

# Service Organization Control (SOC 1) Report on the Suitability of the Design and Operating Effectiveness of Controls

Montana Medicaid Management  
Information System  
For the Period July 1, 2014 to  
June 30, 2015



©2015 Xerox Corporation. All rights reserved. Xerox® and Xerox and Design® are trademarks of Xerox Corporation in the United States and/or other countries. BR11229

# Table of Contents

I. Independent Service Auditor’s Report.....	2
Independent Service Auditor’s Report.....	3
II. Xerox Business Services, LLC’s Management Assertion .....	6
Xerox Business Services, LLC’s Management Assertion .....	7
Management’s Assertion Process .....	9
III. Description of the System Provided by Xerox Business Services, LLC	10
Overview of the Company .....	11
Overview of Operations Related to Montana Medicaid Management Information System .....	12
Relevant Aspects of the Control Environment, Risk Assessment Process and Monitoring.....	13
Information and Communication.....	16
Control Objectives and Related Controls.....	17
Complementary User Entity Controls .....	24
IV. Xerox Business Services, LLC’s Control Objectives, Related Controls, and the Independent Service Auditor’s Description of Tests of Controls and Results.....	26
Control Objectives, Related Controls, and Results of Testing.....	27
Change Management.....	28
Logical Access .....	30
Computer Operations.....	32
Physical Access .....	33
Reference Files.....	35
Claims Processing .....	37
Provider Enrollment.....	39
Plan Benefit Parameters .....	40
V. Other Information Provided by Xerox Business Services, LLC.....	41
Management Response to Testing Deviations .....	42
Business Continuity and Disaster Recovery .....	44

# I. Independent Service Auditor's Report



Ernst & Young LLP  
One Commerce Square  
Philadelphia, Pennsylvania 19103

Tel: +1 215 448 5000  
Fax: +1 215 448 4069  
ey.com

## Independent Service Auditor's Report

### To the Management of Xerox

#### Scope

We have examined Xerox Business Services, LLC's ("Xerox") accompanying "Description of the system provided by Xerox Business Services, LLC" ("Description") for its Montana ("MT") Medicaid Management Information System (MMIS) for processing Medicaid transactions for the State of Montana throughout the period July 1, 2014 to June 30, 2015 and the suitability of the design and operating effectiveness of controls described therein to achieve the related control objectives stated in the Description. 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 Xerox controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Xerox uses Digital Harbor for provider background checks and Electronic Data Interchange (EDI) Gateway for EDI services. In addition, the Xerox Pittsburgh Data Center hosts the Montana MMIS servers. The Description includes only the controls and related control objectives of Xerox and excludes the control objectives, and related controls of Digital Harbor, EDI Gateway and the Xerox Pittsburgh Data Center. Our examination did not extend to controls of Digital Harbor, EDI Gateway or the Xerox Pittsburgh Data Center.

The information in the accompanying "Other Information Provided by Xerox Business Services, LLC" is presented by management of Xerox to provide additional information and is not part of the Xerox Description. Such information has not been subjected to the procedures applied in our examination and, accordingly we express no opinion on it.

#### Xerox responsibilities

Xerox has provided the accompanying assertion titled, Xerox Business Services, LLC's Management Assertion (Assertion) about the fairness of the presentation of the Description and suitability of the design and operating effectiveness of the controls described therein to achieve the related control objectives stated in the Description. Xerox is responsible for preparing the Description and Assertion, including the completeness, accuracy, and method of presentation of the Description and 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 to achieve the related control objectives stated in the Description.



## **Service auditor's 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 described therein to achieve the related control objectives stated in the Description, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the Description is fairly presented and the controls described therein are suitably designed and operating effectively to achieve the related control objectives stated in the Description throughout the period July 1, 2014 to June 30, 2015.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the service organization's controls described therein to achieve the related control objectives stated in the Description 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 those controls to achieve the related control objectives. Our procedures included 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. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives were achieved. An examination engagement of this type also includes evaluating the overall presentation of the Description, the suitability of the control objectives, and the suitability of the criteria specified by the service organization and described in the Assertion. We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

## **Inherent limitations**

Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or omissions 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 or fail.

## **Opinion**

In our opinion, in all material respects, based on the criteria described in the Xerox Assertion:

- a. the Description fairly presents the MT MMIS system that was designed and implemented throughout the period July 1, 2014 to June 30, 2015.



- 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 July 1, 2014 to June 30, 2015 and if the State of Montana applied the complementary user entity controls contemplated in the design of Xerox controls and if subservice organizations applied the controls contemplated in the design of Xerox controls throughout the period July 1, 2014 to June 30, 2015.
- c. the controls tested, which, together with the complementary user entity controls and subservice organization's controls referred to in the scope paragraph of this report if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the Description were achieved, operated effectively throughout the period July 1, 2014 to June 30, 2015.

### **Description of tests of controls**

The specific controls tested and the nature, timing, and results of those tests are listed in the accompanying "Xerox Business Services, LLC's Control Objectives, Related Controls, and the Independent Service Auditor's Description of Tests of Controls and Results" ("Description of Tests and Results").

### **Restricted use**

This report, including the description of tests of controls and results thereof in the Description of Tests and Results, is intended solely for the information and use of Xerox, the State of Montana and the independent auditors of the State of Montana, who have a sufficient understanding to consider it, along with other information including information about controls implemented by the State of Montana themselves, when assessing the risks of material misstatements the State of Montana's financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

*Ernst & Young LLP*

September 1, 2015

Philadelphia, Pennsylvania

## II. Xerox Business Services, LLC's Management Assertion

## Xerox Business Services, LLC's Management Assertion

We have prepared the description of Xerox Business Services, LLC's ("Xerox") Montana ("MT") Medicaid Management Information System (MMIS) ("Description") for the State of Montana during the period July 1, 2014 through June 30, 2015, and their user auditors who have a sufficient understanding to consider it, along with other information, including information about controls implemented by the State of Montana when assessing the risks of material misstatements of the State of Montana's financial statements. We confirm, to the best of our knowledge and belief, that:

- a. the Description fairly presents the MT MMIS system made available to State of Montana during some or all of the period July 1, 2014 through June 30, 2015, for processing their transactions. Xerox uses a sub-service organization for hosting of the MT MMIS online servers at the Xerox Data Center in Pittsburgh. Additionally, the provider enrollment function is supported by a sub-service organization, Digital Harbor, and Electronic Data Interchange ("EDI") is handled by the EDI Gateway. The description includes only the controls and related control objectives of Xerox and excludes the control objectives and related controls of the sub-service organizations. The criteria we used in making this assertion were that the description
  - i. presents how the system made available to the State of Montana was designed and implemented to process relevant transactions, including, if applicable:
    - 1) the types of services provided, including, as appropriate, the classes of transactions processed.
    - 2) the procedures, within both automated and manual systems, by which 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 the State of Montana.
    - 3) the related accounting records, supporting information, and specific accounts that are used to initiate, authorize, record, process, and report transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for the State of Montana.
    - 4) how the system captures and addresses significant events and conditions, other than transactions.
    - 5) the process used to prepare reports or other information for the State of Montana.
    - 6) the specified control objectives and controls designed to achieve those objectives, including as applicable, complementary user entity controls contemplated in the design of Xerox controls.
    - 7) other aspects of our control environment, risk assessment process, information and communication systems (including related business processes), control activities, and monitoring controls that are relevant to processing and reporting transactions of the State of Montana.
  - ii. does not omit or distort information relevant to the scope of the MT MMIS system.

