating training for new customers, and overall management of the account to ensure continued customer satisfaction.

SYNERGEN Health is committed to equal opportunity of employment, and all employment decisions are based on merit, qualifications, and abilities. Employment-related decisions are not influenced or affected by an employee's race, color, nationality, religion, sex, marital status, family status, sexual orientation, disability, or age. SYNERGEN Health endorses a work environment free from discrimination, harassment, and sexual harassment.

Procedures

SYNERGEN Health has an Information Security Officer / Data Protection and Privacy Officer who is responsible for the design and oversight of security and privacy initiatives. The Information Security Officer / Data Protection and Privacy Officer reports directly to the Leadership/Managing Partners and Managing Director (MD). The IT policy framework describes the procedures followed to ensure the performance of consistent processes over the security, availability, confidentiality, and operation of the SYNERGEN Health's Infrastructure Facilities and Systems that facilitate Revenue Cycle Management Services and Technology Solutions that are provided by the organization. All IT policies are reviewed on an annual basis, or more frequently as needed, by the Information Security Officer / Data Protection and Privacy Officer.

All employees are expected to adhere to SYNERGEN Health's IT policy framework as acknowledged during new hire onboarding and during annual security awareness training. The IT policy framework includes procedures that provide guidance on the consistent performance of controls and processes necessary to meet service commitments and system requirements.

Incident Disclosure

No security incidents were detected or reported during the audit period that would affect SYNERGEN Health's service commitments or system requirements.

Complementary Subservice Organization Controls

Certain principal service commitments and system requirements can be met only if complementary subservice organization controls (CSOC) assumed in the design of SYNERGEN's controls are suitably designed and operating effectively at the subservice organizations, along with related controls at SYNERGEN.

Description of Complementary User Entity Controls

SYNERGEN controls were designed with the assumption that certain controls would be implemented by user entities (or "customers"). Certain requirements can be met only if complementary user entity controls assumed in the design of SYNERGEN's controls are suitably designed and operate effectively, along with related controls at SYNERGEN.

ATTACHMENT B: PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Company Background

Founded in 2011, SYNERGEN Health provides transformational revenue cycle solutions and services using innovative Analytics, Artificial Intelligence/Machine Learning, and Robotic Process Automation to Digitize Healthcare.

SYNERGEN Health utilizes technology, analytics, and deep domain expertise to help their clients collect the revenue due in a compliant and efficient manner, from government and commercial insurance companies and from patients, for the services they have rendered. They have refined and elevated what many refer to as revenue cycle management to be reimagined and achieved as "technology and data-driven revenue cycle transformation."

They utilize their innovation and excellence to drive significant value, efficiency and cost savings to their clients, patients, and the entire healthcare system. Their solutions and services are being utilized in over 45 States in the USA.

Description of Services Provided

SYNERGEN Health provides following products and services:

- **Revenue Management Cycle Services**: This includes but not limited to Verification of Benefits, Coding, Claims Submissions, Denials Management, Collections and Appeals, Payment Posting and Reconciliation, and Patient Billing using streamlined and organized processes, tools, and techniques. Automation of processes and activities where possible drives the efficiency in delivering these services.
- **SYNERGEN Software Solutions**: Transformation of the revenue cycle starts with analyzing, optimizing and automating routine business processes. SYNERGEN Health's technology solutions are built to address challenges across the entire revenue cycle process from patient access to final account resolution powered by process automation, machine learning, and artificial intelligence. An array of products that drive efficiency of Revenue Cycle Management processes and used as standalone products by customers include the following:
    - **Collection and Denial Management System (CDMS)**: SYNERGEN Health's CDMS is an intelligent central automation hub that provides predictive nuances using machine learning to revolutionize the collection and denial management process. Suggestive follow up fixes, claim queue prioritization, powerful rules engine, dynamic workflow queues, and integrated knowledge management are just a few of the tools available in this unique solution.
    - **Revenue Cycle Management Automation (RCMA)** [this consists of an array of automation tools]: SYNERGEN Health's revenue cycle automation solutions can execute repetitive manual processes, saving hundreds of hours of manpower,

eliminating countless data entry mistakes. Even more, SYNERGEN's digital workforce tools "learn" on the fly the most efficient and effective way to achieve the desired outcome, thereby continually improving toward the organization's goals.

