REPORT ON

MEDICAL CLAIMS ASSISTANCE INC.'S

DESCRIPTION OF ITS MEDICAL BILLING SYSTEM AND ON THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF ITS CONTROLS

AUGUST 1, 2020 TO JULY 31, 2021

MARCUM
ACCOUNTANTS ▲ ADVISORS

MCA – SOC 1 TYPE II TABLE OF CONTENTS

Acronym Table

- ACL — Access Control List
- AD — Active Directory
- AICPA — American Institute of Certified Public Accountants
- CIO — Chief Information Officer
- CO — Company
- DNS — Domain Name System
- EFT — Electronic Funds Transfer
- EMS — Emergency Medical Services
- EPCR — Electronic Patient Care Record
- ESO — ESO Billing Software
- HCFA — Health Care Finance Administration
- HIPAA — Health Insurance Portability and Accountability Act
- HR — Human Resources
- ID — Identification
- IDS — Intrusion Detection System
- IP — Internet Protocol
- IPS — Intrusion Prevention System
- IT — Information Technology
- MCA — Medical Claims Assistance, Inc.
- NAT — Network Address Translation
- OS — Operating System
- PCS — Physician Certification Statement
- SaaS — Software as a Service
- SFTP — Secure Shell File Transfer Protocol
- SOC — System and Organization Controls
- SSL — Secure Socket Layer
- TLS — Transfer Layer Security
- UAT — User Acceptance Testing
- UPS — Uninterruptable Power Supply
- VP — Vice President
- VPN — Virtual Private Network
- WV — West Virginia

Section 1: Assertion of MCA Management

Assertion of MCA Management

We have prepared the description of MCA's Medical Billing System entitled "MCA's Description of its Medical Billing System" for processing user entities' transactions throughout the period August 1, 2020 to July 31, 2021 (description) for user entities of the system during some or all of the period August 1, 2020 to July 31, 2021, and their auditors who audit and report on such user entities' financial statements or internal control over financial statement reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by subservice organizations and user entities of the system themselves, when assessing the risks of material misstatement of user entities' financial statements.

MCA uses subservice organizations to perform backup colocation services, IT managed services, medical billing software development, and clearinghouse services. The description includes only the control objectives and related controls of MCA and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified in the description can be achieved only if complementary subservice organization controls assumed in the design of our controls are suitably designed and operating effectively, along with the related controls. The description does not extend to controls of the subservice organizations.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls, assumed in the design of MCA's controls, are suitably designed and operating effectively along with related controls at the service organization. The description does not extend to controls of the user entities.

We confirm, to the best of our knowledge and belief, that:

1. The description fairly presents the Medical Billing System made available to user entities of the system during some or all of the period August 1, 2020 to July 31, 2021 for processing user entities' transactions as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description:
    a. Presents how the system made available to user entities of the system was designed and implemented to process relevant user entity transactions, including, if applicable:
        i. The types of services provided, including, as appropriate, the classes of transactions processed.
        ii. The procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the system.
        iii. The information used in the performance of the procedures including, if applicable, related accounting records, whether electronic or manual, and

supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.

iv. How the system captures and addresses significant events and conditions other than transactions.

v. The process used to prepare reports and other information for user entities.

vi. The services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them.

vii. The specified control objectives and controls designed to achieve those objectives including, as applicable, complementary user entity controls and complementary subservice organization controls assumed in the design of the controls

viii. Other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.

b. Includes relevant details of changes to the Medical Billing System during the period covered by the description.

c. Does not omit or distort information relevant to the system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors and may not, therefore, include every aspect of the Medical Billing System that each individual user entity of the system and its auditor may consider important in its own particular environment.

2. The controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period August 1, 2020 to July 31, 2021 to achieve those control objectives if subservice organizations and user entities applied the complementary controls assumed in the design of MCA's controls throughout the period August 1, 2020 to July 31, 2021. The criteria we used in making this assertion were that:

a. The risks that threaten the achievement of the control objectives stated in the description have been identified by management.

b. The controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved.

c. The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority

/s/ Kendra Black, VP
Medical Claims Assistance, Inc.
November 5th, 2021

Section 2: Independent Service Auditors' Report

Independent Service Auditors' Report

To: Medical Claims Assistance, Inc.

Scope

We have examined MCA's description of its Medical Billing System entitled "MCA's Description of its Medical Billing System" for processing user entities' transactions throughout the period August 1, 2020 to July 31, 2021, (description) and the suitability of the design and operating effectiveness of controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in the "Assertion of MCA Management" (assertion). The controls and control objectives included in the description are those that the management of MCA believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the Medical Billing System that are not likely to be relevant to user entities' internal control over financial reporting.

The information in Section 5, "Other Information Provided by MCA" is presented by management of MCA to provide additional information and is not a part of MCA's description of its Medical Billing System made available to user entities during the period August 1, 2020 to July 31, 2021. Information about MCA's responses to testing exceptions has not been subjected to the procedures applied in the examination of the description of the Medical Billing System and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description of the Medical Billing System and, accordingly, we express no opinion on it.

MCA uses subservice organizations to perform backup colocation services, IT managed services, medical billing software development, and clearinghouse services. The description includes only the control objectives and related controls of MCA and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified by MCA can be achieved only if complementary subservice organization controls assumed in the design of MCA's controls are suitably designed and operating effectively, along with the related controls at MCA. Our examination did not extend to controls of the subservice organizations and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls contemplated in the design of MCA'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.

Service Organization's Responsibilities

In Section 1, MCA has provided an assertion about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. MCA is responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and the assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

Service Auditors' Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination.

Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period August 1, 2020 to July 31, 2021. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves:

- Performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on the criteria in management's assertion.
- Assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description.
- Testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved.
- Evaluating the overall presentation of the description, suitability of the control objectives stated in the description, and suitability of the criteria specified by the service organization in its assertion.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become ineffective.

Description of Tests of Controls

The specific controls tested, and the nature, timing, and results of those tests are listed in Section 4.

Opinion

In our opinion, in all material respects, based on the criteria described in MCA's assertion:

a. The description fairly presents the Medical Billing System that was designed and implemented throughout the period August 1, 2020 to July 31, 2021.
b. The controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period August 1, 2020 to July 31, 2021 and the subservice organizations and user entities applied the complementary controls assumed in the design of MCA's controls throughout the period August 1, 2020 to July 31, 2021.
c. The controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period August 1, 2020 to July 31, 2021, if complementary subservice organization and user entity controls assumed in the design of MCA's controls operated effectively throughout the period August 1, 2020 to July 31, 2021.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of MCA, user entities of MCA's Medical Billing System during some or all of the period August 1, 2020 to July 31, 2021, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the

risks of material misstatement of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

Marcum LLP

November 5th, 2021
Tampa, Florida

Section 3: MCA's Description of its Medical Billing System

Purpose and Scope of Report

This report on the internal controls placed in operations is intended to provide interested parties with sufficient information to obtain an understanding of those aspects of MCA's controls that may be relevant to MCA's clients' internal control structure. This report, when combined with an understanding of the policies and procedures at user organizations, is intended to assist user auditors in planning the audit of the user organization and in assessing control risk for assertions of the user organizations' financial statements that may be affected by policies and procedures of MCA's Medical Billing System.

This report describes the system and control structure of MCA as it relates to their Medical Billing System. It is intended to assist MCA's customers and their independent auditors in determining the adequacy of the internal controls of services that are outsourced to MCA and are relevant to user organizations' internal control structures as it relates to financial reporting risks.

This description is intended to focus on the internal control structure of MCA that is relevant to its Medical Billing System and does not encompass all aspects of the services provided or procedures followed by MCA.

Company Overview and Services Provided

MCA was established in 1986 in Huntington, WV to provide billing services for the use of the participating emergency ambulance services. Operations are still located in Huntington, WV, but the customer base has expanded to over 170 customers located in eight states.