- iii. includes relevant details of changes to MT MMIS system during the period covered by the description.
- b. the controls related to the control objectives stated in the Description, which together with the Complementary User Entity Controls and subservice organizations' controls referred to above, if suitably designed and operating effectively, were suitably designed and operating effectively throughout the period July 1, 2014 through June 30, 2015 to achieve those control objectives. The criteria we used in making this assertion were that
  - i. the risks that threaten the achievement of the control objectives stated in the description have been identified by management;
  - ii. the controls identified in the description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved; and
  - iii. the controls were consistently applied as designed, and manual controls were applied by individuals who have the appropriate competence and authority.

Xerox Business Services, LLC

September 1, 2015

## Management's Assertion Process

Xerox Management has developed and implemented a process, with the assistance of Xerox Internal Audit, to help ensure that management's assertion about whether, in all material respects, and based on suitable criteria,

- the description of the system fairly presents the system that was designed and implemented throughout the period.
- the controls related to the control objectives stated in the description of the system were suitably designed throughout the period to achieve those control objectives.
- the controls related to the control objectives stated in the description of the system operated effectively throughout the period to achieve those control objectives.

Management's assertion process was designed to leverage the knowledge and experience of many employees, including, but not limited to, senior management, business unit leaders, and control owners, and management utilized suitable criteria as the basis for the assertion as documented in the description of the system.

Through the assertion process, management evaluated the control objectives as part of the description of the system. Management also identified and documented the risks that could threaten achievement of the control objectives and the controls designed to mitigate those risks to an acceptable level to achieve the control objectives.

Monitoring of the controls is the process to assess the effectiveness of internal control performance over time. Management accomplishes monitoring of controls through ongoing activities, separate evaluations, or a combination of the two. Ongoing monitoring activities are often built into the normal recurring activities and include regular management and supervisory activities. Monitoring activities may also include using information communicated by external parties, such as customer complaints and regulator comments, which may indicate potential problems or highlight areas in need of improvement.

### III. Description of the System Provided by Xerox Business Services, LLC

## Overview of the Company

Since the invention of Xerography more than 75 years ago, the people of [Xerox](#) (NYSE: XRX) have helped businesses simplify the way work gets done. Today, Xerox is the global leader in business process and document management, helping organizations of any size be more efficient so they can focus on their real business. Headquartered in Norwalk, Conn., Xerox has more than 140,000 employees and does business in more than 180 countries, providing [business services](#), [printing equipment](#) and software for commercial and government organizations. Learn more at [www.xerox.com](http://www.xerox.com).

## Overview of Operations Related to Montana Medicaid Management Information System

The State of Montana receives federal funds for processing Medicaid claims according to its agreement with the Centers for Medicare and Medicaid Services (CMS), the cognizant federal agency for the Medicaid program. The client also has implemented certain additional business processes for processing claims for its residents that are eligible to receive Medicaid benefits. The Fiscal Agent responsibilities and the processing of data through the Medicaid Management Information System (MMIS) have been contracted to Xerox Montana; the client retains overall responsibility for funds availability and compliance with the federal regulations. Xerox Montana, as the Fiscal Agent, is subject to formal oversight and direction from the client in the conduct of its operations. An element of such oversight, as recommended by relevant federal regulations, is the SOC 1 report.

Furthermore, Xerox Montana's (Xerox MT) fiscal agent operations encompass all functional areas and business processes supporting the client's. The Director of Operations is responsible for ensuring all operational processes and desk level procedures are followed across the account. All key support areas for Xerox MT have documented desk procedures which support the processes. Each desk procedure is reviewed on a quarterly basis with the applicable updates being made. Updates to desk procedures are also completed at the time a change in process is made and the appropriate teams are educated on the change.

The MMIS system includes a repository of member demographic, eligibility, case, and other member information. Member management is the source of all member eligibility and demographic data for the MMIS. Member information contained on the MMIS supports claims processing, management and administrative reporting, other MMIS subsystems, and the information inquiry needs of providers. Enrollment operations are supported by personnel trained to perform tasks that facilitate the enrollment of providers who meet the qualifications and have passed the credentialing criteria set by the client to participate in the MT Medicaid program. The enrollment personnel are also responsible for the ongoing maintenance of the enrolled provider files.

# Relevant Aspects of the Control Environment, Risk Assessment Process and Monitoring

## Control Environment

### Integrity and Ethical Values

The mission of the Xerox Business Ethics and Compliance Office is to oversee our ethics and Code of Business Conduct policies and activities on behalf of our operating unit management, corporate management, and the Audit Committee of the Board of Directors to ensure that all our employees, and those working on behalf of Xerox, understand their obligation to uphold our values and to abide by our policies, laws and regulations.

Xerox has instituted a Xerox Corporate Ethics Program designed to instill a climate of integrity and ethical values, which are critical to the establishment and maintenance of an effectively controlled organization. The Xerox Business Ethics and Compliance Office communicates and disseminates ethics program materials, tracks and monitors ethics awareness and compliance training for each employee, while continuously evaluating and improving the ethics program effectiveness. The Business Ethics and Compliance Office also oversees an Ethics Helpline that is available globally 24 hours a day, seven days a week in multiple languages via a web-based reporting tool and toll-free telephone numbers.

The Xerox Code of Business Conduct serves as the foundation of the Company's ethics program. It embodies and reinforces our commitment to integrity and helps our people resolve ethics and compliance concerns consistent with our core values and legal and policy controls. Our Code of Business Conduct is available in 15 languages and accessible on our internal and external websites. The Code is aligned to our core values and covers policies and guidance on key topics including sales and marketing activities, controllership, insider trading, bribery, nondiscriminatory employment practices, privacy rights, human rights and environmental stewardship. The Code also specifies employees' obligations to report suspected ethical violations and reinforces our strong "no retaliation policy."

All employees are required to complete the Xerox Code of Business Conduct Training course upon employment, and must refresh their understanding and commitment to the Xerox Code of Business Conduct by completing training annually.

In addition to our global Code of Business Conduct, Xerox has a supplemental code of conduct for finance employees and a specific code of conduct for the Board of Directors. As a member of the Electronic Industry Citizenship Coalition, Xerox uses the Electronic Industry Code of Conduct (EICC) as our supplier code of conduct.

### Commitment to Competence

Our values and commitment to competence begin with Human Resources documentation of the employee hiring and promotion processes. Job descriptions are created and maintained for each key position. Further, our commitment to quality and competence is evidenced by the fact that the skills and knowledge base of employees are fairly monitored and evaluated and are supported by the employee review process, and staff training and development. Key management practices are incorporated into the performance appraisal process.

