Description of Novologix's Medical Prior Authorization and Medical Claims Editing System

SOC 1® Report

For the period October 1, 2018 through September 30, 2019

TABLE OF CONTENTS

Section I. Independent Service Auditor's Report

Ernst & Young LLP
200 Clarendon Street
Boston, Massachusetts
02116

Tel: +1 617 266 2000
ey.com

Building a better working world

INDEPENDENT SERVICE AUDITORS' REPORT

The Board of Directors
CVS Health

Scope

We have examined Novologix, L.L.C.'s (Novologix), a wholly owned indirect subsidiary of CVS Health, description entitled "Management's Description of its Novologix Medical Prior Authorization and Medical Claims Editing System" (Description) throughout the period October 1, 2018 to September 30, 2019 of its Medical Benefit Management (MBM) system (System) for processing user entities' transactions and the suitability of the design and operating effectiveness of controls described therein to achieve the related control objectives stated in the Description (Control Objectives), based on the criteria identified in Management's Assertion on its Novologix Medical Prior Authorization and Medical Claims Editing System (Assertion). The Control Objectives and controls included in the Description are those that management of Novologix believes are likely to be relevant to user entities' internal control over financial reporting, and the Description does not include those aspects of the System that are not likely to be relevant to user entities' internal control over financial reporting.

The Description indicates that certain Control Objectives can be achieved only if complementary user entity controls assumed in the design of Novologix'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.

The information included in Section V - Other Information Provided by Novologix, L.L.C. is presented by management of Novologix to provide additional information and is not a part of Novologix's Description. Information about Novologix's health insurance portability and accountability act, disaster recovery, business continuity plans, emergency management plan, and trademarks has not been subjected to the procedures applied in our examination of the description of the System and of the suitability of the design and operating effectiveness of controls to achieve the related Control Objectives, and, accordingly we express no opinion on it.

Novologix's responsibilities

Novologix has provided the accompanying assertion titled, Management's Assertion on its Novologix Medical Prior Authorization and Medical Claims Editing System (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. Novologix 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 that are suitably designed and operating effectively to achieve the related Control Objectives.

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, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, 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 throughout the period October 1, 2018 to September 30, 2019. We believe that the evidence we have 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, 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.
- Testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related Control Objectives were achieved.
- Evaluating the overall presentation of the Description, the suitability of the Control Objectives, and the suitability of the criteria specified by the service organization in the 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 the accompanying "Section IV. Description of Control Objectives and Related Controls, and Tests of Controls and Test Results" (Description of Tests and Results).

Opinion
In our opinion, in all material respects, based on the criteria described in Novologix's Assertion:

a. the Description fairly presents the System that was designed and implemented throughout the period October 1, 2018 to September 30, 2019.

b. the controls related to the Control Objectives were suitably designed to provide reasonable assurance that the Control Objectives would be achieved if the controls operated effectively throughout the period October 1, 2018 to September 30, 2019.

c. the controls operated effectively to provide reasonable assurance that the Control Objectives were achieved throughout the period October 1, 2018 to September 30, 2019.

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 management of Novologix, user entities of Novologix's System during some or all of the period October 1, 2018 to September 30, 2019, 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 misstatements of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than these specified parties.

Ernst & Young LLP

November 21, 2019
Boston, Massachusetts

Section II. Management's Assertion on its Novologix Medical Prior Authorization and Medical Claims Editing System

Management's Assertion on its Novologix Medical Prior Authorization and Medical Claims Editing System

November 21, 2019

We have prepared the description of Novologix, L.L.C.'s (Novologix) a wholly owned indirect subsidiary of CVS Health, Medical Benefit Management (MBM) system entitled, "Management's Description of its Novologix Medical Prior Authorization and Medical Claims Editing System" (Description) for processing user entities' transactions throughout the period October 1, 2018 to September 30, 2019, for user entities of the system during some or all of the period October 1, 2018 to September 30, 2019, 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 the Description, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements.

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 Novologix'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:

a. The Description fairly presents the Novologix Medical Prior Authorization and Medical Claims Editing system (System) made available to user entities of the System during some or all of the period October 1, 2018 to September 30, 2019 for processing their transactions through its Novologix Medical Prior Authorization and Medical Claims Editing system as it relates to controls that are likely relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the Description:

(1) Presents how the System made available to user entities of the system, was designed and implemented to process relevant transactions, including, if applicable:

- The types of services provided, including, as appropriate, the classes of transactions processed.
- 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.
- 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 prepared for user entities.

- How the System captures and addresses significant events and conditions, other than transactions.
- The process used to prepare reports and other information for user entities.
- 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.
- The specified control objectives and controls designed to achieve those objectives, including, as applicable, complementary user entity controls assumed in the design of Novologix's controls.
- Other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring activities that are relevant to the services provided, including processing and reporting transactions of user entities.

(2) Includes relevant details of changes to the System during the period covered by the Description.

(3) 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 System that each individual user entity of the System and its user auditor may consider important in the user entity's own particular environment.

b. The controls related to the control objectives stated in the Description were suitably designed and operated effectively throughout the period October 1, 2018 to September 30, 2019 to achieve those control objectives, if subservice organizations applied the complementary subservice organization controls and user entities applied the complementary user entity controls assumed in the design of Novologix controls throughout the period October 1, 2018 to September 30, 2019. The criteria we used in making this assertion were that:

(1) The risks that threaten the achievement of the control objectives stated in the Description have been identified by management of the service organization.

(2) 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

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

The Management of Novologix, L.L.C.
Wholly owned indirect subsidiary of CVS Health

Section III. Management's Description of its Novologix Medical Prior Authorization and Medical Claims Editing System

Description of Novologix Medical Prior Authorization and Medical Claims Editing System

CVS Health provides certain medical benefit management (MBM) services through its specialty pharmacy business division (CVS Specialty), which includes the Novologix System, delegated prior authorization review (performed by the case review unit (CRU)), medical rebates, site of care and other. CVS Specialty also provides pharmacy and other therapeutic services for plan members with rare and/or complex conditions. The Novologix System and other services offered by Novologix fall under CVS Specialty's MBM services. This report focuses on the Novologix System, and this section provides a description of the various components that comprise that System.

3.1 Organizational Background

CVS Specialty's operations are conducted primarily through two CVS Health operating subsidiaries, Caremark, L.L.C. (Caremark) and CaremarkPCS, L.L.C.. Caremark a wholly-owned indirect subsidiary of CVS Health, owns 100% of Novologix, L.L.C. (Novologix) as the result of an acquisition by merger that occurred in March 2013.

Prior to the acquisition, Novologix was a privately held medical pharmacy software company whose technology platform identified and captured cost savings for specialty drugs billed under the medical benefit to ensure appropriate medication utilization. The Software-as-a-Service (SaaS) platform created customizable capabilities which effectively and efficiently managed drugs covered under the medical benefit. Novologix processed medical pharmacy transactions for more than 25 million lives, covering approximately 7 health plan clients. The Novologix headquarters is located in Bloomington, Minnesota.

The CVS Health's corporate headquarters is located in Woonsocket, Rhode Island with primary operational facilities in Irving, Texas; Buffalo Grove, Illinois; and Scottsdale, Arizona. Caremark distributes prescription drugs to client's employees, health plan members, beneficiaries, and retirees and their dependents (collectively referred to as Plan Members) covered under client-sponsored benefit plans from four mail order pharmacies, 20 specialty mail pharmacies, and a national network of over 67,000 participating retail pharmacies.

3.2 Novologix Services and System Overview

CVS Specialty offers a comprehensive array of specialty pharmacy (and medical pharmacy) services for patients who require treatment for rare and/or complex conditions, including drug/medication therapy management, dispensing services, customized clinical support and personalized counseling to help guide appropriate and safe medication use. Other specialty services include ongoing condition education and therapy counseling, benefits verification, coordination of care with health care providers, patient education and adherence management. As part of its MBM services, Novologix validates drug coverage and edits claims based on Novologix System parameters derived from the Client's plan specifications established during implementation and through ongoing client requested changes.