MCA provides medical billing services to its customers, also known as providers or EMS first responders, in a streamlined and mostly automated system. MCA is responsible for receiving the run reports from the ambulance personnel, entering it to the Medical Billing System, following up on open balances for services provided by MCA's customers, receiving and recording record of payment, and forwarding payments to the providers. MCA follows-up on open balances and help providers receive payment for the services they have provided.

Subservice Organizations

The company utilizes subservice organizations to perform certain functions to improve operating and administrative effectiveness. MCA performs annual reviews of the subservice organizations' systems to help ensure the security and processing commitments of the subservice organizations are being met. The reviews include obtaining attestation reports or other related evidence. The following subservice organizations are utilized to assist in the delivery of the Medical Billing

System:

- Advantage Technology – data backup colocation services
- ESO – Medical Billing SaaS
- ZirMed – Clearinghouse services

Advantage Technology

MCA uses Advantage Technology to perform colocation of backup services and other managed IT services. Advantage Technology is responsible for the uptime and management of the infrastructure that supports the delivery of managed backups that are utilized to support the Medical Billing System. Advantage Technology is also responsible for restricting logical and physical access to backup media and for encrypting the backups according to MCA's requested protocols. Advantage Technology performs an annual external vulnerability scan on the productions systems.

The applicable controls relating to the control objectives that are intended to be met by Advantage Technology, alone or in combination with controls at MCA, and the types of controls expected to be implemented at Advantage Technology to meet those controls are described in the table below.

Control Activities Expected to be Implemented by Advantage Technology	Applicable Control Objective
Advantage Technology is responsible for restricting physical access of backup media to authorized MCA personnel.	Physical Security
Advantage Technology is responsible for the provisioning of MCA workstations and servers.	Computer Operations (Backup and Storage)
Advantage Technology is responsible for restricting logical access of backup media to authorized MCA personnel.	Computer Operations (Backup and Storage)
Advantage Technology is responsible for the encryption and logical security of MCA backup media.	Computer Operations (Backup and Storage)
Advantage Technology is responsible for the completion of an annual external vulnerability scan and the confidentiality of the results.	Data Communications

ESO

MCA uses ESO to provide the medical billing Software. ESO is responsible for updating the application and providing a new application version with any changes requested by ESO clients.

The applicable controls relating to the control objectives that are intended to be met by ESO, alone or in combination with controls at MCA, and the types of controls expected to be implemented at ESO to meet those controls are described in the table below.

Control Activities Expected to be Implemented by ESO	Applicable Control Objective
ESO is responsible for developing, testing, and implementing changes to the medical billing software.	Application Change
ESO is responsible for implementing changes to the Medical Billing System requested by MCA.	Application Change

ZirMed

MCA uses ZirMed to perform clearinghouse services. ZirMed is responsible for the uptime and management of the infrastructure that supports the delivery of clearinghouse services that are utilized to support the Medical Billing System. ZirMed is also responsible for maintaining logical separation of virtual environments from other ZirMed clients. Zirmed is responsible for the secure transmission of client claims and payments. Finally, ZirMed is responsible for processing payments completely, accurately, and timely according to the agreements in place with MCA.

The applicable controls relating to the control objectives that are intended to be met by ZirMed, alone or in combination with controls at MCA, and the types of controls expected to be implemented at ZirMed to meet those controls are described in the table below.

Control Activities and Related Control Objectives Expected to be Implemented by ZirMed	Applicable Control Objective
ZirMed is responsible for maintaining logical segregation of virtualized environments from other ZirMed clients.	Information Security
ZirMed is responsible for maintaining availability of Internet and power services, as well as preventative maintenance of cooling and power equipment.	Computer Operations (Systems Availability)
ZirMed is responsible for processing payments completely, accurately, and timely.	Payment Processing

Significant Changes Throughout the Examination Period

There were no significant changes that occurred throughout the examination period.

System Description

Control Environment

Control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline, and structure. Below are the key areas and the description of controls that support MCA's control environment

Integrity and Ethical Values

The effectiveness of controls is greatly influenced by the level of integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are important elements of MCA's control environment, affecting the design, administration, and monitoring of other components. The communication and implementation of ethical behavior throughout the organization is designed to reduce the likelihood of personnel to engage in dishonest, illegal, or unethical acts.

MCA enforces high ethical standards in all levels of communication to and through its employees and continuously audits employees' communication with customers and outside resources, ensuring compliance with company standards and addresses any issues as they arise. MCA emphasizes high standards during interpersonal communications via meetings, email, and phone calls. Any questionable acts are addressed, and positive acts are recognized and acknowledged in public forums in an effort to reinforce positive/constructive behaviors. Employees who violate these standards are disciplined according to company policies. MCA requires that employees sign an acknowledgement form indicating that they have access to, read, and understand their responsibility for adhering to the policies and procedures outlined in the employee handbook. Each employee is also required to read and sign an employee agreement that includes acknowledgement of the policies and procedures.

Commitment to Competence

Management has established a framework for the basic skills necessary to perform each of the jobs at MCA. This framework is then augmented with more specific requirements for each position and for additional specialization within each position based on any other skills an employee may have. The job descriptions for each position are descriptive but remain fairly broad due to the nature of the work for which each position is responsible. Employees understand that there are general skills that individuals within their given role must have and that the job description augments those skills.

Management's Philosophy and Operating Style

Management's philosophy and operating style encompasses a broad range of characteristics that may include management's approach to taking and monitoring business risk and management's attitude and actions for the security and confidentiality of information. Management has documented policies and standard operating procedures for specific information processing and accounting functions and personnel are expected to adhere to these procedures to help ensure the proper operation of the control environment. MCA's management takes a relatively conservative approach to information processing and risk associated with new business ventures.

Organizational Structure

Management has designed the organizational structure to provide quality service and accountability in support of MCA's mission. In order to achieve quality in performance, they strive for continuous improvement in all areas of the business by planning and committing to

accomplishing targets and empowering employees to perform their duties. MCA's operations are highly specialized and require the ability to adapt to industry changes and best practices. MCA has a centralized, flat management framework which allows them to quickly react to industry changes and provide excellent response times to customer needs. In addition, the President, VP, and Director of Administration are active participants in day-to-day operations and supervisors report directly to the executive group. Organizational charts are in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel. These charts are available to personnel via the shared drive.

Human Resource Policies and Practices

MCA's HR policies and practices including hiring, training, disciplinary actions, and termination procedures are clearly written and communicated where appropriate and are listed in the employee handbook. MCA has implemented these policies and procedures to screen candidates prior to making offers of employment and perform necessary actions in the event of an employee termination.

Risk Assessment

MCA's management performs periodic risk assessments that require the identification of risks in its areas of responsibility and to implement appropriate measures to address those risks. MCA's management formally reevaluates risk annually to both update previous assessments and to identify any new potential areas of concern.

The risk assessment process consists of the following phases:

- Identifying – The identification phase includes listing out risks (including threats and vulnerabilities) that exist in the environment. This phase provides a basis for all other risk management activities.
- Assessing – The assessment phase considers the potential impact(s) of identified risks to the service organization and their likelihood of occurrence.
- Mitigating – The mitigation phase includes enacting controls, processes, and other physical and virtual safeguards in place to prevent and detect both identified and assessed risks.
- Reporting – The reporting phase results in risk reports provided to managers with the necessary data to make effective business decisions and to comply with internal policies and any applicable regulations.
- Monitoring – The monitoring phase includes the performance of monitoring activities by MCA's management team to evaluate whether the processes, initiatives, functions, and/or activities are mitigating the risk as designed.