## **Xerox Management Audit Committee**

The Xerox Management Audit Committee (“Committee”) is a control monitoring process within Xerox. The Committee plays a significant role in our management process and is the cornerstone of the Company’s internal control monitoring process. The purpose of Committee is to ensure that 1) there exists a well-designed and implemented Internal Control Management Process, 2) controls are properly designed and operating effectively, 3) there is appropriate visibility and emphasis on significant control related issues aligned to the achievement of our business objectives, and 4) the impact of these controls ensures business changes including new systems are monitored through this process. Committee meetings are held 2-4 times per year by all significant Operating Units.

## **Human Resources Policies and Practices**

People are the key to our success and Human Resources is our people department. Its goal is to build an organization of excellent employees in an environment that encourages maximum development and professional growth. Xerox is committed to respecting and supporting one another, regardless of physical differences, beliefs or personal values. It is on the basis of this respect that all dealings with people are pursued. The commitment is expressed in our personnel policies and related Human Resource programs. This begins with the recruiting process, which is the joint responsibility of the Operations’ hiring managers and the Recruiting Department.

Xerox is an equal opportunity employer and Xerox is committed to an active non-discrimination program. Decisions on employment are made based on each individual’s qualifications and merit without regard to race, color, creed, religion, ancestry, national origin, age, gender/sex, marital status, sexual orientation, physical or mental disability, use of a guide dog or service animal, military/veteran status, citizenship status, the basis of genetic information, or any other group protected by Federal or State law or local ordinance. This approach extends to every phase of the employment process including recruiting, hiring, training, promotion, compensation, benefits, transfers, and company-sponsored educational, social and recreational programs. The department is committed to adding value to our community while providing exceptional customer service to every employee.

## **Risk Assessment Process**

Our Board of Directors oversees our Enterprise Risk Management (ERM) process which is designed to strengthen our risk-management capability and to assess, monitor and manage all categories of business risk, including strategic, operational, compliance and financial reporting. Our Chief Financial Officer is responsible for the Company’s ERM function through the Enterprise Risk Steering Committee which includes leaders from our Services and Document Technology segments as well as corporate functional leaders. The Enterprise Risk Steering Committee inspects risk mitigation plans and progress, identifies and addresses emerging risks, and shares mitigation best practices across the Company. Additionally, to ensure that ERM is fully integrated with our business management, our Management Committee, the Business Ethics and Compliance Board, and various Internal Control committees, monitor risk exposure and the effectiveness of how Xerox manages these risks.

While the Board of Directors has ultimate oversight responsibility for the risk management process, various committees of the Board have been delegated responsibility for certain aspects of risk management. The Audit Committee focuses on financial risk, including risks associated with internal controls, audit, financial reporting

and disclosure matters. At least quarterly, the Audit Committee discusses with management and our internal and external auditors these exposures, our policies with respect to risk assessment and risk management and the steps management has taken to monitor and control these exposures. In addition, the Compensation Committee seeks to incent employees in a manner that discourages unnecessary or inappropriate risk-taking, while encouraging a level of risk-taking behavior consistent with our business strategy.

## **Monitoring**

Within Xerox, ongoing monitoring includes regular management and supervisory activities, and other actions personnel take in performing their duties to meet Xerox Management Audit Committee and other Internal Control Management Process (ICMP) objectives. The Internal Control groups, reporting ultimately to the Chief Accounting Officer, are Senior Management's primary driver of these activities, although other monitoring activities, such as, rigorous operating results (FP&A) reviews, are driven by process owners.

## Information and Communication

### Information Systems

The following describes the Xerox State Healthcare MMIS data processing environment which supports the services provided. Automated and manual data processing procedures are in place to support the effectiveness of controls over the Healthcare MMIS Solution.

The Xerox primary hardware infrastructure is located at the Xerox Pittsburgh Data Center. The Montana Department of Public Health and Human Services has access to this system through a secure communications network provided by Xerox. The primary hardware configuration supporting the Montana MMIS Solution is a variety of IBM CMOS hardware utilizing MVS (Z/OS and OS/390) operating systems.

The State Healthcare MMIS Solution was developed by Xerox State Healthcare in order to meet the requirements of the Montana Department of Public Health and Human Services (DPHHS). The solution is a mainframe based application, interfacing with multiple trading partners, and connected to several subsystems.

### Information Systems Hardware and Software

User transactions in the Xerox MMIS environment are processed on an IBM CMOS mainframe utilizing MVS (Z/OS and OS/390) operating systems. The system software currently supporting the Xerox MMIS system includes, but is not limited to:

- CA ACF2 (“ACF2”)
- ASG-Zeke (“Zeke”)
- CA Endeavor (“Endevor”)
- CICS

### Communication

Xerox has implemented various methods of communication to ensure all employees understand their individual roles and responsibilities over transaction processing and controls and to ensure significant events are communicated in a timely manner. These methods include orientation and training programs for newly hired employees and the use of electronic mail messages to communicate time-sensitive messages and information. Managers also hold periodic staff meetings as appropriate.

Xerox has also implemented various methods of communication to ensure user entities understand the role and responsibilities Xerox has in processing their transactions and to ensure significant events are communicated to users in a timely manner. These methods include active participation in user meetings, as well as the designation of Department Manager, who maintain contact with designated user representatives to inform them of new issues and developments. User organizations also are encouraged to communicate questions and problems to their liaison, and such matters are logged and tracked until resolved, with the resolution also reported to the State of Montana.

## Control Objectives and Related Controls

### Change Management

Control Objective 1: Controls provide reasonable assurance that changes to applications and database software are authorized, tested, approved, properly implemented, and documented to protect data from unauthorized changes.

The MT MMIS account defines the following types of change requests, each falling under the authority of a change management process.

- Maintenance
- Enhancement

Formal requests for system enhancements are generated by the Department of Public Health and Human Services for the State of Montana or internally from employees of Xerox through customer service request (CSR) forms issued to the Xerox Systems Manager. The Xerox Systems Manager then reviews the CSR form, and assigns it to a programmer and business analyst. The review of the request along with the assignment of the ticket serves as authorization for the change. Development on the change occurs within Endeavor. Xerox uses the Endeavor version control tool to develop, test and migrate all changes to production.

Changes are developed in the development environment, and are tested in the staging environment. Changes are tested and verified by the requestor with the help of the development team. The Systems Manager reviews the results and the results are presented to the Change Control Board (CCB) for review and final approval for migration to production. The CCB meeting occurs weekly and consists of managers and supervisors at Xerox and the State. The CCB Approval of the change comes from the Department of Public Health and Human Services and the Xerox managers are copied on the approval.

Access to the production environment is limited to authorized personnel. Users with access to development have "Executor" access in Endeavor. Users with the ability to migrate changes have "Approver" access in Endeavor.

### Logical Access

Control Objective 2: Controls provide reasonable assurance that administrative and general user access to application and database resources is restricted to authorized and appropriate users.

For all Xerox Montana MMIS application access requests, the MMIS Systems Coordinator emails a Systems Access Control form to the Learning & Development Consultant/Trainer. The form includes the user's manager sign off indicating approval for the new user's access. The Learning & Development Consultant/Trainer reviews the Systems Access Control form to validate that appropriate approvals are present. For new users, an ACF2 ID Request Form is completed to request the creation of the mainframe ID. The completed ACF2 Request Form is emailed to the Xerox IT Help desk, who is responsible for creating the mainframe ID. Once the ACF2 ID is created, the Xerox IT Help Desk will email the information to the Learning & Development Consultant/Trainer. Upon receipt of the information, the Learning & Development Consultant/Trainer sets the security levels of access as requested. Once access is complete, the user log on credentials are emailed to the user and user's manager.