The type of clients that implement the Novologix System include:

- Commercial health plans
- Government plans
- Specialties pharmacies
- Pharmacy benefit managers (PBMs)

- Network managers
- Healthcare providers

As part of the MBM service offerings, the Novologix System includes:

- *Medical prior authorization processing (Novologix Prior Authorization)* - enables a seamless experience for clients (e.g., healthcare providers or health plans, as applicable), as they can use a single web-based portal to request and complete requests for any drug requiring a prior authorization, including specialty or non-specialty, and within either the medical or pharmacy benefit. The primary use of the Novologix System has been for authorizations covered under the medical benefit and medical claims for specialty drugs.

- *Medical claims editing (Novologix Claims Editing)* - provides an automated solution with pricing logic that enhances accuracy and specificity, and applies fee schedule pricing, administrative and clinical edits that typically do not exist within legacy health plans claims adjudication systems. The Novologix System does not apply plan benefits or adjudicate and pay claims.

Novologix Prior Authorization

A prior authorization is an extra step that some health plans (medical insurance companies) require before deciding to pay for a drug and/or service. It is a separate activity from a claim. The prior authorization gives the provider a determination (i.e., approval or denial) from the insurance company for a drug or service that is not always covered.

A prior authorization takes place prior to rendering services or dispensing the drug. Providers requesting the service/drug are required to submit a form (either fax, phone or electronically online via the Novologix System) that states the clinical rationale/medical necessity for a specific drug or service for the member. In the case of a drug prior authorization via the Novologix System, there are specific questions asked about the drug (referred to as clinical protocol or question set) to determine whether the drug is appropriate for the member. At the end of the request, the health plan (or delegated entity) sends a letter to the provider and member stating the final determination (i.e., approval or denial) of the request, which is also made available on the Novologix application.

A prior authorization is not a guarantee of payment, but rather a verification of the clinical necessity for a drug. Typical medications that require a prior authorization include:

- Brand name medicines that have a generic available
- Expensive medicines
- Medicines with age limits
- Drugs used for cosmetic reasons
- Drugs prescribed to treat a non-life threatening medical condition
- Drugs not usually covered by the plan, but said to be “medically necessary” by the Provider
- Drugs that are usually covered but are prescribed at a dose higher than “normal”

Novologix Claims Editing

A claim is a transaction in which the Provider of the drug or service bills the health plan (medical insurance company or payor) for rendering the service or the drug (Claim). There are many types of Claims in the industry; the Novologix Claims Editing system focuses on a small subset of medical Claims that are for specialty drugs.

The Novologix Claims Editing system is a "preprocessor" performing several proprietary (back-end) algorithmic assessments prior to providing the edit on the Claim to the health plan to adjudicate in their system. The claims edit checks available within the system include pricing, clinical and administrative edits. The Novologix Claims Editing system does ***not*** apply benefits, including copays and/or deductibles, and it does not pay or adjudicate claims. Further, a client/payor may reject the recommendation made by the Novologix System prior to final adjudication.

Additionally, the Novologix Claims Editing system is capable of pricing and editing other Claims such as per diem (*supplies used to administer a drug*), nursing care (*clinical resource performing the drug administration*), and other non-specialty drugs for home infusions and total parenteral nutrition (TPN) care.

Novologix System Support

The primary applications supporting Novologix MBM services related to management of prior authorizations and editing of claims processed through the medical benefit is the Novologix technology systems (Novologix System).

The following is a description of the critical IT operating systems and databases that support the Novologix System:

Application	***Operating System***	***Database***
Novologix System	Microsoft® Windows® Server 2008 R2	Microsoft SQL Server 2012
	RHEL 7.5	

Organizational Structure

The senior leadership of Novologix (Vice President and Sr. Director of Product Management) is responsible for the overall management of the business unit. Reporting to these senior leaders are mid-level managers of the organization, responsible for various functional areas critical to the development, configuration, implementation, maintenance, and administration of the Novologix System. Significant functional areas are summarized below.

Novologix Functional Areas

Significant activities are performed by the following internal Novologix business units:

1. *Clinical Configuration:* This team consists of clinical and non-clinical employees within Novologix responsible for implementation and maintenance of all clinical-related configuration processes in the Novologix System. Key supporting responsibilities include:

- Prior authorization and Claims drug list review and maintenance

- NDC/HCPCS mapping and QA
- Missing crosswalks and QA
- Building and testing protocols
- New client configuration, QA and maintenance
- Provider NPI loads

2. *Fee Schedule/Pricing Configuration:* This team is responsible for the management, configuration and implementation of claims pricing edits for health plan clients using the Novologix Claims Editing system. Additionally, this team manages the fee schedule/pricing configuration process from end-to-end and works directly with the team supporting Novologix's implementations to identify and define the Client's specific requirements to support their pricing methodology.

3. *User Provisioning:* The user provisioning team that supports Novologix reviews, maintains and provisions internal and external user access requests to the Novologix System.

4. *Client Support Services (Novologix Call Center):* The client support services team that supports Novologix consists of non-clinical employees responsible for answering general Novologix application questions (e.g., navigating the application, password reset support, etc.) by external Provider users

Other significant activities performed by internal CVS Health enterprise business units that support Novologix in its provision of the Novologix System services include:

1. *Information Technology (IT):* This team is responsible for code development and configuration activities in the Novologix System. This team collaborates with the quality assurance team (QA) to ensure the code and system are working as expected, and develops code changes to resolve and/or correct any defects identified during testing. Additional IT functional teams provide support as follows:

   IT Operations:

   a. Participates in the process to complete the communication channel SecureTransport file transfer protocol (sFTP) process with clients; creates and manages the structure and security of the sFTP server.

   b. Performs the deployment of new code during releases.

   c. Manages Novologix data security activities supported by the CVS Health enterprise IT security team (IT Security).

   d. Provides application and infrastructure support for the Novologix platform.

   IT Security:

   a. Provides a consistent and accurate description of the CVS Health enterprise (including Novologix) overall information security program for a variety of requests.

   b. Supports the organization's ability to respond to client information security assessment requests through a single point of contact.

c. Partners with technical experts as necessary, delivers a consistent, accurate, and repeatable process to provide quality responses and an effective customer experience.

IT Architect:

a. Consults, evaluates and assesses client interfaces with the Novologix System on sFTP, eligibility service calls, etc. to ensure security/compliance with encryption, certificates, etc. and code scans.

b. Consults, evaluates and assesses platform performance, reliability and scalability including service level agreements (SLAs) for various transactions and evaluates/plans for client-specific anticipated transaction volume against the system's existing infrastructure and architecture.

2. *Quality Assurance (QA):* This team reviews requirements and enhancements for releases to check for alignment with the client's request as established during implementations and as highlighted in the requirements documentation. Additionally, this team creates test plans, test cases, provides test statuses/results, tests the code through all environments (integration, quality assurance, production), performs regression testing and manages test automation as needed.

3. *Implementations:* The Implementation Lead is the primary contact for the client during implementation and is responsible for implementing new clients in the Novologix System. The implementation team is also responsible for managing complex changes to established clients plans, including:

   a. Overseeing the project plan (tasks and schedule), risks, assumptions, issues, dependencies (RAID) log, action items, and executive summaries (reporting project status).

   b. Facilitating and documenting internal and external team meetings, and assigning appropriate subject matter experts (SME) to specific topics, issues, and questions.

   c. Coordinating activities of the implementation with various functional teams (individuals who support the implementation), including collecting and documenting requirements to ensure that the client's expectations and intent are met.

   d. Transitioning the client account to the Account Team (defined below) after the established warranty period following implementation.

4. *Sales:* This team is responsible for execution of the contract agreement and owns the direct, corporate relationship with the client.

5. *Account Management:* This team is responsible for maintaining the Novologix relationship with the client after implementation is complete. Additionally, this team manages all ongoing client issues and questions, and oversees all non-complex enhancements, whether such enhancement is part of the client contract or as enterprise-wide Novologix System enhancement.

6. *Analytics:* This team is responsible for developing reports for clients which includes outcomes and maintaining the reporting process documentation.

7. *Clinical Development:* This team is responsible for development and maintenance of the standard (and some custom) clinical development of drug categories and clinical criteria (protocols) used by the enterprise and Novologix to support the Novologix Prior Authorization system. Additionally, this team

develops the quantity and clinical edits used by Novologix to support the Novologix Claims Editing system.

Information Services

Information Services offers full service technology solutions for the Company and comprises various departments that have clearly defined roles and responsibilities. The responsibilities of the major departments are outlined below.