Information and Communication

Information

Information is necessary for MCA to carry out internal control responsibilities to support the achievement of its objective related to the MCA's Medical Billing System. Management obtains

or generates and uses relevant and quality information from both internal and external sources to support the functioning of internal control including but not limited to the following:

- Application change requests are documented and reviewed by IT personnel prior to initiating a change request.
- A help desk ticketing system is used to track and respond to report incidents.
- External monitoring is completed via the third party vendor monitoring application and alerts are configured to be sent to appropriate computer operations personnel.
- The backup system is configured to notify computer operations personnel of failed backups.
- An environmental monitoring system is in place and configured to notify IT personnel if environmental condition thresholds being met.
- External vulnerability scans are performed annually and reports are reviewed for any system vulnerabilities noted.
- A log of paper runs received and runs processed is maintained on a daily basis.
- Collection reports are published to MCA's secure website for each provider group to help aid provider groups in their reconciliation.

Communication

Management is involved with day-to-day operations and is able to provide personnel with an understanding of their individual roles and responsibilities. This includes the ability to provide necessary training so that personnel understand how their daily activities and roles relate to the overall support of services. MCA's management believes that open communication throughout the organization ensures that deviations from standards are identified, reported, and appropriately addressed.

Monitoring

Monitoring is the process of assessing risks linked to achieving operation objectives. This requires establishing a monitoring program consisting of procedures for evaluating risks to MCA's customers. Monitoring activities include monitoring of employee behavior, assessment of control activities, and reporting the results of assessments and any required corrective measures.

MCA has established a monitoring program performed through active, hands-on management including weekly and monthly reconciliations of transactions and monitoring of employee behavior. MCA utilizes a risk-based approach to monitoring business units by prioritizing and addressing risks in order of significance and potential impact. Management documents the results of risk assessments and provides them to management for review.

Control Objectives and Related Controls

Physical Security

Control Objective 1: Control activities provide reasonable assurance that physical access to the business premises and information systems is limited to properly authorized individuals.

MCA prevents unauthorized physical access to user organization systems by implementing a number of physical security controls including locked doors and restricting access to and within the facilities. An electronic door access system and security alarms are utilized to monitor access 24/7 and only authorized personnel have access to alarm codes. MCA limits access to the facility to personnel and approved designated vendors. Visitors are required to sign in, wear a visitor badge, and must be escorted at all times during visit. The visitor sign-in sheet records date, name, company, purpose for visit, as well as time-in and time-out.

IT management restricts access to the server rack located at the office in Huntington, WV. Keys to MCA's server rack are tightly controlled, inventoried annually, and collected upon termination.

Environmental Security

Control Objective 2: Control activities provide reasonable assurance that critical IT infrastructure is protected from certain environmental threats.

MCA contracts with a third party provider to monitor environmental conditions for their corporate facility including smoke and fire detection throughout and hand-held fire extinguishers are present in several locations for emergency use.

Critical IT infrastructure, including servers and network equipment, are housed in raised racks to help prevent potential damage from local flooding. The server rack includes a UPS unit to provide power to critical infrastructure equipment in the event of temporary power outage. The unit is tested on a bi-weekly basis to monitor for availability and reliability of power supplies.

Computer Operations (Backups and Storage)

Control Objective 3: Control activities provide reasonable assurance that system data is regularly backed up and available for restoration in the event of processing errors or unexpected interruptions.

Management has formally documented backup, storage, and restoration procedures to define the organizational backup and restoration strategy to help prevent data loss. To achieve the objectives defined in the backup and retention policy, MCA utilizes an automated backup system to schedule and perform daily incremental and weekly full backups of production application data. The backup system is configured to send notifications to IT personnel in the event of a failed backup. Physical and logical access to the backups is restricted to authorized IT personnel. Backups are scheduled, monitored, and transmitted over a secured point-to-point connection to an offsite colocation center.

Computer Operations (Systems Availability)

Control Objective 4: Control activities provide reasonable assurance that production systems are designed, maintained, and monitored to help ensure system availability.

Information systems are deployed in MCA's production application network located at the corporate facility and are formally documented in a data recovery plan. The Advantage Technology colocation data center houses the backup systems and is responsible for maintaining

power and connectivity redundancies that are monitored and maintained through the use of enterprise monitoring systems.

MCA monitors application level accessibility through Advantage Technology's system to help ensure services are available. Alerts are generated and sent to computer operations personnel via e-mail when server conditions reach predetermined thresholds or suspicious activity is detected. Production servers and workstations are equipped with antivirus software to detect the transmission of data or files that contain virus signatures and is configured to update virus signatures as they become available from the vendor, and continuously scans servers and workstations for threats.

MCA has incident response procedures in place to assist IT personnel in the resolution process. Computer operations personnel are responsible for managing internal requests to support their internal IT software services. Incidents are tracked through a ticketing process used to manage and monitor incident status and resolution.

Application Change Control

Control Objective 5: Control activities provide reasonable assurance that requests for application changes are initiated by authorized individuals and that changes are authorized prior to production migration.

MCA utilizes ESO's application to administer its Medical Billing System and is responsible for initiating the change requests and authorizing the changes to be implemented. ESO is responsible for the development, testing, and implementation of application updates.

Information Security

Control Objective 6: Control activities provide reasonable assurance that logical access to critical systems and data is restricted to authorized individuals.

MCA's information security is governed by their documented corporate information security policies and procedures. Logical access to IT resources including network, server operating system, application, and database systems is authenticated using Windows AD and is provisioned using the principle of least privilege allowing users only the minimum necessary access to resources to perform their job responsibilities. Through the use of Windows Active Directory and by defining and assigning roles in applications throughout the environment, MCA reduces the likelihood of inappropriate or unauthorized access as a result of individual/unique access permissions. Account username and password settings adhere to the group policy settings set forth by management.

Data Communications

Control Objective 7: Control activities provide reasonable assurance that data maintains its integrity and security as it is transmitted between third parties and MCA.

IT management implements various security controls to help ensure that data within the boundaries of the system and data transmitted to and from its network is protected from unauthorized access. MCA restricts access to the corporate and production networks using stateful inspection firewalls, alongside NAT, configured to deny all inbound traffic from the public internet by default and to allow the ingress of only specific services on specific ports.

An annual external vulnerability scan is performed by Advantage Technology on the production systems to detect potential vulnerabilities. Web sessions are encrypted using TLS protocol to help ensure the privacy and integrity of sessions.

Remote access to the corporate network requires a secure connection through the SonicWall VPN. MCA's clients securely transfer confidential data through SFTP.

Runs Received

Control Objective 8: Control activities provide reasonable assurance that runs received are properly identified, verified, and made available to the assigned insurance verification staff timely and accurately.

Run reports are documents that detail the services provided to a patient while being transported within an ambulance. The run reports include patient information, insurance information, and ride details such as mileage and medicine/services administered. These reports are received by MCA in one of two ways: paper via the mail or electronically.

Runs reports received in the mail are sorted by the mailroom attendant. The mailroom attendant counts and records the number of paper runs received in the log, scans the paper runs, and saves them on a shared drive within a date specific folder. The insurance verification department reviews the paper runs, manually enters the patient and insurance information, and attaches the run report, PCS, and patient signature form to the 'open' ticket in ESO. The insurance verification department records the number of runs they reviewed and opened tickets for in the ESO system in the same paper run reports log to help verify all paper runs received were converted into an 'open' ticket in ESO.

Run reports can also be received electronically through an SFTP or from an EPCR provider. In both instances, the run reports received either create a new patient record or tie the new run report to an existing patient in the database. The insurance verification department is responsible for verifying the information was imported correctly and verifying that a patient does not have more than one record in the patient database. Duplicate patient records are remediated by the insurance verification department. All other information from the electronically received run report must then be entered by the insurance verification department and supporting documents attached to the 'open' ticket.

Once a ticket is 'open' it will then create a task for the processing department to process the ticket.

Payments Received

Control Objective 9: Control activities provide reasonable assurance that payments received are properly identified, posted, and made available to the Director of Administration for invoicing completely and accurately.