For user access modifications, a similar process is followed. However, the Xerox IT Help Desk is not required to create an ACF2 ID as an ID already exists within the MMIS System.

When a user is terminated, the user's manager emails the user's termination form to the Learning & Development Consultant/Trainer, who is responsible for changing the user status to 'D' or Delete in MMIS to revoke the user's access in MMIS. Additionally, the Learning & Development Consultant/Trainer notifies the IT Help Desk to request the removal of the terminated user's ACF2 access. Once the ACF2 access is removed, an email notification is sent to the user's manager confirming that the user's access has been revoked.

Authentication to the application requires a user to have a valid user ID and password. Password configurations are governed by Xerox Corporate Policy for all three layers.

A user access recertification is performed on a quarterly basis. The Services Technician Manager, extracts and sends an MMIS user listing to the managers responsible for reviewing user access to the MMIS System. The managers respond through email regarding whether user's access is appropriate or needs to be revoked or modified. Managers reply in 2 business days from the date the original email is sent to them. In the case any access needs to be modified or revoked, the same process is followed as that of a terminated user or a new/modified user where a user access form is filled out and the access is granted or revoked.

Access to modify user access is limited to privileged users within the MMIS System. Users with privileged access (e.g. the ability to add new users, modify access, and terminate accounts) must have 'U' access to screen menu 0, Security Code Maintenance, within MMIS. Requests for administrator level access follows the same process as the normal user process as described above. Administrator access is requested based on the user's job role and is approved by the user's manager.

## **Computer Operations**

Control Objective 3: Controls provide reasonable assurance that system processing is authorized and executed in a complete and timely manner, and deviations are identified and resolved in a complete and timely manner.

The mainframe job scheduling tool, Zeke, is used to schedule production and backup jobs for Montana MMIS. Changes to jobs are on an as needed basis. To request schedule changes to production and backup jobs, a Zeke Request Form needs to be filled out. Zeke request forms can be filled out for new jobs, jobs being deactivated, or changes to the frequency or timing of a job. Once completed, the form is then sent to Production Control within the Xerox Pittsburgh Data Center.

Access to modify the Zeke job schedule is limited to the Production Control team at the Pittsburgh Data Center. Changes to the Zeke tool are restricted to Xerox Pittsburgh Data Center personnel and the Xerox Montana team does not have this access.

All jobs are monitored by Production Control at the Xerox Pittsburgh Data Center. In the event of a job failure, the job can be resolved two ways:

- A failed production job or backup job can be resolved by the Production Control team at the Xerox Pittsburgh Data Center. The production control team receives an alert of the failed job and then investigates the issue and attempt to rerun the job until it is successfully resolved.

- If the Production Control team in the Xerox Pittsburgh Data Center is unable to resolve the failed production job or backup job, they notify the on-call Montana MMIS contact person for the particular job. The Pittsburgh Data Center contacts the on-call person by phone and then the Montana MMIS contact person investigates the failure until the job is rerun successfully.

## **Physical Access**

Control Objective 4: Controls provide reasonable assurance that physical access to resources within Xerox facilities is restricted to authorized and appropriate personnel.

Physical access, by electronic card entry, to the computer facilities in Helena is restricted and separate computer rooms are established to house the local area network servers, hubs and routers. The computer facility is also equipped with twenty-four (24) hour environmental monitoring. After hours and weekend access to the building in which Xerox MT is located is limited to authorized personnel by electronic card key access.

For both employees and visitors, access is not restricted by card reader with the exception of the computer, telecom and mail rooms. In order to access these rooms, the user would need to be assigned access to these rooms.

New user access to Xerox facilities are requested as part of the new hire request form (I9). Initiation of the request implies approval from the user's manager for the requested access. Based on the access requested, the IT Services staff will configure the user's key card based on the departments and areas the new user requires access to.

When a user is terminated from Xerox a formal request has to be submitted from the user's manager or supervisor. Once the termination request is received, IT Services staff will deactivate the user's key card and they will no longer have physical access to the Xerox facilities and are treated as a visitor. The key card is also collected from the employee upon termination.

A periodic review of physical access to the Xerox Montana facilities is performed quarterly. The review is initiated by the systems manager and performed by the QA manager on a quarterly basis.

Visitors to the Xerox Montana facilities are required to sign-in at the front desk prior to entry into the building.

## **Reference Files**

Control Objective 5: Control policies and procedures provide reasonable assurance that reference data is processed accurately and completely.

Approved Procedure Drug, Diagnosis, and DRG (PDDD) reference files are received either electronically (email) or physically via mail from the State. Each File Update Request (FUR) will include a unique FUR number to identify the request. The received form will detail any additions or changes that need to be made to a reference file record. Once the file is received, the Program Support department will manually look at the request to ensure all required fields and information is documented on the FUR. The form must accurately document the reference information being modified. If the form is missing the key information, it is sent back to the State for correction and will not be processed until the necessary information is received by Xerox. Each FUR and the related documentation is examined and evaluated by Quality Assurance (QA) personnel to verify the information for completeness and accuracy. After evaluation of the

information entered, the QA personnel sign off on a Quality Control (QC) form to validate that the PDDD updates are made correctly prior to being input into MMIS.

The Program Support department will key in the reference file information to be updated from the update form received. If any of the requested additions and/or changes were not entered into MMIS completely and accurately, an automated error message appears. This prevents the user from moving forward in the process until correct field values are entered. If there is an error with the additions/changes, it is communicated back to the State for clarification. The State is responsible for updating the document with the correct information and sending it back to Xerox for processing.

Once all the edits are cleared and entered successfully into MMIS, the PDDD reference files go through the QA process. The individual who performs the QA is independent of the submitter to ensure completeness and accuracy of the updates. The QA Department verifies that the updates mentioned in the request form are accurately depicted in the MMIS system. Once QA is complete the individual will sign off evidencing that updates were made accurately in MMIS. The Program Support Manager will then notify the State that all changes are complete and the request is closed.

## **Claims Processing**

Control Objective 6: Control policies and procedures provide reasonable assurance that claims data is processed accurately and completely.

To facilitate claim submissions by providers, claims are received by several methods. The Mail Room accepts and scans paper claims received by U.S. mail, courier and fax. Claims can also be entered electronically, via batch job, through Electronic Data Interchange (EDI). Completeness and accuracy of claims entered via EDI are handled by a third party vendor, EDI Gateway.

Once the claims are received, they are manually checked and reviewed by claims processing team personnel for key required fields such as a 'provider number'. Claim forms that are missing information and fields are sent back to the provider and marked as 'return-to-provider' (RTP).

Once claims are validated, they are sorted by type of claim such as institutional, nursing home, and dental, among other classifications. The claim status, type, and any errors detected in each of the claims are updated into an internal tool called OmniTrack. OmniTrack is used as a claims tracking tool. The claims are then grouped by type of claim so they can be input into MMIS in batches.