Information Technology (IT) Innovation and Architecture

IT Innovation and Architecture is responsible for architecture and technology planning across the Company including standards, research and development of new technologies.

1. *Application Information and Database Architecture*: Supports all information and data related needs of the Company. Provides information design and database implementation support focusing on optimal data structure design, information reuse and database performance.

2. *Enterprise Common Services*: Improves the consistency, quality, integrity and accuracy of enterprise data.

3. *Security Architecture*: Provides enterprise security architecture services allowing the business to create secure enterprise applications, infrastructure, networks and services in a cost-effective and timely manner. Security Architecture is responsible for the following:

    - The security technical strategy and security technology roadmap.
    - Developing both technical security standards as well as security architectural standards.

4. *Consulting*: Provides project and business teams, through the software development life cycle (SDLC), a process to ensure that all projects adhere to the Information Security & Risk Governance Standards and Frameworks.

Enterprise IT Services (EITS)

EITS helps ensure that the IT organization is providing business partners with cost-effective IT service, support, and solutions. This is accomplished by providing end-to-end operational process excellence through connected metrics, controls and continuous improvement frameworks, methodologies and tools.

IS Service Center (ISSC) is the communication hub for Caremark. The ISSC works closely with other Information Systems (IS) areas and the business to escalate system and workstation problems, administer problem management, provide outage notifications, change notifications, and answer 'How To' questions as well as working with Loss Prevention – Retail and Corporate Security to identify lost or stolen technology resources. Helpdesk tickets are tracked for documentation and resolution purposes.

Service Delivery Management

The Service Delivery Management organization is chartered to plan, schedule and deploy the solutions and services designed by the EITS Architecture and Engineering organization. Service Delivery Management

is responsible for the acquisition, configuration and deployment of new and/or updated infrastructure services and is made up of the following functions:

1. *Network/Telecom Build*: Responsible for acquisition, configuration and deployment of new and/or updated network, telecom services and middleware services.

2. *Server/Storage Build*: Responsible for acquisition, configuration and deployment of new and/or updated server and storage.

3. *Database Build*: Responsible for acquisition, configuration and deployment of new and/or updated database services.

4. *Delivery Support Services*: Responsible for change, release and asset management across the Company. Also responsible for managing EITS resource allocations to projects.

5. *Program Delivery*: Responsible for planning and coordinating the execution of IT infrastructure projects (and sub projects, which support IT business-line projects) across all EITS functional areas. Ensures delivery of new and/or updated infrastructure services and solutions meet CVS Health standards.

Infrastructure and Operations (Run/Maintain)

Infrastructure and Operations manages the infrastructure, platforms and operating environments required for computer applications and functionality, as well as the core processes for maintaining stability within these environments.

1. *Data Center Services*: Responsible for Data Center Infrastructure across the Company. This includes oversight and management of the main Data Center in Scottsdale, Arizona. Other responsibilities include management of shared services resources who implement, operate and support Unix, Windows and Mainframe, hardware and data storage services. These functions include:

    - *Mainframe and Midrange Operations*: Performs system administration and technical and operational support for the adjudication engine, mid-tier Unix servers, and Windows servers.

    - *Database Engineering*: Performs database administration functions for DB2, IMS, Oracle, SQL/MP, and MS SQL server databases.

    - *Operations Production Control and Data Center Operations*: Performs production job scheduling, and monitors and reports on the batch job schedule and production (batch and online) application processing.

    - *System Monitoring*: Controls the monitoring and identification of potential problems. Manages problem escalation and resolution process for the IS Organization.

    - *Capacity Planning*: Plans for and obtains adequate resources to support business requirements, including system, network, storage, and other related resources.

2. *Change Control*: Coordinates system change management including Change Advisory Board (CAB) review and final approval on production changes that are scheduled to be implemented.

3. *Disaster Recovery (DR) Coordination*: Maintains the technical DR Plan and coordinates technical DR testing.

4. *Desktop Services*: Provides primary end-user desktop computing hardware/software support (procurement, installation, diagnosis, repair, application, and messaging support) for Caremark.

5. *Network Services*: Directly manages and supports the local area network (LAN), wide area network (WAN) and Web connectivity for Caremark and remotely supports the LANs at pharmacy sites and all other Caremark corporate offices. Network Services also provides support services to all Company business units including external customers.

6. *IS Identity & Access Management*: Manages user IDs and access to systems, platforms, and applications, while protecting the confidentiality, integrity, and availability of sensitive corporate assets.

7. *IT Security Operations:* Provides IT security and compliance services to the organization. The team maintains tools, processes and procedures to execute or evaluate requirements defined by Information Security Governance and Risk Management. IT Security Operations performs information asset-related or systems-related investigations including computer forensics' investigations in support of Asset Protection, Legal, Human Resources (HR), Compliance and Integrity, IS, or other strategic business units. IT Security Operations is responsible for providing the following to the organization:

    - Security Operations Center (SOC)
    - Information Security Event & Incident Management
    - Centralized Computer Security Logging & Correlation
    - Minimum Security Baseline Evaluation (MSB)
    - Patch Validation
    - Vulnerability Management
    - Web Application Scanning
    - IT System Penetration Testing
    - File Integrity Monitoring (FIM)
    - Database Security Monitoring
    - Data Loss Prevention (DLP)
    - Intrusion Detection & Prevention Systems (IPS)

Program and Project Delivery

1. *Enterprise Project Support Office*: Responsible for governance, SDLC standards, procedures, templates, methods, and compliance. The team is responsible for on-demand and project progression tracking and allocation, stage gate analysis, and performance tracking.

2. *Controls Assessments & Monitoring (CAM)*: Manages audit and IT Compliance governance to the organization by serving as a liaison between the IS Team, business groups, internal and external auditors, and other IS Teams. The team is responsible for assessment coordination, assessment remediation efforts and various compliance support for ongoing and new projects. The CAM Team has IT department wide responsibilities. CAM's primary mission is to provide guidance on matters related to external and internal compliance initiatives to the organization by providing independent verification and validation of key controls that support various IS processes. If deficiencies are identified during testing, CAM will engage the appropriate process and application owners to develop remediation plans.

3. *IS Education and Training*: Works closely with the IS Management Team to identify key technical and professional training requirements for internal IS. It uses these teams to develop formal course requirements and work with outside vendors to provide both general and customized training.

4. *Information Reporting*: Responsible for systems dedicated to meeting direct informational needs of Novologix's clients.

Information Security Services

The organization has an Information Security Services division which provides tactical and strategic security guidance to the various business units, clients and customers. The primary focus of this division is the placement of appropriate controls that ensure confidentiality, availability and integrity of Client and corporate information.

Information Security Services manages the CVS Health Global Information Security program that defines, governs and safeguards information assets against unauthorized use, disclosure or modification, or damage and loss. Information Security Services is responsible for the following:

- Developing Information Security policies, standards and control requirements in accordance with Industry Best Practices and Legal and Regulatory requirements.

- Providing security awareness and training including ongoing education and regular reminders to inform and motivate all personnel to follow the stated IS and Physical security policies.

- Completing risk assessments for critical business processes, new services or solutions, as well as existing systems or solutions.

- Overseeing the Information Security Policy/Risk Management Process.

- Facilitating all prospective and existing client information security program inquiries.

IS Application Development

IS Application Development develops and maintains the computer applications supporting the enterprises' configurations. Responsibilities for specific systems are held by the following departments:

1. *Novologix Configurations (Clinical and Fee Schedule processing*) - implements, manages and maintains all clinical-related configuration processes, claims pricing edits and fee schedule configurations in the Novologix System.

2. *Novologix Helpdesk (Novologix Call Center)* - answers general questions about the Novologix System and assists Providers with navigating through such System, as applicable.

3. *External Clients* - specific adopters/customer types (Commercial Health Plans, Government Plans, Specialties Pharmacies, others) that implement the Novologix System.

3.3 Description of the Entity Level Controls

This section provides information about the five interrelated components of internal control at CVS Health (including Novologix):

1. *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.

2. *Control Activities*: Policies and procedures that help make sure that management's directives are carried out.

3. *Information and Communication*: Systems, both automated and manual, that support the identification, capture, and exchange of information in a form and timeframe that enables people to carry out their responsibilities.