- **SYNERGEN Pay**: SYNERGEN Pay is a secure, simple-to-use, patient statement delivery and online portal that streamlines patient collections from pre-visit scheduling to post-visit follow up. SYNERGEN Pay empowers health care organizations with the flexibility to accept payments at any time, from anywhere, all while providing multiple payment channels to patients.
- **SYNERGEN Client Bill**: SYNERGEN Client Bill is an innovative solution that simplifies the complexities of Business to Business (B2B) Billing into a manageable and fluid process. SYNERGEN Client Bill helps to boost staff's ability to transact efficiently and influence timely payments.
- **SYNERGEN Connect**: Secure Communication Platform for collaborating with Central Billing Office (CBO), referring providers and outsourced vendors.
- **SYNERGEN Billing Data Entry (BDE)**: Application with the view of documents to assist the team in capturing missing information from HL7 and other sources. It automates the process by capturing the required data through pre-defined rules and configurations to eliminate the manual work.
- **SYNERGEN Billing Interface**: SYNERGEN Billing Interface automates the charge entry process by utilizing the benefits of the messaging standard HL7 or.csv and retrieving the patient demographic, insurance, guarantor, referring physician, diagnosis, financial order, or result details at the point a claim is considered ready to bill.
- **SYNERGEN Coding Automation:** Automated coding using a rule-based engine to maintain the right level of coding and maintaining compliance. It eliminates the need for manual coding and improves accuracy to reduce denials.
- **Analytics Solution**: DOCTRIX® is a cloud-based analytics solution that simplifies complex healthcare revenue cycle financial data with user-friendly dashboards, making information easy to review, evaluate and share in real-time.

- **Credentialing & Enrollment Services**: Credentialing is the process of reviewing a health professional's credentials to determine if privileges to practice can be granted. Enrollment is the process of enrolling a health professional in contracts required by payors for reimbursement for medical services and/or products provided. Both credentialing and enrollment activities are critical to an organization's financial performance. SYNERGEN Health eases the burden of credentialing by using integrated credentialing software and experienced credentialing team members. Years of credentialing experience in the medical field allow SYNERGEN Health to streamline the paperwork and eliminate any errors that can keep organizations/individuals from getting properly credentialed and contracted with payors and medical facilities, while also providing visibility to the credentialing and enrolling statuses through reports and dashboards.

Principal Service Commitments and System Requirements

SYNERGEN Health's security, availability, and confidentiality commitments to customers are documented and communicated to customers in the Master Services Agreement and the description of services published on the customer-facing website www.synergenhealth.com. The principal security, availability, and confidentiality commitments, and the HITRUST CSF security controls include, but are not limited to:

- Maintain appropriate administrative, physical, and technical safeguards to protect the security and integrity of SYNERGEN Health's Infrastructure Facilities, Systems, and the customer data in accordance with SYNERGEN Health's security requirements.
- Perform annual third-party security and compliance audits of the environment, including, but not limited to:
  - Reporting on Controls at a Service Organization Relevant to Security, Availability, Confidentiality, Processing Integrity, or Privacy (SOC 2) examinations.
  - International Organization for Standardization (ISO) 27001:2013 certification reviews.
- Use formal HR processes, including background checks, code of conduct and company policy acknowledgements, security awareness training, disciplinary processes, and annual performance reviews.
- Follow formal access management procedures for the request, approval, provisioning, review, and revocation of SYNERGEN Health personnel with access to any production systems.
- Prevent malware from being introduced to production systems.
- Continuously monitor the production environment for vulnerabilities and malicious traffic.
- Use industry-standard secure encryption methods to protect customer data at rest and in transit.
- Transmit unique login credentials and customer data via encrypted connections.
- Maintain an availability SLA for customers as per the applicable service/product contracts-based uptime for each calendar quarter.
- Maintain a business continuity plan with disaster recovery features to ensure availability of information following an interruption or failure of critical business processes.
- Maintain and adhere to a formal incident management process, including security incident escalation procedures.
- Maintain confidentiality of customer data and notify customers in the event of a data breach.
- Identify, classify, and properly dispose of confidential data when retention period is reached and/or upon notification of customer account cancellation.

SYNERGEN Health establishes system and operational requirements that support the achievement of the principal service commitments, applicable laws and regulations, and

other system requirements. These requirements are communicated in SYNERGEN Health's policies and procedures, system design documentation, and/or in customer contracts. Information Security policies define how systems and data are protected. These policies are updated as appropriate based on evolving technologies, changes to the security threat landscape, and changes to industry standards, provided any updates do not materially reduce the service commitments or overall service provided to customers as described in the customer contracts.

SYNERGEN Health regularly reviews the security, availability, and confidentiality commitments HITRUST CSF Requirements, and performance metrics to ensure these commitments are met. If material changes occur that reduce the level of security, availability, and confidentiality commitments or HITRUST CSF Requirements within the agreement, SYNERGEN Health will notify the customer directly via email.