Manually received claims are scanned and imaged through an Optical Character Recognition (OCR) scanner in batches. The OCR converts the images into machine-encoded text using the Recognition Research Incorporated (RI) tool. These claims are uploaded into MMIS twice a week, every Monday and Wednesday, where the claims imaged from the OCR are uploaded into MMIS through a batch upload job process.

On a weekly basis, the Quality Assurance (QA) team randomly selects a sample of claims to review. The QA personnel review the claims for accuracy and completeness. The QA personnel compare the information in the claim forms against the information uploaded into MMIS. Once the claim has been successfully verified and reviewed, the QA personal signs off on a quality control form evidencing the QA review of completeness and accuracy of the claim. Any mismatch or discrepancies is investigated and resolved. Once the discrepancy is resolved, the QA personal signs off on a quality control form evidencing the review.

Claims are processed against various edit and audit checks agreed upon with the State and designated in MMIS system via defined business rules during the adjudication process. During this phase MMIS automatically calculates the payment amount based on benefit and eligibility information, and automatically scans the claims and key fields for any errors, missing fields or incorrect fields entered. This validation process captures items that do not meet business rule eligibility requirements based on client issued reference files programmed into MMIS such as third party liability and Medicare specifications.

Suspended claims are those which have not finalized due to any number of issues, including errors by the provider, claims data omission, or questionable medical necessity. Claims personnel work suspended claims to resolution.

## **Provider Enrollment**

Control Objective 7: Control policies and procedures provide reasonable assurance that providers are properly authorized and that provider transactions are processed completely, accurately and timely.

The MT MMIS Health Enterprise Provider subsystem supports the entry, maintenance and reporting of current and historical information for all providers who participate in the Medicaid program. This subsystem facilitates provider participation and retention, and maintains security and control over all provider-related data.

MMIS utilizes the provider file to verify that the provider is enrolled with an active license for the category of service and dates of service. It is also used to verify any special restrictions for the provider for the service dates. For each edit that fails, an exception code is posted and the claim is adjudicated according to the exception disposition code.

Providers are enrolled into the State Healthcare Programs system by submitting a Provider enrollment application either on paper or through the web portal to the Provider Relations Department. The provider application website captures and validates all required information from providers and automatically triggers error messages if key fields are not populated accurately and according to field types. The provider enrollment application can only progress if there are no pending error messages.

Paper enrollments are entered by Provider Relations Department through the web portal. The form is reviewed for completeness and accuracy as well as verification of the status of the provider's license, if required. The Provider Relations department reviews the OIG (Office of Inspector General) web site, the Medicare Exclusions Database and the GSA Excluded Parties List System for a sanctions list as part of the enrollment process. The enrolling provider, all owners, managing employees and other entities listed on the enrollment application are reviewed for sanctions in the data bases listed above.

Upon receipt of the executed agreement, Xerox reviews the agreement and approves the enrollment in the Enterprise Provider Subsystem. MMIS assigns a unique provider number utilizing numeric digits. The application and supporting detail is forwarded to the State, if State approval is required. The State approves the application and returns to Xerox. On certain providers, the State also assigns provider rates. A Xerox staff member keys in the appropriate provider information that is reviewed by QA personnel for accuracy. The QA department reviews all provider file changes. All new provider applications and supporting detail are maintained in a provider file.

For out of state providers, if a provider's license expires and the renewed license is not forwarded, Xerox issues a State approved series of letters requesting licensure prior to

termination or cancellation of the provider's enrollment. For in state providers, a monthly report is generated by MMIS of all providers whose certification date ends during the month. Xerox Provider Relations staff accesses the appropriate provider type licensure board (Montana Department of Labor and Industry website) to validate licensure. During the licensure verification process, the sanction web sites are reviewed for sanctions related to the provider, the managing employees, owners and other entities listed in the provider files.

Xerox has implemented a process to automate the inquiries of exclusion data bases and licensure information into a single electronic request. This process uses a tool called Know your Provider (KYP) to review provider and owner information against accumulated data sources to determine if the provider is eligible to participate in the program. These data sources include OIG excluded provider listing and some licensure databases. KYP is administered by a third party vendor, Digital Harbor.

Only authorized individuals have access to update provider enrollment information. Users with "U" access to the Provider Subsystem in MMIS have access to update provider information.

If an update needs to be made to the provider's profile, a formal letter on the provider's letterhead with a wet signature is needed requesting the change. The provider must provide their Provider Number, Taxonomy Number and/or their Social Security Number so they can be uniquely identified within the system.

### **Passport Provider File**

The State has contracted with Xerox to recruit Passport to Health providers in each county. The provider must be a current Medicaid provider to be eligible to become a Passport to Health provider

When an eligible provider applies to participate as a Passport to Health provider, the Xerox Passport Provider Lead processes the application to determine that all necessary information is included. When the application is complete it is entered into MMIS. The provider is assigned a unique Passport to Health provider number systematically, utilizing consistent and random numbers. Once the Passport to Health provider number is assigned, it is immediately placed in an inactive status so the Passport to Health number cannot be used to submit Medicaid claims.

### **Plan Benefit Parameters**

Control Objective 8: Procedures exist to ensure benefit parameters agree with the established plan criteria and any updates are approved by authorized personnel and the State.

Plan Benefit parameters and pricing file updates are sent to Xerox by the State via a new/update form to managed care plans or any other specific plan packages updates. Forms are manually input into the system by the Registered Health Information Administrator (RHIA). There are edit and validation checks that ensure input is entered correctly. In the case that any of the fields are incorrect or any key fields are missing, the system generates an automated error message and does not allow the user to move forward in the system with the plan benefit input. Upon entry the updates are reviewed to confirm valid data is input into MMIS by the RHIA.

The access to create, update, and remove plans and pricing file records is restricted to the RHIA team.

Once plan benefit parameter creations or updates are made, QA personnel review the information in MMIS against the creation or update form submitted. The individual who performs the QA is independent of the submitter to ensure completeness and accuracy of the updates. The QA Analyst verifies that the updates mentioned in the request form are accurately depicted in the MMIS system. Once the QA is complete the individual will sign off evidencing that updates were made accurately in MMIS.

### **Passport Case Management Cycle**

The Passport to Health Case Management generation process examines each client who has an enrollment record. The system searches for a date span encompassing the current enrollment period possessing a valid plan code and plan provider number. If all criteria are met, then a Passport to Health Case Management claim is systematically generated.

The Passport to Health Case Management generation process performs the following functions:

- Produces Passport to Health Case Management claims.
- Maintains a Passport to Health Case Management history file.

Passport to Health Case Management generation occurs monthly on the Tuesday before the first Wednesday payment cycle of the month. A valid, successful managed care eligibility update results in a Passport to Health Case Management claim.

The Passport to Health Case Management generation process creates Passport to Health Case Management claims for all eligible clients. After their creation, the Passport to Health Case Management and fee for service (FFS) claims are processed together in the next payment cycle. The system will generate a Passport to Health Case Management claim in advance for each client that has a rate and is enrolled for the next month. This system-generated Passport to Health Case Management claims are subjected to duplicate claim and other history-related edits. Passport to Health Case Management claims pass through the same edits that FFS claims go through, such as data validity, provider edits, client eligibility and pricing.