4. *Monitoring*: Process that assesses the quality of internal control performance over time.

5. *Risk Assessment*: Identification and analysis of relevant risks to the achievement of its objectives, forming a basis for determining how the risks can be managed.

CVS Health's internal control components include controls that may have a pervasive effect on the organization, an effect on specific processes, account balances, disclosures, classes of transactions or applications or both. Some of the components of internal control include controls that have more of an effect at the entity level, while other components include controls that are primarily related to specific transactions, processes or applications. When assessing internal control, CVS Health considers the interrelationships among the five components.

Control Environment

An organization's control environment reflects the overall attitude, awareness, and actions of management and others concerning the importance of controls, as well as the emphasis given to controls within the organization. Relevant elements of Caremark's control environment include organizational structure and assignment of authority and responsibility, direction and oversight provided by CVS Health Board of Directors (the Board) and Audit Committee, management committees, budgetary controls, policies and procedures, and confidentiality measures. These control environment elements are described below.

Organizational Structure and Assignment of Authority and Responsibility

Senior management personnel reporting to the Caremark President are responsible for their respective functional area(s), providing clear reporting lines and defined areas of authority. (Reference the previous section titled Organizational Background for details on relevant functional areas.)

The viability and effectiveness of reporting structures is monitored and periodically adjusted based on organizational need. Changes to organizational and reporting structures are conveyed through corporate mail and/or the Intranet. Within each department, cross training, documented job descriptions and responsibilities are in place to provide guidance regarding employee authority and to facilitate the continuity of operations.

Board of Directors and Audit Committee

The CVS Health Board includes professionals in the financial, legal, and/or pharmaceutical industries. The Board's Audit Committee provides oversight for the integrity of the financial statements, compliance with legal and regulatory requirements, Independent Auditor's qualifications and independence, as well as the assessment of Internal Audit's (IA) performance and objectivity. The Audit Committee reviews and approves the IA annual audit plan and is apprised on the status of the plan's revision and/or completion periodically throughout the year.

Management Committees and Budgetary Controls

Management committees meet periodically to review, approve and advise management regarding corporate plans and policies and to monitor the organization's progress. Management develops plans and budgets on an annual basis. The budgets are revised periodically throughout the year. Reports are provided to management on a regular basis informing them of progress in achieving plans, budget goals and objectives.

Confidentiality

CVS Health strives to maintain Client confidentiality and holds information about a Plan Member's health in strict confidence in accordance with applicable privacy and record retention laws.

Access to, and use of, confidential information is limited to CVS Health business use and is further limited to the amount necessary for the employee to perform their job function. The use of confidential information for any other purpose is a violation of corporate policy. Violators are subject to appropriate disciplinary action, up to and including termination.

At the time of an employee's hiring, the organization requires employees to sign, or electronically accept, a confidentiality agreement and/or an employment agreement containing confidentiality provisions. The purpose of this policy is to specify the responsibilities for using confidential information. Additionally, employees are required to attend integrity training on an annual basis. The importance of confidential information is discussed at this training and in the Company's Code of Conduct.

Control Activities

CVS Health maintains policies and standard operating procedures (SOPs) covering a variety of financial and operational matters including, but not limited to: hiring, ethics and integrity, regulatory compliance, as well as compensation and training. The organization's hiring practices are designed to help ensure that new employees are qualified for their job responsibilities. Hiring policies include requiring minimum education and professional licensure or certification (where applicable), experience, reference and security checks,

pre-employment drug screening and execution of confidentiality statements. Training of employees is accomplished through new hire orientation, ongoing formalized in-house training, department training courses, supervised on the job training, and external seminars. Job performance is measured and evaluated on an ongoing basis to help ensure that job requirements are being met in an effective manner that ensures quality service. Immediate supervisors conduct formal performance reviews at least twice a year. Employees are evaluated on criteria that support CVS Health's corporate objectives and achievement of the department and individual's goals.

Information and Communication

CVS Health's organizational structure promotes clear lines of authority and responsibility. Employees are able to refer to the organization charts, as well as other job-related reference materials on the CVS Health Intranet.

Employee duties and responsibilities are communicated through a combination of some or all of the following: job descriptions, policies and procedures, live training, and/or training manuals.

CVS Health's structure allows for timely follow up and action on communications from both internal and external sources. Examples include Account Management Teams for Client communications, Compliance and Integrity Group (CIG) for corporate communications, Legal, and/or executive management for communications from regulators. Vendor communications are managed through Finance and/or Operations Management, and employee communications are managed by Human Resources (HR) and Corporate Communications. In addition, CVS Health adheres to a communication process designed to help ensure that external communications with media, Clients, Plan Members and others, obtain executive management, Legal, and/or functional area review as needed.

Monitoring

Monitoring at CVS Health includes, but is not limited to, management financial and operational monitoring, IS monitoring, quality processes and IA activities.

Management Financial and Operational Monitoring

Ongoing monitoring occurs in the course of operations. It includes regular management and supervisory activities, financial and operational reporting, and other actions personnel take in performing their duties.

IS Monitoring

The Operations Production Control, System Monitoring and Capacity Planning teams within Information Services regularly monitor system performance and capacity of systems and networks. A process is in place through the IS Service Center and other teams to respond to poor performance or reduced capacity in a timely manner.

Quality Processes

CVS Health fulfills its commitment to quality through tightly controlled policies and procedures that drive consistency among the various business entities. Consistency and quality is facilitated through the use of process work instructions and job aides, which contain detailed standards aligned with specific approved policies and procedures and/or standards. These policies and procedures encompass both the mandatory operational procedures to be followed and the mechanisms designed to measure compliance.

Through the analysis of complaint data, CVS Health's Quality Management program continually strives to eliminate potential problems at the source. Upon request, a root cause analysis is performed, and measures to resolve the problem at the source are developed and implemented.

Internal Audit (IA)

IA is an objective appraisal function to examine and evaluate CVS Health's control systems and activities. IA reports functionally to the Audit Committee of the Board of Directors and advises management and the Audit Committee on the adequacy of CVS Health's internal controls and procedures.

Sarbanes-Oxley

Sarbanes-Oxley (SOX) testing is performed by management and IA periodically. As part of the SOX compliance evaluation, business and IS processes and controls are documented, related risks are assessed, and internal controls are evaluated for design and operating effectiveness.

Risk Assessment

Corporate objectives define the manner in which the organization directs its activities to achieve shareholder value and are directly in support of CVS Health strategic direction. The identification and analysis of internal and external risks that may prevent achievement of those objectives and how those risks should be managed is addressed through evaluation of the risk of fraud, an ongoing risk assessment process and regulatory compliance.

Anti-Fraud

CVS Health has procedures in place to detect, correct, prevent, and monitor the occurrence of fraudulent activities to diminish their frequency and effect. The CIG performs several anti-fraud activities through a variety of measures that are primarily designed to mitigate risk to the organization. CIG coordinates with IA, Legal, Loss Prevention - Retail and Corporate Security, and other departments as necessary, to detect and monitor fraudulent activity including those applicable requirements under CMS that governs fraud, waste, and abuse. The CVS Health Chief Compliance Officer meets periodically with the Compliance Committee, Legal Department and management to identify areas of fraud risk within the organization.

Three key elements of the anti-fraud program are:

- *Awareness*: CVS Health promotes awareness of ethical behavior through its code of conduct, an ethics line advertising campaign and annual integrity training for employees and executives. In addition, compliance training relating to Medicare Part D is provided on an annual basis to those individuals who have been identified as being involved directly or indirectly in the administration or delivery of Medicare Part D services or activities. Finally, through the development and maintenance of key policies and procedures, employees are informed about potential fraudulent and/or non-compliant practices that they should be aware of and avoid while performing their responsibilities.

- *Detection/Monitoring*: CVS Health operates a 24 hour toll free ethics line. The ethics line provides a mechanism for employees, Clients, and Plan Members to report anonymously any suspected illegal or unethical activity. Ethics line calls are triaged daily by CIG. The corresponding Open Cases Status reports are reviewed by management monthly. An appropriate course of action in response to the calls is determined by CIG with support, as needed, from the Legal Department and the Compliance Committee. The Compliance Committee meets at least four times annually and on

an as needed basis. A separate Compliance Committee was formed to specifically focus on Medicare Part D activities and to address appropriate topics, timely and consistently with CMS requirements. The Medicare Part D Compliance Committee meets at least quarterly. CIG also conducts ongoing compliance-based risk assessment activities and performs audits and/or reviews in conjunction with an annual audit work plan. These work plans are prepared for both the Corporate Compliance Program and the Medicare Part D Compliance Program.