Payments can be received in one of two ways; paper via the mail or remits reports from the clearinghouse. Payments received in the mail are first sorted by the mailroom attendant and put in the appropriate Payment Processor's mailbox unopened according to the defined groups posted in the mailroom. The Payment Processor retrieves the checks from their mailbox, scans a copy of the check, records the payment, and places the paper payments in the invoice drawer for the Director of Administration.

MCA processes all electronic claims through its clearinghouse, ZirMed. Payments received from the clearinghouse can come in two forms of payment. The clearinghouse provides a remit report of EFTs and a notice of credit card payment processing. In both cases, the clearinghouse provides reports of payment processing and the appropriate Payment Processor receives those reports, records payment, and places the reports in the invoice drawer for the Director of Administration.

Run Processing

Control Objective 10: Control activities provide reasonable assurance that runs are processed completely, accurately, and timely.

Processing personnel complete tasks within ESO to process tickets from 'open' to 'ready to bill' status. Each processor is assigned a group of providers for which they are responsible for processing tickets. The Supervisor of Processing is responsible for overseeing the processing tasks dashboard to help verify that tickets are moving through the process and not sitting idle. Processors utilized a tool called Payerlogic which is integrated with the ESO billing system. Payerlogic is an insurance verification tool which assists MCA employees with insurance coverage discovery.

The first task processors complete is confirming the completeness and accuracy of the run details, personal information, and insurance information imported into the new ticket by spot checking what is in the open ticket to the source documents attached. Next, the processors enter in the proper billing codes based on the description of the services provided and the medicine administered. Once complete, the processors perform a clearinghouse audit on the 'open' ticket to help confirm all the information necessary for the clearinghouse is entered correctly. After the clearinghouse audit has passed, the ticket is set to a 'ready' status. On an hourly basis, an automated final audit is performed on all tickets set to 'ready' to perform a final check and to change the status to 'ready to bill'. All audit findings are reported to processors until resolved.

Based on the payer information and structure of the patient's insurance, a HCFA form might need to be submitted. HCFA claims are printed on special HCFA printer paper and are required to be released from the printer to help ensure personal information and HIPAA protected information is not accessible to unauthorized parties. Once daily, the HCFA files are boxed up and taken down

to the post office drop box for submission. An electronic confirmation sheet of the HCFA submission is retained with the run ticket data while awaiting payment.

If a HCFA form is not required, then the 'ready to bill' tickets are converted to a single file in a nightly automated job. The following morning, the file is automatically uploaded to the clearinghouse's SFTP and counts of the number of records submitted and the number of records uploaded is reconciled to help ensure complete and accurate transmissions.

A report of the tickets billed is run automatically and posted to MCA's secure website on a monthly basis. The reports are available for providers' review.

Claims that are billed and denied are researched and remediated by the processing department.

Payment Processing

Control Objective 11: Control activities provide reasonable assurance that payments are processed completely, accurately, and timely.

Payment Processers complete tasks within ESO to process payments and change billed tickets from 'open' to 'closed' status. Each Payment Processor is assigned a group of providers for which they are responsible for. The Supervisor of Payment Processing is responsible for overseeing the payment tasks.

Payments are processed in daily batches to help with accounting and reconciliation. Check, credit card, and EFT payments received are recorded against the correct account. Payments received are totaled and reconciled to the actual amounts posted in ESO. Differences are resolved prior to closing a batch. Payments can have one of two effects on a billed ticket. The payment could be for a partial amount that does not cover the total due, in which case the ticket remains in a 'billed' status. A payment could also "zero-out" the amount due in which case the ticket moves to a 'closed' status. A report of the tickets 'closed' and dollar amount of payments received is run automatically and posted to MCA's secure website on a monthly basis. The reports are available for providers' review.

Payments received are processed daily. The payments received via checks, credit card, and EFT are totaled for each type of payment and put in the fireproof file cabinet for the Director of Administration. The Director of Administration uses the summary of payments processed to create the weekly invoices sent to providers. The invoices are sent to the provider with the payment checks received and the check for credit card payments deposited. Credit card payments present a unique situation. Although MCA does not process any credit card transactions, a separate entity is set up to deposit credit card transactions into and then checks are written weekly to disburse the credit card funds to the providers. On a monthly basis, an employee completely separate from the credit card transactions reconciles the check images of the checks written by the Director of Administration to help verify the legitimacy of the checks.

The ESO software is configured to send monthly statements from the provider to the commercial payer or patient until a ticket is 'closed'. MCA is able to configure the number of statements that

are sent before a ticket is sent to collections or written off to bad debt expense. 'open' tickets with over 45 days of no new activity are flagged and show up in the follow-up personnel's tasks. The follow-up personnel are responsible for calling and/or emailing commercial payers to help ensure all efforts for collecting payments are exhausted prior to sending a ticket to collection. A report of the tickets and dollar amounts sent to collections and written off are run automatically and posted to MCA's secure website on a monthly basis. The reports are available for the provider's review.

User Entity Control Considerations

MCA's Medical Billing System control framework was designed with the assumption that specific internal controls would be implemented by client organizations. In certain situations, the application of specified internal controls at client organizations is necessary to achieve the specific control objectives included in this report. The client's organizational internal controls should be in operation to complement MCA's Medical Billing System controls. It is each interested party's responsibility to evaluate the client organization control considerations information presented in this section in relation to the internal controls that are in place at client organizations to obtain a complete understanding of the total internal control structure and to assess control risk. If effective client internal controls are not in place, MCA's Medical Billing System controls may not compensate for such weaknesses.

This section describes other internal controls that should be in operation at client organizations to complement the controls at MCA's Medical Billing System. The auditors of MCA's Medical Billing System clients should consider whether the following controls have been placed in operation at client organizations.

Computer Operations (Backup and Storage)

- User entities are responsible for maintaining their own system(s) of record.

Application Change Control

- User entities are responsible for approving changes that could have an impact on processing of customer data in a timely manner.

Information Security

- User entities are responsible for notifying MCA, in a timely manner, when changes are made to technical, billing, or administrative contact information.
- User entities are responsible for ensuring that user IDs and passwords to MCA's secure website are assigned only to authorized individuals and that the roles assigned to the user accounts are appropriate.
- User entities are responsible for ensuring the confidentiality of any user IDs and passwords assigned to them for use with MCA's systems.
- User entities are responsible for ensuring that MCA is notified of any required user account maintenance in a timely manner.

- User entities are responsible for immediately notifying MCA of any actual or suspected information security breaches, including compromised user accounts.

Runs Received

- User entities are responsible for providing complete and accurate records of the run reports.
- User entities are responsible for reconciling the number of runs submitted to MCA to the number of runs received by MCA.

Payment Processing

- User entities are responsible for reconciling their weekly MCA payment received reports to their bank records.

Section 4: MCA's Control Objectives and Related Controls and Independent Service Auditors' Tests of Controls and Results Thereof

Introduction

This report on the internal controls placed in operations and tests of operating effectiveness is intended to provide interested parties with sufficient information to obtain an understanding of those aspects of MCA's controls that may be relevant to a user organization's internal control structure. This report, when combined with an understanding of the policies and procedures at user organizations, is intended to assist user auditors in planning the examination of the user organization and in assessing control risk for assertions of the user organizations' financial statements that may be affected by policies and procedures of MCA's Medical Billing System.

The system description, control objectives and related controls are the responsibility of MCA's management. Marcum LLP's responsibility is to express an opinion that the system description was fairly presented and controls were suitably designed to achieve the control objectives specified in the testing matrices and were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives, specified by MCA's management, were achieved during the period of August 1, 2020 to July 31, 2021.

Control Environment

The control environment represents the collective effect of various components in establishing and enhancing the effectiveness of specific controls and mitigating identified risks. In addition to testing the design and operating effectiveness of the control activities in Section 4 of this report, our review also included tests of and consideration of the relevant components of MCA's testing matrices pertaining to their support of the Medical Billing System.