Passport to Health Case Management rates are determined by the State. The rate may be changed annually or as needed by the State. Client eligibility information in managed care is received through the file transfer protocol process from the State's eligibility system. The RHIA updates the plan of benefit file at the request of the State.

## Complementary User Entity Controls

The Xerox processing of transactions and the controls over transaction processing related to the Xerox State Healthcare MMIS system were designed with the assumption that certain controls would be placed in operation at the user entity. The application of such controls by user entity is necessary to achieve certain control objectives identified in this report. In addition, there may be control objectives and related controls that are not identified in this report that would be appropriate for the processing of user entity transactions.

This section describes additional controls that should be in operation at user entity to complement the controls at Xerox. The user control considerations identified below should not be considered as a comprehensive list of all controls to which the Xerox user entity should adhere:

### **Control Objective 1**

- Controls should be established to ensure that state requested changes made by Xerox are authorized, tested, and approved prior to migration.

### **Control Objective 2**

- Controls should be established to ensure that only authorized users from the user entity have access to the MT MMIS system.
- Controls should be established to ensure that the user entity is responsible for authorizing and approving their employees' access to the MT MMIS portal.
- Controls should be established to ensure that the user entity firewalls are installed and configured to restrict unauthorized access to the MT MMIS network from external resources.
- Controls should be established to ensure that the user entity has controls in place regarding the encryption of participant data (using HTTPS SSL –secured socket layer protocol) transmitted between an end user's qualified Web browser and the MMIS application.

### **Control Objective 3**

- Controls should be established to ensure that access to the client enrollment master data file is restricted to appropriate personnel.
- Controls should be established to ensure that information sent inbound and outbound interface files are complete and accurate.

### **Control Objective 5**

- Controls should be established to ensure that the user entity is reviewing and validating any rate changes or changes to master files.
- Controls should be established to ensure complete and accurate reference file update documentation is submitted to Xerox.

### **Control Objective 6**

- Controls should be established to ensure that access to the claim processing master data file is restricted to appropriate personnel.

**Control Objective 7**

- Controls should be established to ensure that the user entity are reviewing and approving provider requested services prior to services being performed.

# IV. Xerox Business Services, LLC's Control Objectives, Related Controls, and the Independent Service Auditor's Description of Tests of Controls and Results

## Control Objectives, Related Controls, and Results of Testing

### **Testing Performed and Results of Tests of Entity Level Controls**

In planning the nature, timing and extent of its testing of the controls specified by Xerox, Ernst & Young LLP considered the aspects of the Xerox control environment, risk assessment processes, communication and management monitoring procedures and performed such procedures as we considered necessary in the circumstances.

### **Control Objectives and Related Controls**

On the pages that follow, the description of control objectives and the controls to achieve the objectives have been specified by Xerox and are the responsibility of Xerox. The testing performed by Ernst & Young LLP and the results of tests are the responsibility of the service auditor.

## Change Management

Control Objective 1: Controls provide reasonable assurance that changes to applications and database software are authorized, tested, approved, properly implemented, and documented to protect data from unauthorized changes.			
Control Number	Description of Controls Specified by Xerox	Tests of Operating Effectiveness	Test Results
1.1	Change requests are documented and approved through a change management process.	Inquired of management to determine that all change requests are documented and approved through a formal change management process prior to being implemented.	No deviations noted
		For a sample of changes, inspected evidence to determine whether changes are documented and approved through a formal change management process prior to being implemented.	No deviations noted
1.2	Changes are tested and approved prior to being moved into a production environment.	Inquired of management to determine whether changes are tested and approved through a formal change control process prior to being implemented.	No deviations noted
		For a sample of changes, inspected evidence to determine whether changes are tested and approved prior to being moved into a production environment.	No deviations noted
1.3	Access to the production environment is limited to authorized personnel based on job responsibilities.	Inquired of management to determine whether access to the production environment is limited to authorized Xerox personnel based on job title and responsibilities.	No deviations noted
		For Xerox users with access to the MT MMIS production environment, inspected screenshots and validated that access to the production environment is limited to authorized personnel based on job responsibilities.	<p>Deviations noted.</p> <p>Three (3) of 16 users with approval access in Endeavor were terminated users. It was confirmed that the identified users did not access the system after their termination date.</p> <p>Refer to Section V for Management's Response.</p>

**Control Objective 1: Controls provide reasonable assurance that changes to applications and database software are authorized, tested, approved, properly implemented, and documented to protect data from unauthorized changes.**

Control Number	Description of Controls Specified by Xerox	Tests of Operating Effectiveness	Test Results
1.4	The software version control tool only allows programs to be checked out by one programmer at a time.	Inquired of management and inspected the system to determine that MT MMIS software version control tool only allows programs to be checked out by one programmer at a time.	No deviations noted
1.5	The software version control tool requires two approvals prior to changes being migrated to production	Inquired of management and inspected the system to determine software version control tool requires two approvals prior to changes being migrated to production. In addition, for a sample change observed in the system that two approvals were required prior to the change being migrated to production.	No deviations noted

## Logical Access

Control Objective 2: Controls provide reasonable assurance that administrative and general user access to application and database resources is restricted to authorized and appropriate users.			
Control Number	Description of Controls Specified by Xerox	Tests of Operating Effectiveness	Test Results
2.1	Administrator level access to application and database resources must be approved by an authorized individual.	Inquired of management to determine that administrator level access to application and database resources must be approved by an authorized individual.	No deviations noted
		For all administrator level access to the application and database, validated access was appropriate by inspecting documentation evidencing approval from an authorized individual.	No deviations noted
2.2	User access to application and database resources must be approved by an authorized individual.	Inquired of management to determine whether access to in scope production systems is documented and properly approved.	No deviations noted
		For a sample of Xerox users who were granted access to the in scope application (MT MMIS) and database, we inspected user access documentation to determine whether user access was properly documented and approved by an authorized individual.	No deviations noted
2.3	<p>Passwords for the systems are required to comply with established Xerox or client policies. The password requirements include:</p> <ul style="list-style-type: none"> <li>• Expiration,</li> <li>• Minimum Length,</li> <li>• History,</li> <li>• Complexity, and</li> <li>• Lockout after unsuccessful login attempts</li> </ul>	Inquired of management and inspected the system to determine whether password configurations for the in scope application and related database comply with established Xerox policies.	<p>Deviation noted.</p> <p>The password history setting for MMIS was enabled; however, the current setting did not meet the corporate password policy.</p> <p>Refer to Section V for Management's Response.</p>
2.4	Administrator and general user access to application and database resources is removed upon notification of termination.	Inquired of management to determine whether Xerox user access to the in scope application (MT MMIS) and database, is removed upon notification of termination.	No deviations noted

**Control Objective 2: Controls provide reasonable assurance that administrative and general user access to application and database resources is restricted to authorized and appropriate users.**