In addition to the CVS Health general enterprise detection and monitoring activities described above, Novologix provides reports on claims activity submitted by providers under the terms of the contract with clients for the Novologix System. The client reviews for changes in drug utilization, clinical appropriateness and independently identifies any possible fraud, waste or abuse (FWA). The client coordinates as necessary with their internal compliance guidelines to determine if evidence exists to support whether FWA or other misconduct have occurred.

- *Investigation*: CIG initiates an investigation when information on possible unethical or fraudulent behavior is received. The investigation may be performed together with IA, Loss Prevention – Retail and Corporate Security, HR, and/or the Legal Department. The Chief Compliance Officer reports occurrences of suspected fraud to the Audit Committee and the Board of Directors. The Medicare Part D Compliance Officer reports potential fraudulent and/or non-compliant activity through the Medicare Part D Compliance Committee.

Ongoing Risk Assessment Process

CVS Health employs a bilateral risk assessment process. First, a decentralized assessment process is performed by functional management to identify operational and financial risks. Appropriate actions to mitigate risks are identified and then taken. Actions requiring new or changed hardware or software are subject to prescribed change management and SDLC procedures.

Risk assessment is also performed on an annual and ongoing basis by the CIG, IA and IS departments. CIG and IA work together with management to identify the key areas within CVS Health's operations for which their respective resources should be focused. These planning sessions yield annual audit plans that are reviewed and revised as needed throughout the year to ensure the most effective deployment of resources. Information Systems Security (ISS) performs security assessments on critical systems throughout the year. Risk Management's primary objective is to ensure that the organization is adequately protected with appropriate levels and types of insurance against financial loss due to claims (e.g., liability, workers compensation).

Regulatory Compliance

Regulatory and legislative compliance, including Medicare Part D, are key areas integral to the continuing operation of Caremark, its financial performance, and its financial reporting requirements. Numerous departments and resources are dedicated to understanding industry laws and regulations and communicating those regulations to appropriate management groups. New and revised laws and regulations applicable to Caremark, identified by Government Relations, are evaluated by Legal, with the assistance from internal and external subject matter experts. Government Relations, Legal, and CIG work as a cross functional team to ensure awareness and compliance with these laws and regulations. Specific employees are dedicated to Medicare Part D to ensure all CMS memos, guidance, user calls, and regulations are quickly assessed and any impact to the current program is communicated to appropriate internal departments for implementation. Communications are also distributed, as appropriate, to Clients explaining the actions Caremark is taking to comply with such CMS changes.

3.4 Overview of the Novologix System

The Novologix System comprises various processes and supporting technologies centered on the setup and accuracy of Prior Authorizations and Claims that are transacted (edited) through the application. These processes include:

- Client Information Gathering/Setup (Configurations)
    a. Collecting Information
    b. Client Setup, Prior Authorization Protocols, Drug List and Fee Schedule Configurations
    c. Contract Modification Process
- Member Eligibility and Drug File Administration
    a. Member Eligibility Setup and Maintenance
    b. Drug File Administration
- Claims Edit Processing
    a. Claims Edit Recommendations
    b. Claims Edit Messaging
- Claims Input File Submission and Claims Response File
    a. Claims Submission Methods
    b. Claims Input File
    c. Claims Response File
- Prior Authorization (PA) Processing
    a. Prior Authorization Request Submission

These processes and transactions impact the accuracy and completeness of the product requested by the user, as described below.

3.4.1 Client Configurations

Client Setup, Prior Authorization Protocols, Drug List and Fee Schedule Configurations

During the initial implementation phase, clients make key clinical and business decisions based on the system selected (Prior Authorization or Claims Editing). Those key decisions include product workflow, drug list, clinical protocols, provider network and fee schedule/pricing. Configuration change work instructions and policies and procedures are in place to guide internal resources through required steps to facilitate and manage the process.

After implementation, changes to configurations (maintenance or client requests) are documented within a change support ticket in the Novologix ticketing system, noting authorization by the client or other authorized representative, as applicable, and based on the nature and type of change. Configuration changes go through review and internal testing by Novologix (i.e., QA or Clinical Configurations), and/or the client where applicable, based on the type of change requested. Self-service clients are responsible for performing QA testing on their own and providing approval to Novologix to deploy changes to production.

Configuration changes to the Novologix System are reviewed and approved by Novologix clinical management and/or the client, as applicable, prior to implementation. Only authorized client resources or approved account representatives can request or approve changes to drug lists, fee schedules, claims edits, or prior authorization protocol configurations. Only specific, authorized Novologix Clinical Configuration members have the ability to make changes to the client's clinical configurations. These members have restricted access to specific user roles that allow them the ability to make changes in the system. When necessary for deployment, a change request is submitted to Novologix IT to deploy the change to production on the servers/database.

Contract Modification Process

While implementing the plan design as set forth in the client's contract with Novologix and/or its affiliate ("Novologix Contract"), there are several controls to ensure systems are programmed and administered in accordance with such contract. During contracting and implementation, the client and/or Novologix may discover the need to amend or modify the contract to address any necessary changes.

3.4.2 Data Transmission, Input and Administration

Member Eligibility Setup and Maintenance

Eligibility files are required as a part of the Novologix prior authorization System services in that they allow Novologix to determine the eligibility of a particular patient at the time of request. Eligibility files are provided by clients via the SecureTransport File Transfer Protocol (sFTP) site, or other approved, secure method of transmission negotiated with the client at the time of implementation. Eligibility files consist of fields containing specific member data needed for processing and reporting. Clients typically send files in the Novologix proprietary or industry standard 834 format.

Regardless of the delivery method or file format, an automated file processing program receives the client's file from the SecureTransport site once it is loaded. Automated jobs are configured to detect and retrieve member eligibility files from the SecureTransport server and load into the Novologix platform. The automated jobs retrieve the client-specific file, perform an integrity check to validate that the file is in the proper format, and place the file in a staging client-specific network folder. A file is flagged for manual intervention if it fails to pass this integrity check for any reason. To help ensure that files are successfully loaded, the automated jobs are configured to notify Novologix if an error occurs during the load process. If the file successfully passes the checks, the data will automatically be applied to the Novologix production eligibility database. A separate automated file processing program archives the text file into a client-specific directory folder.

Drug File Administration

On a predetermined frequency, the MediSpan Drug List (which includes related drug pricing information) is loaded into the Novologix System. After the Drug List detail is loaded, the Novologix report database is automatically updated with this most current drug list records. Clinical Configurations conducts a crosswalk

(i.e., mapping) of National Drug Codes (NDCs) to the appropriate Healthcare Common Procedure Coding System (HCPCS) codes and loads the revised/mapped drug list into the Novologix System. The mapped Drug List is reviewed and tested by clinical pharmacists prior to being loaded into the system to ensure that drugs are coded/mapped correctly.

Claims Input File

Claims are sent to the Novologix System at the determined client frequency via a claims file. Novologix applies edits to each claim and sends the file back to the Payor, typically within 24 hours. Claims input policies and procedures are in place to guide personnel with managing claims file input activities. The claims input file submission and claims response file processes are primarily driven by automated jobs and local services.

The process begins when clients load claim files to a SecureTransport site via sFTP server, or another pre-determined secure transmission method. Clients are restricted to their client-specific designated folders on the SecureTransport site. An automated workflow moves the claim files from the SecureTransport site to an internal client-specific file share server directory. From there, automated jobs are configured within the ActiveBatch job scheduling tool to retrieve client-specific EDI claims files (837 or approved proprietary file format) from the client-specific file share server directories. Additionally, the automated file processing program is configured to notify Novologix IT if an error occurs during the file loading procedure.

An automated integration and connectivity server is configured to pull EDI and proprietary claims files as they are moved to the Inbound Transactions directories, perform syntactical quality checks and process the files as individual claims. The platform is configured to notify Novologix IT if failures or errors occur. If elected, an automated acknowledgment file is provided to the client.