Our tests of the control environment included the following procedures to the extent we considered necessary to address management's relevant control environment and included the following:

- Obtaining an understanding of MCA's organizational structure, including the segregation of duties, policy statements, and personnel policies.
- Discussions with management, operations, administrative, and other personnel who were responsible for developing and enforcing daily activities and requirements.
- Testing of oversight and company-level controls on a sample basis to ensure key control environment activities were operating as described

Testing Approach

The objective of our testing is to determine the operating effectiveness of the controls specified by MCA's management throughout the examination period of August 1, 2020 to July 31, 2021. Testing was designed with the intent to perform procedures to provide reasonable but not absolute assurance that the specified controls were achieved throughout the examination period. The nature of the tests conducted took into consideration the type of control testing and the evidential matter that is available to perform a test to determine the operating effectiveness.

Types of Tests Performed:

1) **Inquiry:** tests include the corroboration of relevant personnel to verify the knowledge and understanding of the described control activity.
2) **Observation:** tests include the physical observation of the implementation, application of, or, existence of specific controls.
3) **Inspection:** tests include the physical validation of documents, records, configuration, or settings.
4) **Re-performance:** tests include the reprocessing of transactions, procedures, and calculations to ensure the accuracy and completeness of the control description.

Sampling Approach

The table below illustrates sampling that is utilized to determine the operating effectiveness of the controls specified by MCA:

Nature of Control and Frequency of Performance	Minimum Number of Items to Test
Occurrence based	10%, minimum of 5, maximum of 25
Manual control performed weekly	5
Manual control performed monthly	2
Manual control performed quarterly	2
Manual control performed annually	1
Application/Programmed control	Test one application of each programmed control for each type of transaction if supported by effective IT general controls (that have been tested); otherwise test at least 25

Testing Matrices

Physical Security

Control Objective 1: Control activities provide reasonable assurance that physical access to the business premises and information systems is limited to properly authorized individuals.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.1	Physical security policies and procedures exist to guide personnel in the performance of job responsibilities.	Inspected the physical access policy to verify that physical security policies and procedures were documented and in place	No exceptions noted.
1.2	External perimeter doors are limited to secure badge entry access after normal business hours.	Inspected the badge access time schedules to verify that access to external perimeter doors was limited to secure badge entry access after normal business hours.	No exceptions noted.
1.3	A badge access system restricts access to perimeter doors of the facility.	Inspected the badge access user listing and permission levels to verify that the badge access system restricted access to perimeter doors of the facility	No exceptions noted.
1.4	Badge access request requires the approval of the HR Director.	Inspected the new hire checklist for a sample of employees hired throughout the examination period to verify that badge access required the approval of the HR Director.	No exceptions noted.
1.5	Badge access zone definitions are established and assigned to personnel based on their job responsibilities.	Inspected the badge access user listing, badge access time settings, and the active employee listing to verify that badge access zone/time definitions were established and assigned to personnel based on their job responsibilities.	No exceptions noted.
1.6	Access to administer the badge access system is limited to personnel based on their job responsibilities.	Inspected the listing of badge access administrators and the active employee listing to verify that the ability to administer the badge access system was restricted to appropriate personnel.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.7	The badge access system documents access attempts to and within the facility premises. Badge access logs are reviewed on a bi-weekly basis.	Inspected the badge access logs and the badge log review for a sample of weeks throughout the examination period to verify that the badge access system documented access attempts to and within the facility and the logs were reviewed on a bi-weekly basis.	No exceptions noted.
1.8	Terminated employees' badge access rights are revoked as a component of the termination process.	Inspected the badge access user listing and the completed termination checklist for a sample of employees terminated throughout the examination period to verify that terminated employee's badge access rights were revoked upon termination.	No exceptions noted.
1.9	Visitor access logs are used to record the visitor's name, company affiliation, arrival and departure times, and reason for visit.	Inspected the visitor sign in log for a sample of months throughout the examination period to verify that visitor access logs were used to record the visitor's name, company affiliation, arrival and departure times, and reason for visit.	No exceptions noted.
1.10	A visitor badge is required to be worn while on site.	Inspected the visitor sign in log for a sample of months and the visitor badge required to be worn by visitors in office to verify that a visitor badge was required to be worn while on site. Inquired of the HR Director to verify that all visitors were required upon entry to sign the visitor log and obtain a badge to be worn during the entire duration of the visit.	No exceptions noted.
1.11	Physical keys are restricted to a limited number of management personnel. An inventory of physical keys is maintained to track and monitor key access.	Inspected the physical key inventory listing and the active employee listing to verify that physical keys were restricted to a limited number of management personnel and an inventory was used to track and monitor physical keys.	No exceptions noted.
1.12	A security alarm system is installed and monitored by a third party alarm monitoring provider to detect unauthorized access/events.	Inspected the third party security system provider certificate and invoice to verify that a security alarm system was monitored by a third party provider to detect unauthorized access.	No exceptions noted.
1.13	Server room access is limited to appropriate personnel based on their job responsibilities.	Inspected the physical key inventory and the active employee roster to verify that the server room access was limited to appropriate personnel based on their job responsibilities.	No exceptions noted.

Environmental Security

Control Objective 2: Control activities provide reasonable assurance that critical information technology infrastructure is protected from certain environmental threats.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.1	The corporate facility is protected by fire detection and suppression systems that include: ➢ Fire alarm ➢ Water sprinklers ➢ Smoke detector ➢ Hand-held fire extinguishers	Inspected the facility maintenance contract to verify that the corporate facility was protected by fire detection and suppression systems that included: ➢ Fire alarm ➢ Water sprinklers ➢ Smoke detector ➢ Hand-held fire extinguishers	No exceptions noted.
2.2	Annually, a third party provider performs inspection and as needed maintenance on the fire detection and suppression systems.	Inspected the third party maintenance invoice to verify that a third party provider performed maintenance inspections on the fire detection and suppression systems annually.	No exceptions noted.
2.3	Production servers are maintained in racks raised above the floor to reduce the impact of localized flooding.	Inspected the server rack to verify that production servers were maintained in racks raised off the floor to reduce the impact of localized flooding.	No exceptions noted.
2.4	Environmental monitoring applications are utilized to monitor the following server rack environmental conditions: ➢ Temperature ➢ Humidity ➢ UPS ➢ Availability	Inspected the environmental monitoring application settings and the UPS monitoring dashboard to verify that an environmental monitoring application was utilized to monitor the following: ➢ Temperature ➢ Humidity ➢ UPS ➢ Availability	No exceptions noted.
2.5	The environmental monitoring application notifies personnel via e-mail of conditions outside of the defined parameters.	Inspected the environmental monitoring application notification settings and a sample alert sent throughout the examination period to verify that IT personnel were notified via e-mail of conditions outside of predefined parameters.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.6	A UPS provides power to critical infrastructure equipment in the event of a temporary power outage or power surge and notifies appropriate personnel in the case of any failures.	Inspected the UPS system and the UPS monitoring configurations to verify that a UPS system provided power to critical infrastructure equipment in the event of a temporary power outage or power surge and notified appropriate personnel in the case of any failures.	No exceptions noted.
2.7	The UPS system is tested bi-weekly to monitor the availability and reliability of temporary power supplies.	Inspected the UPS self-test configurations to verify the UPS System was tested bi-weekly to monitor the availability and reliability of temporary power supplies.	No exceptions noted.