Control Number	Description of Controls Specified by Xerox	Tests of Operating Effectiveness	Test Results
		<p>For a sample of terminated Xerox users, inspected email notifications and system user listings to determine whether access to the in scope application (MT MMIS) and the related database application was removed upon notification of termination.</p>	<p>No deviations noted</p>
2.5	<p>Administrator and general user access to application and database resources is reviewed on a periodic basis.</p>	<p>Inquired of management to determine whether users' access to MMIS and the related system resources are reviewed/ recertified on a periodic basis. For a sample quarter, inspected email evidence to support the completion of the review.</p>	<p>Deviation noted</p> <p>The periodic review /recertification of the MMIS user access was not fully completed. Responses from five (5) of the eight (8) managers were not received.</p> <p>Refer to Section V for Management's Response.</p>

## Computer Operations

Control Objective 3: Controls provide reasonable assurance that system processing is authorized and executed in a complete and timely manner, and deviations are identified and resolved in a complete and timely manner.			
Control Number	Description of Controls Specified by Xerox	Tests of Operating Effectiveness	Test Results
3.1	Requests for production job schedule changes are documented, reviewed and approved through a formal change control process prior to the job being scheduled.	Inquired of management to confirm whether production job schedule changes are documented, reviewed and approved through a formal change control process prior to the job being scheduled.	No deviations noted
		For a sample of changes to the production job schedule, inspected evidence to determine whether the change requests were documented, reviewed and approved prior to being implemented.	No deviations noted
3.2	Production jobs are monitored for success or failure, and failed jobs are tracked to resolution.	Inquired of management to determine that production jobs are monitored for success or failure, and failed jobs are tracked to resolution.	No deviations noted
		For a sample of dates, obtained evidence of the daily scheduled job history showing all successfully completed and failed jobs. For any identified failures, inspected support evidence to determine whether the failures were escalated to resolution.	No deviations noted
3.3	Access to job schedulers is restricted to authorized personnel through the use of usernames and passwords, which are configured to comply with password policies.	Inquired of management to determine whether access to the job scheduler is limited to authorized Xerox personnel based on job title and responsibilities.	No deviations noted
		Inspected the list of Xerox users with access to the job scheduler and validated that access is limited to authorized Xerox personnel based on job title and responsibilities.	No deviations noted

## Physical Access

Control Objective 4: Controls provide reasonable assurance that physical access to resources within Xerox facilities is restricted to authorized and appropriate personnel.			
Control Number	Description of Controls Specified by Xerox	Tests of Operating Effectiveness	Test Results
4.1	Access to Xerox facilities is restricted to authorized employees via card key readers.	Inquired of management and observed people accessing the facility to determine whether access to Xerox facilities is restricted to authorized employees via card key readers.	No deviations noted
4.2	Requests for new access to Xerox facilities are authorized and approved by an authorized individual.	Inquired of management to understand how the physical access provisioning process is performed.	No deviations noted
		For a sample of new employees, inspected supporting documentation and access lists to determine whether new employees' access to the Xerox facilities were approved and authorized.	No deviations noted
4.3	Employee access to Xerox facilities is removed upon notification of termination.	Inquired of management to understand the physical access deprovisioning process.	No deviations noted
		Inspected a sample of terminated users to validate that physical access removal process including badge access removal process occurred timely.	No deviations noted
4.4	Access to Xerox facilities is reviewed on a periodic basis.	Inquired of management as to whether access to Xerox facilities is reviewed on a periodic basis.	No deviations noted
		For a sample of quarters, inspected supporting documentation to determine whether managers reviewed access to the Xerox facilities to verify that all personnel with access are appropriate.	<p>Deviations noted</p> <p>The quarterly physical access reviews were not performed. However, access as of June 30, 2015 was validated with the users' managers as authorized and appropriate.</p> <p>Refer to Section V for Management's Response.</p>

**Control Objective 4: Controls provide reasonable assurance that physical access to resources within Xerox facilities is restricted to authorized and appropriate personnel.**

<b>Control Number</b>	<b>Description of Controls Specified by Xerox</b>	<b>Tests of Operating Effectiveness</b>	<b>Test Results</b>
4.5	Visitors to Xerox facilities are required to sign in at the front desk.	Inquired of management and inspected the visitor's log to determine whether visitors to the Xerox facilities are required to sign in and be escorted by Xerox personnel.	No deviations noted

## Reference Files

Control Objective 5: Control policies and procedures provide reasonable assurance that reference data is processed accurately and completely.			
Control Number	Description of Controls Specified by Xerox	Tests of Operating Effectiveness	Test Results
5.1	All PDD (Procedures, Drug, and Diagnosis) files and updates are entered into MMIS upon authorized approval and validated by QA.	Inquired of management to determine the process for adding/updating PDD files, and observed management enter information upon authorized approval and inquired about the QA process and observed evidence of the QA being performed.	No deviations noted
		For a sample of PDD changes, inspected evidence to determine whether PPD updates were entered appropriately and observed evidence and validated QA review was performed.	No deviations noted
5.2	PDD (Procedures, Drug, and Diagnosis) files are reviewed by the QA team for completeness and accuracy. Any discrepancies resulting from the review are investigated and resolved.	Inquired of management to determine the process for reviewing PDD (Procedures, Drug, and Diagnosis) files updates.	No deviations noted
		For a sample of PDD file updates, inspected evidence to determine whether PPD files were reviewed by the QA department and any discrepancies were investigated and resolved.	No deviations noted
5.3	Edit/validation checks are in place for key data entry fields when inputting PDD (Procedures, Drug, and Diagnosis) files additions/updates into MMIS. Any failures resulting from the edit/validation checks are suspended from further processing until resolved.	Inquired of management to determine whether edit/validation checks are in place for the key data entry fields and that any claims with failures resulting from the checks are suspended from further processing until resolution.	No deviations noted
		Observed a Xerox representative enter invalid information in a sample of fields in MT MMIS and verified that the system displayed error messages and suspended the updates until resolution.	No deviations noted

**Control Objective 5: Control policies and procedures provide reasonable assurance that reference data is processed accurately and completely.**

Control Number	Description of Controls Specified by Xerox	Tests of Operating Effectiveness	Test Results
5.4	Access to update PDD (Procedures, Drug, and Diagnosis) files is limited to authorized personnel.	Inquired of management to determine that access to update PDD files is limited to authorized personnel.	No deviations noted
		Inspected the user access listing to validate access to update PDD files is limited to authorized personnel who require access as part of their job function.	No deviations noted

## Claims Processing

Control Objective 6: Control policies and procedures provide reasonable assurance that claims data is processed accurately and completely.			
Control Number	Description of Controls Specified by Xerox	Tests of Operating Effectiveness	Test Results
6.1	All claims are entered and processed in MMIS. Any errors are logged and tracked to resolution.	Inquired of management to determine whether all claims are processed completely and accurately and any errors are logged and tracked to resolution.	No deviations noted
		For a sample of claims, inspected documentation to determine whether they were processed completely and accurately.	No deviations noted
6.2	Claims are reviewed weekly by the QA team for completeness and accuracy. Any discrepancies resulting from the review are investigated and resolved.	Inquired of management to determine whether claims are reviewed weekly by the QA team for completeness and accuracy and any discrepancies are investigated and resolved.	No deviations noted
		For a sample of claims, observed the QA form and procedures to validate completeness and accuracy and in the case there was a discrepancy observed that it was investigated and resolved.	No deviations noted
6.3	Edit/validation checks are in place for key data entry fields to validate accuracy and completeness of claims. Failures resulting from the edit/validation checks are suspended from further processing until resolved.	Inquired of management to determine whether edit/validation checks are in place for the key data entry fields to validate accuracy and completeness of claims submissions and that input failures result in suspension until resolution.	No deviations noted
		For a sample of claims, observed the edit/validation checks being performed and, when an error occurred as a result, observed the corresponding error message generated and confirmed the claim was suspended from further processing.	No deviations noted
6.4	The 'pay to provider' cannot be changed once a claim is in the to-be-paid status.	Inquired of management and observed MMIS system deny access to change the 'pay to provider' once the claim is in the to-be-paid status.	No deviations noted