Production support personnel utilize the TPAM (EDI Trading Partner Agreement Manager) application to monitor claims input and file processing information on a real-time basis. Claims files that are unable to be processed are automatically moved to a specific “Failed Transactions” directory and the automated job is configured to notify Novologix IT.

3.4.3 Claims Edit Processing

Claims Submission Methods

There are three ways a claim can enter the Novologix System for editing, but may vary based on the client’s arrangement/implementation:

1) Claims are sent to Novologix via a claims file (automatic file submission process outlined above).
2) Claims can be entered directly into the Novologix System by the Payor/Provider.
3) Claims are sent to the Novologix Claims Processing team by Providers via email/fax (CMS 1500 form) for direct entry into the Novologix System.

Claims Edit Recommendations

Regardless of claim entry method, processing of medical claims edits occurs systematically through Novologix’s proprietary logic which includes configuration changes and/or coding. While processing, the system performs a series of administrative, clinical and/or pricing edits that are grouped in the defined categories below:

1) Quantity or Quantity Level Limits (Maximum one time daily) - identifies when a claim exceeds its allowable units based on FDA recommendations
2) Authorization (Auth) to Claim Matching - matches the claim to an approved or denied prior authorization
3) Administrative - identifies missing information on the claim (member or provider demographics) and specific transaction types (duplicates or overlapping claims, voids and/or replacement claims, other)
4) Pricing - applies to claims based on the client's Fee Schedule and indicates when a claim does not match/meet a Fee Schedule
5) Service Date Too Soon / Refill Too Soon / Frequency - determines when a drug is administered at a higher frequency than the approved FDA recommendation labeling
6) Medical Drug Utilization Review (mDUR) - maintains edits for any in-scope drug and identifies claims where clinical edits apply.

Claims Edit Messaging and Response File Assembly

After a claim enters the system, the Novologix System "processes" the claim to apply edits, assigns a claim number, and adds messaging (reject, warn, inform) based on the client elected and configured claims edit checks. Individual "processed" claims within the Novologix System are then re-assembled within the original claims file ("response file"). Prior to re-assembly, the System is configured to perform a completeness validation check to help ensure the claims processed match the claims received. If the number of claims processed does not match the number of claims received, a matching error has occurred and the file is not automatically re-assembled. The error is investigated and resolved by Novologix prior to returning the re-assembled file to the client.

The claims response file includes the client's original claims data returned "as is" (in the original format with no modification to the claims data), and Novologix assembly adds additional data points, including the following, as applicable:

- Novologix Claim Reference Number
- Authorization Matched to the claim in the system, if applicable
- Novologix Priced Amount, if applicable
- Novologix Approved Quantities, if applicable
- Novologix Proprietary Messaging Codes

Following re-assembly by the Novologix System, automated jobs are configured to move the claims response files from the file server to the client-specific sFTP directories, based on each client's implementation delivery method and frequency. Clients receive a response file for each claims file submitted.

3.4.4 Prior Authorization Processing

Prior Authorization Request Submission

When a prior authorization is required by a plan to authorize payment for a specialty medication, the Provider must submit a prior authorization request, which generally takes place prior to rendering services. Providers requesting the service submit a prior authorization form in one of the following three ways: fax, phone, or electronically online via the Novologix system. A prior authorization is submitted for a specified drug or service for a Member and includes the rationale for the request (i.e., patient condition). Typically, there are specific set of questions asked about the drug, member, condition, etc. (protocol) to determine if the Member is a proper "fit" for the drug. At the end of the request, the Health Plan (or the delegated entity) sends a letter to the Provider and the Member stating approval or denial of the drug.

The fax ("fax form") is an electronic document that describes the drug protocol a Provider needs to complete and return to the CVS Health CRU (for delegated client arrangements). The CRU is responsible for entering the information on the completed fax form into the Novologix system.

Providers also have the option of submitting a prior authorization request over the phone. For delegated client arrangements, the call is routed to the CVS Health CRU team for entry into the Novologix System. For non-delegated clients, the Provider submits their request to the Novologix Payor UM Team which is entered into the Novologix System by Payor Techs. The prior authorization request follows the standard process of review for decision rendering upon entry into the System regardless of submission method.

Before a Provider can initiate a prior authorization request, certain information is required to help ensure that processing is not delayed. The Novologix System is configured with front-end data field controls/edit checks to help ensure that the information entered for the prior authorization is complete, as applicable and elected.

Novologix has field validations in place to reduce data entry errors and help ensure that the information entered meet requirements defined by the client. In the event that invalid data is detected, the application returns an error message or will not allow submission of the prior authorization until all the required information is included. For example, the application will not accept a number less than 10 digits for a National Provider Identifier (NPI), which is a unique 10-digit identification number required by HIPAA for all healthcare Physicians and Providers in the United States.

The Novologix system is configured to prevent the creation of a prior authorization for a member or Provider that is not setup or has been deactivated in the system. Upon creation of a prior authorization request, only approved members setup in the system via the member load process are able to be selected. The Novologix System is configured by default to restrict updating of member demographic and eligibility information within the application (updates must be made through the eligibility load process), unless elected by the client to opt out of this default setting.

The Provider is responsible for entering appropriate and valid information. Specifically, the Provider's NPI, frequency, quantity, refill number and treatment duration must be completed before the prior authorization can be submitted. In addition, the Novologix System is configured by default to perform a duplication check and prevent duplicate prior authorizations from being created for a member/patient based on drug, date of service and NPI (if elected). Clients may elect to have the System provide a warning rather than disallowing the creation of the prior authorization when identified as a duplicate.

Prior authorization processing happens electronically and is automated using client-specific rules and clinical question sets that are configured within the system. Upon completion of the protocol question set, a prior authorization request is evaluated using Novologix's clinical algorithm and can result in one of the following statuses:

- Approved
- Require additional clinical review
- Pend for clinical validation of medical records
- Denied

The Novologix System automatically routes prior authorizations that do not result in auto-approval and require further clinical review to the appropriate clinical review team based on the established workflow. For delegated clients, the PA is routed to the Case Review Unit (CRU) queue based on role assignment. For non-delegated clients, the PA is routed to the appropriate queue based on role assignment, as established specific to each client during implementation. Following clinical review, the review decision is entered into the Novologix System (Approved or Denied).

Denied PAs can be modified (i.e., change or update protocol responses or input detailed clinical appropriateness) by going through the appeal process within the Novologix System. The Novologix System will update/append the original PA status as 'PA Appeal'.

The Novologix System displays the prior authorization status during the course of the submission process. Once a prior authorization request is in an "Approved" or "Denied" status, an automated job routes the information to a subsystem for letter notifications. For purposes of this report, the letter notification process is not considered in-scope.

Novologix provides clients with a system-generated list of drugs that are setup within the Novologix system to support prior authorizations. Clients must review the provided drug list for each plan they have implemented within Novologix and notify Novologix of any discrepancies or changes identified within the established time frame. Changes that are determined necessary or requested by the client follow the standard Novologix Change Request process.

3.5 Information Systems and General Controls

3.5.1 General Computer Controls

General computer control procedures establish the control environment in which computer applications are developed and maintained. Therefore, general computer controls procedures, if suitably designed and operating effectively, provide an environment for the development and processing of applications to achieve specific application control objectives. The enterprise's general computer control procedures are described under the following categories:

- Physical Security
- Access to Data Files and Programs
- Virus Protection

- System Software
- Change Management Process
- Job Scheduling
- Incident and Problem Management
- Backup

Physical Security

A badge access system is used to control and restrict access to Caremark Data Centers. Each user is assigned an access badge with a unique identification number that is recorded each time the badge is used. The system's control panel is secured in a locked cabinet. A list of personnel with access to Data Centers and/or server rooms is generated monthly and reviewed by designated IT Management for ongoing appropriateness of access. Discrepancies are followed up and resolved. Upon demand, Asset Protection personnel can provide management with reports of accesses and access attempts meeting defined criteria such as those occurring after hours, or other invalid or suspicious access activities. Those spaces not controlled by badge access systems are secured by key lock. Access to the keys is limited to appropriate personnel based upon their job responsibilities.