Computer Operations (Backups and Storage)

Control Objective 3: Control activities provide reasonable assurance that system data is regularly backed up and available for restoration in the event of processing errors or unexpected interruptions.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.1	Formal backup, storage, and restoration procedures are documented and available to computer operations personnel.	Inspected the backup policies and procedures and its location on the company shared drive to verify that formal backup storage and restoration procedures were documented and made available to computer operations personnel.	No exceptions noted.
3.2	An automated backup system is utilized to schedule and perform system backups.	Inspected the backup system schedule and the listing of systems being backed up of to verify that an automated backup system was utilized to schedule and perform backups.	No exceptions noted.
3.3	The backup system is configured to perform daily differential backups.	Inspected the backup configurations and the backup log for a sample of days throughout the examination period to verify that the backup system was configured to perform daily differential backups.	No exceptions noted.
3.4	The backup system notifies computer operations personnel of failed backups. Failed backups are assessed to determine if a new backup is required.	Inspected the backup notification configurations and a failed backup alert sent during the examination period to verify that the backup system notified computer operations personnel of failed backups.	No exceptions noted.
3.5	The backup system is configured to encrypt backup media as a component of the backup process.	Inspected the backup system encryption settings to verify that the backup system was configured to encrypt media as a component of the backup process.	No exceptions noted.
3.6	Daily backup files are replicated to a secure offsite facility.	Inspected the backup system schedule settings and log of completed backups files for a sample of production servers to verify that daily backup files were replicated to a secure offsite facility.	No exceptions noted.
3.7	The ability to recall backup media is limited to appropriate personnel based on their job responsibilities.	Inspected the backup system user listing and the active employee roster to verify that the ability to recall backup media was limited to appropriate personnel based on their job responsibilities and access permissions.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.8	Annual restoration testing is performed to verify the integrity of backup media and confirm the ability to restore critical components of the production environment.	Inspected the backup policy and procedures to verify that annual restoration testing was performed to verify the integrity of backup media and confirmed the ability to restore critical components of the production environment.	Exception Noted. There was no annual restoration test completed to test the operating effectiveness of this control during the examination period

Complementary user entity controls. User entities are responsible for establishing controls related to the following:

- User entities are responsible for maintaining their own system(s) of record.

Computer Operations (System Availability)

Control Objective 4: Control activities provide reasonable assurance that production systems are designed, maintained, and monitored to help ensure system availability.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.1	Documented procedures are in place to guide operations personnel in performing daily activities to help ensure system availability.	Inspected the data recovery plan and the monitoring system configurations and a sample alert to verify that system outage policies and procedures were documented and in place to guide employees in helping ensure system availability and provide a point of contact to assist them.	No exceptions noted.
4.2	The production system infrastructure has built in redundancies to minimize potential impact of system failures.	Inspected the network diagram to verify that the production system infrastructure had built in redundancies to minimize the impact of system failures.	No exceptions noted.
4.3	An enterprise monitoring application is utilized to monitor primary server performance and disk space.	Inspected the enterprise monitoring application settings and a sample alert generated during the examination period to verify that an enterprise monitoring application was utilized to monitor primary server performance and disk space.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.4	The enterprise monitoring application is configured to generate alert notification sent to computer operations personnel via e-mail when a primary server fails or predefined disk space thresholds are exceeded on servers.	Inspected the enterprise monitoring application alert settings and a sample alert sent during the examination period to verify that the enterprise monitoring application was configured to send alert notifications to computer operations personnel via e-mail when predefined thresholds were exceeded on servers.	No exceptions noted.
4.5	Help desk procedures are in place to guide personnel through the incident response process.	Inspected the incident response policy and procedures to verify that help desk procedures were in place to guide personnel through the incident response policy and included the following sections: ➢ Receiving ➢ Validating ➢ Logging ➢ Screening ➢ Prioritizing ➢ Assigning ➢ Escalating ➢ Resolving ➢ Closing	No exceptions noted.
4.6	A help desk ticketing system is utilized to track and respond to reported incidents.	Inspected the help desk tickets for a sample of incidents reported throughout the examination period to verify that a help desk ticketing system was utilized to track and respond to reported incidents.	No exceptions noted.
4.7	A patch management and release system is utilized to monitor patch releases to production servers.	Inspected the patch log for a sample of servers utilized throughout the examination period to verify that a patch management and release system was utilized to monitor patch releases to production servers.	No exceptions noted.
4.8	Production servers and workstations are equipped with antivirus software to detect and prevent the transmission of data or files that contain certain virus signatures.	Inspected the antivirus update schedule for a sample of workstations and production servers utilized throughout the examination period to verify that production servers and workstations were equipped with antivirus software that scanned for virus signatures.	No exceptions noted.
4.9	Antivirus software is automatically updated with current virus signatures every hour.	Inspected the antivirus configurations for a sample of workstations and production servers utilized throughout the examination period to verify that the antivirus was configured to automatically update with current virus signatures on an hourly basis.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.10	The antivirus software scans servers for virus signatures and performs a comprehensive scan once a week.	Inspected the antivirus configurations for a sample of workstations and production servers utilized throughout the examination period to verify that the antivirus software scanned servers and performed a comprehensive scan weekly.	No exceptions noted.

Application Change Control

Control Objective 5: Control activities provide reasonable assurance that requests for application changes are initiated by authorized individuals and that changes are authorized prior to production migration.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
5.1	Application change control policies and procedures are documented to guide personnel through the change request and implementation authorization process.	Inspected the change control procedures to verify that application change control policies and procedures were documented and in place to help guide personnel through the request and change authorization process.	No exceptions noted.
5.2	Application change requests are initiated by authorized personnel.	Inspected the change control procedures, the list of users with access to initiate change requests from ESO and the active employee roster to verify that application change requests are required to be initiated by authorized personnel. Inquired of the technical specialist to verify that there were no application changes requested throughout the examination period.	Control did not operate - There were no application changes requested throughout the examination period to test the operating effectiveness of this control.
5.3	Application changes require authorization from MCA management prior to being implemented.	Inspected the change control procedures to verify that application changes required authorization from MCA management prior to being implemented. Inquired of the technical specialist to verify that there were no application changes requested throughout the examination period.	Control did not operate - There were no application changes requested throughout the examination period to test the operating effectiveness of this control.

Complementary user entity controls. User entities are responsible for establishing controls related to the following:

- User entities are responsible for approving changes that could have an impact on processing of customer data in a timely manner.

Information Security

Control Objective 6: Control activities provide reasonable assurance that logical access to critical systems and data is restricted to authorized individuals.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
6.1	Formal information security policies and procedures are in place to establish organizational information security standards.	Inspected the IT security handbook policies to verify that formal information security policies and procedures were documented and in place.	No exceptions noted.
6.2	IT access requests are approved prior to granting access to production systems.	Inspected the information security access authorization form for a sample of employees hired throughout the examination period to verify that the employee's IT access was approved prior to granting access.	No exceptions noted.
6.3	Network domain users are authenticated via an authorized user account and password. The network domain account policies are configured to enforce the following password requirements: ➢ Minimum password length of eight characters ➢ Minimum password history of three previously used passwords ➢ Minimum password age of one day ➢ Maximum password age of 90 days ➢ Password complexity ➢ Lockout threshold of three consecutive failed login attempts	Inspected the network domain account policies to verify that policies were configured to enforce the following password requirements: ➢ Minimum password length of eight characters ➢ Minimum password history of three previously used passwords ➢ Minimum password age of one day ➢ Maximum password age of 90 days ➢ Password complexity ➢ Lockout threshold of three consecutive failed login attempts	No exceptions noted.
6.4	Administrative access to the network domain is restricted to personnel with administration job responsibilities.	Inspected the listing of network domain administrators and listing of active employees to verify admin access to the network domain was restricted to appropriate personnel.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
6.5	Network accounts assigned to terminated personnel are deactivated as a component of the termination process.	Inspected the active directory and network accounts assigned to personnel terminated throughout the examination period to verify network accounts assigned to terminated employees were deactivated as part of the termination process.	No exceptions noted.
6.6	Server operating system access is restricted via network domain credentials and group policy settings inherited from the primary domain controller.	Inspected the listing of servers within the network domain and the group policy inheritance configurations to verify that server operating system access was restricted via network domain credentials and settings were inherited from the primary domain controller.	No exceptions noted.
6.7	Administrative access to the server operating system is restricted to personnel with administration job responsibilities.	Inspected the server administrators for a sample of servers utilized throughout the examination period and the listing of active employees to verify that administrative access to the server operating system was restricted to appropriate personnel.	No exceptions noted.
6.8	Database user access is restricted via Windows authentication.	Inspected the database logon settings to verify that database user access was restricted via Windows authentication.	No exceptions noted.
6.9	Access to the databases is restricted via authorized application and administrator accounts.	Inspected the database logon settings and the database user listing for the only production database utilized throughout the examination period and the active employee roster to verify that access to the database was restricted via authorized application and administrative accounts.	No exceptions noted.
6.10	Application authentication is restricted via unique user account and passwords that required the following password requirements. ➢ Minimum password length of eight characters ➢ Maximum password age of 90 days ➢ Lockout threshold of three consecutive failed login attempts ➢ Password complexity enabled	Inspected the application authentication configurations and the group policy export to verify that policies were configured to enforce the following password requirements: ➢ Minimum password length of eight characters ➢ Maximum password age of 90 days ➢ Lockout threshold of three consecutive failed login attempts ➢ Password complexity enabled	No exceptions noted.
6.11	Access to administer the application is limited to IT personnel based on their job responsibilities	Inspected the listing of application administrators in the ESO admin group and the active employee roster to verify access to administer the application was limited to IT personnel based on job responsibilities.	No exceptions noted.