**Control Objective 6: Control policies and procedures provide reasonable assurance that claims data is processed accurately and completely.**

Control Number	Description of Controls Specified by Xerox	Tests of Operating Effectiveness	Test Results
6.5	Claims payment amounts are automatically calculated by MMIS based on benefit and eligibility information defined by the MMIS system.	Inquired of management to determine whether claims payment amounts are automatically calculated based on benefit and eligibility information defined by the MMIS system.	No deviations noted
		For a sample of claims, we validated the claims payment amount was automatically calculated based on benefit and eligibility information defined by the MMIS system.	No deviations noted

## Provider Enrollment

Control Objective 7: Control policies and procedures provide reasonable assurance that providers are properly authorized and that provider transactions are processed completely, accurately and timely.			
Control Number	Description of Controls Specified by Xerox	Tests of Operating Effectiveness	Test Results
7.1	Edit/validation checks are in place for key data entry fields to validate accuracy and completeness of provider enrollment. Failures resulting from the edit/validation checks are suspended from further processing until resolved.	Inquired of management and observed the MMIS system to determine whether edit/validation checks are in place for the key data entry fields.	No deviations noted
7.2	Only authorized individuals have access to update provider enrollment information.	Inquired of management and observed system generated access listing to determine whether authorized individuals have access to update providers within the MT MMIS system.	No deviations noted
7.3	Provider file updates (enrollment status, address changes, license effective dates, etc.) are entered into MMIS upon authorized approval.	Inquired of management to determine the process to update provider enrollment.	No deviations noted
		For a sample of provider file updates, inspected evidence to determine whether information was approved and entered completely and accurately.	No deviations noted

## Plan Benefit Parameters

Control Objective 8: Procedures exist to ensure benefit parameters agree with the established plan criteria and any updates are approved by authorized personnel and the State.			
Control Number	Description of Controls Specified by Xerox	Tests of Operating Effectiveness	Test Results
8.1	Plan benefits are input into MMIS upon authorized approval.	Inquired of management to determine that plan benefits are input into MMIS completely and accurately upon authorized approval.	No deviations noted
		For a sample of plan benefit files, inspected evidence to validate the updates were made completely and accurately upon authorized approval.	No deviations noted
8.2	Pricing file updates are input into MMIS upon authorized approval.	Inquired of management to determine that pricing file updates are input into MMIS completely and accurately upon authorized approval.	No deviations noted
		For a sample of pricing files, inspected documentation to validate the updates were made completely and accurately upon authorized approval.	No deviations noted
8.3	All updates to the pricing files are reviewed for completeness and accuracy by the Quality Assurance department. Any discrepancies resulting from the review are investigated and resolved.	Inquired of management to determine that all updates to the pricing files are reviewed for completeness and accuracy by the Quality Assurance department and any discrepancies are investigated and resolved.	No deviations noted
		For a sample of pricing file updates, validated the QA review process and verified any discrepancies were investigated and resolved.	The circumstances that required the control to operate did not occur. As a result, no testing was performed.

## V. Other Information Provided by Xerox Business Services, LLC

## Management Response to Testing Deviations

The service auditor has reported certain deviations in performing its test of operating effectiveness of controls in the section above titled "Control Objectives, Related Controls, and Results of Testing". Xerox performed certain additional steps with respect to the identified deviations as reported below.

### Change Management

Control objective 1: Controls provide reasonable assurance that changes to applications and database software are authorized, tested, approved, properly implemented, and documented to protect data from unauthorized changes.

Control Number	Description of Controls Specified by Xerox	Deviation Noted	Management Response
1.3	Access to the production environment is limited to authorized personnel and appropriate based on job responsibilities.	Three (3) of 16 users with approval access in Endeavor were terminated users. It was confirmed that the identified users did not access the system after their termination date.	Xerox MT validated the users did not access the system and validated the access was removed as of June 23, 2015.

### Logical Security

Control Objective 2: Controls provide reasonable assurance that administrative and general user access to application and database resources is restricted to authorized and appropriate users.

Control Number	Description of Controls Specified by Xerox	Deviation Noted	Management Response
2.3	<p>Passwords for the systems are required to comply with established Xerox or client policies. The password requirements include:</p> <ul style="list-style-type: none"> <li>• Expiration,</li> <li>• Minimum Length,</li> <li>• History,</li> <li>• Complexity, and</li> <li>• Lockout after unsuccessful login attempts</li> </ul>	The password history setting for MMIS was enabled; however, the current setting did not meet the corporate password policy.	Xerox MT noted the remaining suite of password controls were aligned to Corporate password policy. Xerox MT MMIS password history setting was changed to align with the Corporate password policy as of July 24, 2015.

Control Number	Description of Controls Specified by Xerox	Deviation Noted	Management Response
2.5	Administrator and general user access to application and database resources is reviewed on a periodic basis.	The periodic review /recertification of the MMIS user access was not fully completed. Responses from five (5) of the eight (8) managers were not received.	For Q4, Xerox MT reviewed the entire list of terminations and additions and deemed all users were authorized and appropriate.  Beginning September 1, 2015, Xerox MT will use role based access for all new employees and effective January 1, 2016 all users access will be assigned to a particular role. In addition, MMIS access will be reviewed on a quarterly basis.

## Physical Access

Control Objective 4: Controls provide reasonable assurance that physical access to resources within Xerox facilities is restricted to authorized and appropriate personnel.

Control Number	Description of Controls Specified by Xerox	Deviation Noted	Management Response
4.4	Access to Xerox facilities is reviewed on a periodic basis.	The quarterly physical access reviews were not performed. However, access as of June 30, 2015 was validated with the users' managers as authorized and appropriate.	Xerox MT validated all access to the facility as of June 30, 2015 and access was deemed authorized and appropriate for all individuals. Moving forward, Xerox MT will conduct a review every quarter pursuant to a new process that was adopted as of June 30, 2015.

## Business Continuity and Disaster Recovery

Xerox State Healthcare has in place a written disaster recovery plan. The data center management and system management teams are responsible for assuring that plans are updated at least annually. The written plan is divided into team sections with each team section containing specific procedures for bringing their teams area of expertise back online. The plan utilizes a "hot site" which is equipped for both voice and data communications to ensure rapid re-establishment of data processing capability following a disaster. In the event of a disaster, the teams will manage their respective disaster related activities and monitor the continuation of business processing and services.