Asset Protection or designated facility personnel grants access to sensitive Caremark facilities (e.g., Data Centers, server rooms) based on request forms approved by Operations and Information Systems (IS) Management. Contractors are required to have background checks and are provided access badges while on premises. Without background checks, contractors are considered visitors. Visitors are required to wear visitor badges distributed by building receptionists, which provide no physical access capabilities to a controlled area, in addition to being escorted by a Company employee.

Termination details for full time employees and contract workers are sent to Asset Protection and other individuals responsible for deactivating badges. These documents are used to confirm all terminated employee and contractor physical access has been deactivated in a timely manner.

Security guards and video cameras are used to monitor physical access to sensitive areas.

Access to Data Files and Programs

Identity & Access Management (IAM) personnel process approved access requests for in-scope applications, database, and operating system environments including the network. Procedures exist to govern timely actions related to requesting, establishing, issuing, suspending, and disabling user accounts. The Novologix System and supporting systems/platforms reside within the CVS Health Corporate network, managed by enterprise-wide teams.

IAM requires the completion of User Access Request forms for adding and modifying user access. The forms are required to be approved by the user's functional leader and when applicable by the Information Asset Steward, before access is granted. Upon granting user access, forms are retained as documentation within the application work instructions.

A user ID and password are required to authenticate the in-scope applications and network, including supporting operating systems and databases. Password composition and lockout settings are in place as defined in Caremark's logical access policies and standards. To reset their password, the user has to contact

IT Service Center and authenticate their identity if it is requested over the phone. If there is an identity authentication exception, the request is referred to user management or IAM for research.

Access to production data and programs is based on business need. Groups/role codes categorize users with similar access needs. These users are assigned one or more "role codes" depending on their position and job functions within Caremark. The role codes allow the user to perform system functions consistent with their assigned job duties.

Application, database, and operating system access is reviewed at least annually, based on risk, to assess and confirm whether rights and privileges are restricted to appropriate personnel based on job responsibilities. IAM facilitates a Periodic Access Review (PAR) on at least an annual basis for all systems and semi-annually (twice a year) for applications deemed high risk (e.g., adjudication engine) with the Information Asset Stewards and Management. The process is performed to review and confirm the appropriateness of users' access rights and privileges, including high privileged access to relevant applications, operating systems, databases, developer access to production, and supporting tools.

Department managers and the HR Department are responsible for notifying appropriate Information Systems User Provisioning IAM personnel of employee termination. Access to the network for terminated employees is removed through an automated script within 72 hours based on notification from HR or Strategic Procurement. Access to the network for terminated contractors is set to automatically expire at a specific end date approved as part of the access request or extension process. The end date cannot be set beyond the date of the contractor agreement.

On a daily basis, logs of security related activities (e.g., failed log on attempts, unusual network based traffic, etc.) across the network are captured using various monitoring tools and reviewed by members of Information Security. A formal Security Operating Center (SOC) is established to provide real-time monitoring and reporting of security events. Any identified incidents are then entered into a centralized reporting tool for escalation and resolution.

Where not specifically noted above, Information Security Policies and Procedures for the LAN environment and in-scope systems are similar in areas such as password rules, terminated employees, and inactive user IDs. The Novologix System requires individual IDs and passwords and utilizes various roles to help ensure users have the appropriate access to data and client sites.

Formal security standards and minimum security baselines have been developed for the in-scope operating systems and databases. The security standards and minimum security baselines are reviewed at least biennially and updated (if needed) by Information Security and sent to the relevant system owner for final approval.

Management performs an annual review of operating systems and databases to ensure configuration settings for in-scope production systems are in compliance with the defined corporate minimum security baselines and that out-of-compliance configurations are corrected appropriately.

Virus Protection

Anti-virus protection software is used to help protect the infrastructure from computer-based viruses/malware. Systems Infrastructure Services supports an enterprise centric anti-virus solution that shifts responsibility for virus protection from the users of the information systems resources to the information systems infrastructure support organization. This shift in responsibility enables the

infrastructure organization to maintain complete control over the quality and depth of the corporate virus protection.

System Software

Based on business needs, IS Management initiates requests for upgrades to system software. System and application changes are processed using the enterprise Change Management Process, described in the section below.

Change Management Process

The following Change Management and "IT Implementation" descriptions apply to the Novologix applications in-scope. Configuration changes made to the Novologix System follow different change procedures as described in the "*Client Configurations*" section above.

Formal policies and procedures have been developed to guide the change control process for application development and support personnel in the development and modification of application systems. Such policies and procedures include the requirements for authorizations, design, testing, and review of changes (application and infrastructure).

Once change requests are fully authorized and funding determined, the system changes are assigned to system developers within the applicable IS Team. Software application changes are initiated, stored, backed up and unit tested by the programmers. Once unit testing is complete, the programs are promoted to system testing. After system testing is complete and results are acceptable, further testing steps will be carried out, ending with UAT to validate user requirements. In addition, for major releases, regression testing is performed to help ensure that core application functions and processes continue to perform as expected after changes have been introduced and tested separately. The results are documented, reviewed and any changes or unexpected results are communicated and addressed. The Data Resource Management Team participates to help ensure the database design is optimal to support the business functionality and meets performance objectives. Changes to the production environment (whether Novologix or Caremark developed software, hardware configurations, infrastructure software, database, or commercial packages) are recorded and tracked by the same production change management process. Both planned and emergency changes are recorded in a change request ticket in the HP Service Manager (HPSM) ticketing system before a change can take place. A full description of the request, a risk assessment, a back-out plan, and approvals are captured in the change management documentation and populated in the change request ticket. The change coordinator who is accountable for completeness and accuracy of the request is also identified in the change request ticket.

A Change Advisory Board (CAB), consisting of representatives from Infrastructure, IS Application Development and vendors (when appropriate) is held on a weekly basis to review pending and recent changes. Approval from the CAB is required before the program turnover request is moved into Production. Areas reviewed include sign-off from various infrastructure teams, conflict resolution, outage impacts, time schedules and back-out plans. Production Change Management Reports from the HPSM system are used to summarize and track activity. The Change Management Team maintains the approvals and reports.

Expedited changes include a "break/fix" to repair or prevent a production problem, or a project that involves penalties or client performance guarantees. To help ensure that production problem issues are resolved appropriately and approved, expedited changes not only adhere to the normal change management process, but also require approval from VP, SVP and by the group's management prior to production implementation. Any "client commitments" change needs to be supported by appropriate documentation

and submitted to the CAB for review. For expedited application software production changes, approval from the line of business Director and the Enterprise Business System (EBS) and IS Technology Infrastructure Director is required prior to submitting the request to the CAB.

Version control software is utilized to maintain and control access to current and prior versions of application code. The version control software is configured to create a new version of the application code when changes are made. If necessary, changes can be rolled back to prior versions of the application code. Development efforts are performed in environments logically separated from the production environment.

IT Implementation

Changes are implemented using different tools and processes based on the type of change and the application or platform involved. In most cases, identified members (Change Executors) of the Novologix IT Operations staff who are not responsible for coding changes are responsible for implementing the change.

For all types of changes, the Change Executor is responsible for verifying that the production change management process has been followed, as evidenced by a completed change request ticket. Application changes are managed through a periodic production release procedure referred to as an "application release," which provides coordination and review of change interdependencies. Changes that are needed more frequently based on client requests are promoted through the defined release, change control, review, and approval processes.

Metrics and reports are generated and reviewed by IS Management to assess the nature and impact of changes. This data is also retained for historical analysis and reporting.

To help ensure the integrity of the production environment, the authority to migrate changes into production is limited to the Novologix IT Operations and EITS Build and Run personnel. Systems and operations personnel monitor system resources and interruptions after the implementation of production software into the production environment.

File Integrity Monitoring (FIM)

Application file modification reports are generated by the FIM tool, or manually for servers not compatible with FIM, and reviewed for appropriateness by Application Managers, as per CVS Health policy. A monitoring process exists to reconcile changes made to critical libraries against supporting change tickets for the Novologix system. This monitoring is supported either automatically through the ArcSight and SCSP tools, or manually for operating systems not compatible with the automated FIM process. In the automated FIM process, SCSP is used to configure critical libraries for monitoring and ArcSight is used to log changes to these critical libraries.

Job Scheduling

Policies and procedures exist for the processes (i.e., monitoring, back-ups, and support) within Computer Operations.