Complementary user entity controls. User entities are responsible for establishing controls related to the following:

- User entities are responsible for notifying MCA, in a timely manner, when changes are made to technical, billing, or administrative contact information.
- User entities are responsible for ensuring that user IDs and passwords to MCA's secure website are assigned only to authorized individuals and that the roles assigned to the user accounts are appropriate.
- User entities are responsible for ensuring the confidentiality of any user IDs and passwords assigned to them for use with MCA's systems.
- User entities are responsible for ensuring that MCA is notified of any required user account maintenance in a timely manner.
- User entities are responsible for immediately notifying MCA of any actual or suspected information security breaches, including compromised user accounts.

Data Communications

Control Objective 7: Control activities provide reasonable assurance that data maintains its integrity and security as it is transmitted between third parties and the service organization.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
7.1	Redundant stateful firewalls are in place and configured to filter unauthorized inbound network traffic from the Internet.	Inspected the firewall rulesets and the network diagram to verify that a stateful firewall was in place and configured to filter unauthorized inbound network traffic.	No exceptions noted.
7.2	NAT is utilized to manage internal IP addresses. Routable IP addresses are not permitted on the internal network.	Inspected the NAT configurations to verify that NAT was utilized to manage internal IP addresses and to prohibit routable IP addresses.	No exceptions noted.
7.3	Access control lists prevent access to production hosted system components by service and IP.	Inspected the ACL ruleset for the firewall to verify that ACLs prevented access to production host system components by service and IP address.	No exceptions noted.
7.4	Administrative access to the firewall system is restricted to personnel with firewall administration responsibilities.	Inspected the listing of firewall administrators and the listing of active employees to verify that administrative access to the firewall system was restricted to appropriate personnel.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
7.5	IPS is utilized to prevent network breaches and report blocked-site IP addresses.	Inspected the IPS configurations to verify that an IPS was utilized to prevent network breaches and report blacklisted IP addresses.	No exceptions noted.
7.6	An external vulnerability scan is performed by a third party provider monthly on the production systems to detect potential vulnerabilities.	Inspected the external vulnerability scan for a sample of months throughout the examination period to verify that annually an external vulnerability scan was performed by a third party provider on the production systems to detect potential vulnerabilities.	No exceptions noted.
7.7	Access for remote connection to production systems is restricted to appropriate personnel	Inspected the listing of VPN users and the listing of active employees to verify that VPN connection to production systems was restricted to appropriate personnel.	No exceptions noted.
7.8	A VPN is utilized for remote access to help ensure the privacy and integrity of the data passing over the public network.	Inspected the VPN settings to verify that a SSL VPN was utilized for remote access to help ensure the privacy and integrity of data.	No exceptions noted.
7.9	VPN access requires a two factor authentication via a user account, password and one time password.	Inspected the VPN configurations to verify that VPN access required two factor authentication via the use of a user account, password, and one time password.	No exceptions noted.
7.10	VPN administration privileges are restricted to appropriate network administration personnel.	Inspected the listing of VPN administrators and the listing of active employees to verify that VPN administrative privileges were restricted to appropriate network administration personnel.	No exceptions noted.
7.11	An SFTP is in place to help ensure the privacy and integrity of data as it passes over the public network.	Inspected the SFTP settings to verify that a secure file server was in place to help ensure the privacy and integrity of data passing over the public network.	No exceptions noted.
7.12	Firewall changes are formally documented and approved.	Inspected the firewall change request tickets for a sample of firewall changes implemented throughout the examination period to verify that firewall changes were formally documented and approved.	No exceptions noted.

Runs Received

Control Objective 8: Control activities provide reasonable assurance that runs received are properly identified, verified, and made available to the assigned Insurance Verification staff timely and accurately.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
8.1	Paper runs received in the mail are sorted at the point of entry and sent to the HR Coordinator.	Observed the Supervisor of Claim Processing complete paper run processing to verify that paper runs received in the mail were sorted at the point of entry and sent to the HR Coordinator.	No exceptions noted.
8.2	A log of the paper runs received and runs processed is maintained on a daily basis to help ensure all paper runs received are processed completely and accurately.	Inspected the run log entries for a sample of paper runs and days throughout the examination period to verify that a log of the paper runs received and processed was maintained to help ensure the runs received for the sample of days were processed completely and accurately.	No exceptions noted.
8.3	Run data received electronically from EPCR vendors and by other electronic means are initially reviewed by the insurance verification team for completeness and accuracy of imported patient data. Identified discrepancies are researched and resolved by the insurance verification team.	Observed the Supervisor of Claim Processing review of the imported patient data to verify that the insurance verification team reviewed the patient information imported from EPCR or other electronic means to help ensure completeness and accuracy of the imported information and discrepancies were researched and resolved.	No exceptions noted.
8.4	Provider run data received electronically from EPCR vendors and by other electronic means are imported by provider group to the Claims Specialist assigned to that provider.	Inspected the daily import runs for the EPCR vendor for a sample of days throughout the examination period to verify that provider runs received electronically from EPCR vendors and by other electronic means were imported by provider group to the Claims Specialist assigned to that provider.	No exceptions noted.

Complementary user entity controls. User entities are responsible for establishing controls related to the following:

- User entities are responsible for providing complete and accurate records of the run reports.
- User entities are responsible for reconciling the number of runs submitted to MCA to the number of runs received by MCA.

Payments Received

Control Objective 9: Control activities provide reasonable assurance that payments received are properly identified, posted, and made available to the Director of Administration for invoicing completely and accurately.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
9.1	Payments received by mail are placed in the appropriate Payment Processor's box in the mail room unopened.	Observed the Payment Processor perform daily tasks to verify that payments received by mail were placed in the appropriate mail box or opened, scanned and placed into the appropriate payment processor's network drive.	No exceptions noted.
9.2	The Payment Processor retrieves the checks from the mailbox, scans a copy, records payment, and places the paper payments in the invoice drawer for the Director of Administration.	Observed the Payment Processor perform daily tasks to verify that checks were retrieved from the mail box or network drive, scanned, payment posted, and placed the paper payment in the invoice drawer for the Director of Administration.	No exceptions noted.
9.3	Payments received by credit card through MCA's clearinghouse are imported by each provider's assigned Payment Processor.	Observed the Payment Processor perform daily tasks to verify that payment received by credit card through MCA's clearinghouse were imported by each provider's assigned Payment Processor.	No exceptions noted.

Run Processing

Control Objective 10: Control activities provide reasonable assurance that runs are processed completely, accurately, and timely.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
10.1	The Supervisor of Processing is responsible for overseeing the processing dashboard to help ensure Processors are completing tasks to process run reports completely, accurately, and timely.	Observed the processing of run reports and the run report dashboard to verify that the Supervisor of Processing was responsible for overseeing the processing dashboard to help ensure Processors were completing tasks completely, accurately, and timely.	No exceptions noted.
10.2	Processors confirm the completeness and accuracy of the run details imported into new tickets by spot checking what is in ESO to the run report.	Observed the processing of run reports to verify that Processors confirmed the completeness and accuracy of the run details imported into new tickets by spot checking what was in ESO to the run reports.	No exceptions noted.
10.3	Processors confirm the completeness and accuracy of the personal and insurance information imported into new tickets by spot checking what is in ESO to the run report, PCS, and patient signature form.	Observed the processing of run reports to verify that Processors confirmed the completeness and accuracy of the personal and insurance information imported into new tickets by spot checking what was in ESO to the run report, PCS, and patient signature form.	No exceptions noted.
10.4	Proper billing codes are entered from a pre-defined list of billing codes by the Processor.	Observed the Supervisor of Processing review entered billing codes to verify that proper billing codes were entered by the Processors. Inspected the claims billing code configurations and definitions to verify that a pre-defined list of billing codes was available.	No exceptions noted.
10.5	Processors perform a clearinghouse audit on tickets prior to setting the ticket status to 'ready'. Audit finding are resolved prior to setting ticket status to 'ready'.	Observed the clearinghouse audit to verify that a clearing house audit was performed on tickets prior to setting the status to 'ready' and that audit findings were resolved by the Processor.	No exceptions noted.
10.6	An automated final audit is performed on all tickets with status set to 'ready' on an hourly basis prior to setting the ticket status to 'ready to bill'. Notifications of audit findings are sent to the Processors for resolution.	Inspected the system settings and a sample audit finding notification to verify that an automated final audit was performed on tickets with status 'ready' on an hourly basis and once the final audit was complete, tickets were set to 'ready to bill' and any notifications of audit findings were sent to the Processors for resolution.	No exceptions noted.
10.7	A HCFA is printed and mailed daily for tickets requiring paper transmission.	Observed the paper transmission procedure to verify that a HCFA was printed and mailed daily for tickets requiring paper transmission.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
10.8	Monthly reports are generated for use by the provider group and are accessible to the provider through MCA's secure web site.	Inspected the monthly report task scheduler configurations and the exported reports for a sample of active clients and months throughout the examination period to verify that monthly reports were generated for use by the provider group and were accessible to the provider through MCA's secure web site.	No exceptions noted.
10.9	Denials are researched and remediated by the processing department.	Observed the processing of a denial to verify that the processing department researched and remediated denials.	No exceptions noted.

Payment Processing

Control Objective 11: Control activities provide reasonable assurance that payments are processed completely, accurately, and timely.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
11.1	Check, credit card, and EFT payments received are recorded against the correct account.	Observed the payment process to verify that check, credit card, and EFT payments were received and recorded against the correct amount.	No exceptions noted.
11.2	Tickets remain in an 'open' status until all payments are received. Once a balance is zeroed out the ticket is set to a 'closed' status.	Inspected the ticket status settings to verify that tickets remained in an 'open' status until all payments were received and once the balance was zeroed out the ticket was set to a 'closed' status.	No exceptions noted.
11.3	When the payment closes the ticket, the ticket is moved to a closed file.	Inspected the ticket status settings to verify that if a payment closes a ticket then the ticket was migrated to a closed file and retained for ad hoc inquiries.	No exceptions noted.
11.4	Tickets with no new activity for 45-60 days are converted to 'follow-up' status and worked by the follow-up department.	Observed the follow-up department complete daily processing of claims to verify that tickets set to 'follow-up' status were available in the follow-up department's task queue.	No exceptions noted.
11.5	Collection reports are published to MCA's secure website for each provider group to help aid provider groups in their reconciliation.	Inspected the MCA website and sample collection report to verify collection reports were published to MCA's secure website for each provider group to help aid provider groups in their reconciliation.	No exceptions noted.
11.6	Checks written from the credit card liability account are reconciled by a separate individual on a monthly basis to help ensure appropriateness of the checks.	Inspected the proof review to confirm that the checks agreed to the liability account for a sample of months throughout the examination period to verify that a separate individual signed off on the report of checks issued from the liability account.	No exceptions noted.
11.7	Billing statements are generated by the system on 30 day intervals as long as the ticket status remains open.	Inspected the billing statement settings and a sample billing statement generated and sent throughout the examination period to verify that billing statements were configured to be generated every 30 days while the ticket status remains open.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
11.8	Tickets awaiting payment after a predetermined number of days have elapsed from the initial billing statement are followed-up by the follow-up department to help ensure all efforts are made to receive payment on billed tickets.	Observed the follow-up department complete daily tasks to verify that tickets awaiting payment after a predetermined number of days from the initial billing statement create a follow-up task for the follow-up personnel to help ensure billed tickets receive payment. Observed the follow-up personnel complete tasks to verify that the follow-up personnel were completing tasks to help ensure all efforts were made to receive payment on billed tickets. Inspected the scheduled tasks settings to verify that tickets awaiting payment after a predetermined number of days have elapsed from the initial billing statement created a follow-up task for the follow-up personnel to complete.	No exceptions noted.
11.9	Accounts that remain inactive are written off to bad debt expense or sent to collections based on the predefined thresholds of account inactivity within ESO.	Inquired of the Claims Processor to verify accounts that remain inactive were written off to bad debt expense or sent to collections based on the predefined thresholds of account inactivity within ESO. Observed tickets placed in the "bucket" and verified tickets were assessed from the oldest to the newest accounts that remained inactive, after the claims assessed for the final time they were written off as bad debt expense.	No exceptions noted.

Complementary user entity controls. User entities are responsible for establishing controls related to the following:

- User entities are responsible for reconciling their weekly MCA payment received reports to their bank records.

Section 5: Other Information Provided by MCA

Testing Exceptions

#	Control Activity Specified By The Service Organization	Test Applied By The Service Auditor	Test Results	Management's Response to Test Results
3.8	Annual restoration testing is performed to verify the integrity of backup media and confirm the ability to restore critical components of the production environment.	Inspected the backup policy and procedure to verify that annual restoration testing was performed to verify the integrity of backup media and confirmed the ability to restore critical components of the production environment.	Exception Noted. There was no annual restoration test completed to test the effectiveness of this control during the examination period	Management was unable to get the restoration test scheduled with our MSP before the end of the examination period. The restoration test will take place in Q4 of 2021.

MARCUMGROUP

Marcum Group is a family of organizations providing a comprehensive range of professional services including accounting and advisory, technology solutions, wealth management, and executive and professional recruiting.

These organizations include:

- Marcum LLP
  www.marcumllp.com
- Marcum Bernstein & Pinchuk
  www.marcumbp.com
- Marcum Insurance Services
  www.marcumis.com
- Marcum RBK Ireland
  www.marcumrbk.com
- Marcum Search
  www.marcumsearch.com
- Marcum Strategic Marketing
  marketing.marcumllp.com
- Marcum Technology
  www.marcumtechnology.com
- Marcum Wealth
  www.marcumwealth.com

MARCUM
ACCOUNTANTS ▲ ADVISORS

Ben Osbrach, CISSP, CISA, QSA, CICP, National Risk Advisory Leader
813.397.4860 ● ben.osbrach@marcumllp.com

Mark Agulnik, CPA, CISA, CIS LI, JD, Regional Advisory Partner-in-Charge
954.320.8013 ● mark.agulnik@marcumllp.com