Novologix utilizes the ActiveBatch automated scheduler for batch job processing. Jobs run automatically based on defined schedules dictated by client agreements and implementations. Active monitoring, notification, and escalation of batch processing by the Production Support team ensure timely problem management and corrective action. Notifications regarding successful completion or errors of the jobs are logged and sent to a centralized e-mail address that is monitored by the Production Support team. Job

failures are investigated and re-run as instructed if necessary by Production Support, or if necessary Production Support escalates problems to the appropriate personnel for resolution.

Changes to the job scheduler are tracked via the Novologix ticketing system and follow the Novologix standard change management processes. Access to automated schedulers is restricted to authorized personnel.

Incident and Problem Management

Production issues are escalated to the appropriate infrastructure support team and an accompanying ticket is completed in HPSM that identifies the problem and action taken. The tickets are investigated and tracked through to resolution. When a user calls the IS Service Center, or the IS Service Center proactively identifies that an outage situation has occurred, the IS Service Center will open a ticket in the HPSM tool. The IS Service Center uses an on-call spreadsheet and/or the xMatters (previously known as AlarmPoint) paging system to ensure appropriate parties have been notified. Notification through pager and cellular phone are the primary methods employed. The on-call spreadsheet includes the appropriate IS Support Group. Follow-up reporting occurs to appropriately manage activity. When the incident is resolved, the responsible support personnel update the status of the HPSM ticket. The highest priority-level incidents such as Priority 1 or 2 are documented in a morning report that is sent to IS Management and reviewed in a daily (Monday to Friday) meeting. They are also tracked in the Client Impact Meeting (CIM)/Problem Elimination Meeting (PEM) database. A tracking report is used to follow-up on HPSM tickets that are not resolved within their service-level agreement.

Daily, weekly, and monthly problem statistics are reported to IS Application Development and IS Operations Management.

Backup

Backup data is replicated real time to the Woonsocket, Rhode Island, Data Center. The inclusion of critical data in the backup or replication processes is validated during the disaster recovery exercises that are performed annually. Backups are conducted in a timely manner for applicable in-scope applications and supporting databases and operating systems.

The Tivoli Storage Manager (TSM) and DDBoost backup software tools are utilized for backing up the Novologix system and supporting infrastructure on a daily basis. Backups are replicated to the Data Center located in Woonsocket, Rhode Island on a daily basis. For aid in the Disaster Recovery process, Zerto replication software is utilized to replicate the VMware virtual servers from Scottsdale, AZ to Woonsocket, RI. EMC SRDF is also utilized in replicating the SQL SAN luns and EMC Isilon luns are replicated for the application file shares.

Additionally, the enterprise has taken measures to help reduce the risk of service interruption. These measures include (as rated by the manufacturers):

- A Spot Network Grid that provides dual power feeds from redundant transformers to the Data Center facility.
- Uninterrupted Power Supply systems and diesel generators. Both systems are tested regularly to help ensure functionality.
- FM200 fire protection and dry-standing sprinkler systems.

- Dual phone system central offices to help ensure communication access to the building.
- Validation during the annual disaster recovery exercises that critical data is included in the backup or replication.

Backups of the Novologix production systems are scheduled and performed in the Shea Data Center (located in Scottsdale, Arizona) on a regular basis. Scottsdale support staff monitor and ensure system backups are performed. Novologix is also protected by the control measures above in the Shea Data center and is supported by replication to Woonsocket, Rhode Island.

3.6 Control Objectives and Controls

The control objectives specified by Novologix, the controls that achieve those control objectives, and management responses to deviations, if any, are listed in the accompanying *Description of Control Objectives and Related Controls, Tests of Controls and Test Results.* The control objectives, controls, and management responses, are an integral part of the Description.

3.7 Complementary User Entity Control Considerations

Novologix controls were designed with the assumption that certain controls would be implemented by user entities (clients, Payor Organizations, Provider Organizations, etc.). It is not feasible for certain control objectives relating to the processing of transactions to be achieved completely by Novologix's management or the user entity acting alone. The application of controls by user entities is necessary to achieve certain control objectives identified in this report.

Below describes other controls that user entities should have placed in operation for the achievement of the control objectives in this report. The user entity control considerations presented below should not be regarded as a comprehensive list of controls that should be employed by user organizations. Other controls may be required at the user entities. User entity auditors should consider whether user entities have placed these controls in operation when understanding and evaluating the internal controls at the respective user entity:

Controls at each user entity should be established to provide reasonable assurance that:

- Clients review requested change configuration testing results before giving authorization to implement the change into production. For changes where client testing is not required/applicable, clients are responsible for identifying and communicating any errors to Novologix in a timely manner. (Control objective 1)
- User entities are responsible for appropriately communicating requested drug list or fee schedule changes to Novologix on a timely basis. (Control objective 1)
- Information, including enrollment related data, supplied to Novologix from user entities is authorized, accurate, complete and provided in a proper format. (Control objective 1 and 2)
- User entities are responsible for reviewing reports and/or system configurations periodically to confirm that fee schedules, drug lists, prior authorization question sets, and the PA clinical review workflow are configured appropriately. (Control objective 1)
- User entities monitor transmissions to Novologix and take corrective action on errors identified during the file submission process. (Control objective 2)
- User entities are responsible for internally securing the data files transmitted to and received from Novologix. (Control objective 2)
- User entities are responsible for performing a timely review of reports, including those identifying eligible members and claims detail, and notifying the Novologix Account team or Help Desk (Novologix Call Center) of any discrepancies. (Control objective 3 and 4)
- User entities are responsible for reviewing the accuracy and completeness of output (i.e., prior authorizations and claims details and edits) produced by the Novologix System, and notifying the Novologix account team or Help Desk of errors or discrepancies to make adjustments as necessary. (Control objective 2, 3 and 4)
- User entities are responsible for entering the valid and accurate prior authorization information including condition, drug, date of service, patient and provider information, and provide valid and accurate responses to prior authorization question sets in order for automatic and accurate processing of prior authorization forms. (Control objective 4)

- Non-delegated user entities are responsible for management and oversight of their own PA clinical review workflow user assignment and monitoring of clinical review decisions (Approved or Denied) entered into the Novologix System. (Control objective 4)
- User entities are responsible for appropriately requesting, authorizing and communicating new user or modification of existing user access to the Novologix System. (Control objective 5)
- User entities are responsible for reviewing that access granted to the Novologix System is appropriate based on the access privileges that were requested. (Control objective 5)
- User entities are responsible for timely communication of terminated users to the Novologix System. (Control objective 5)
- User entities are responsible for performing periodic user access reviews of existing user access to the Novologix System. (Control objective 5)
- User entities are responsible for ensuring the confidentiality of any user accounts and passwords assigned to them for use with the Novologix System. (Control objective 5)
- Client user IDs and passwords are restricted to authorized personnel with approved and proper assignment, administration oversight (terminations, etc.), and use of the application and direct connection accounts. (Control objective 5)
- Adequate password controls are in place on user organization systems, and logical access to the Novologix System by or through the user organization systems is monitored and maintained. (Control objective 5)
- User entities are responsible for immediately notifying Novologix of any actual or suspected information security breaches, including compromised user accounts. (Control objective 5)
- User entities are responsible for communicating any errors or issues that impact their use or ability to process prior authorizations or claims to Novologix on a timely basis. For program changes that do not impact or affect the client; Novologix bares no responsibility. (Control objective 6)

Section IV. Description of Control Objectives and Related Controls, and Tests of Controls and Test Results

4.1 Testing Performed and Results of Tests of Entity-Level Controls

In planning the nature, timing and extent of its tests of the controls specified by Novologix in this Description, Ernst & Young LLP considered the aspects of Novologix's control environment, control activities, risk assessment, information and communication and monitoring activities and performed such procedures over these components of internal control as it considered necessary in the circumstances.

4.2 Procedures for Assessing Completeness and Accuracy of Information Produced by the Entity (IPE)

For tests of controls requiring the use of Information Produced by the Entity (IPE), procedures were performed to assess the reliability of the information, including completeness and accuracy of the data or reports, to determine whether the information can be relied upon in the examination procedures. This includes IPE produced by Novologix and provided to user entities (if relevant and defined as part of the output control objectives), IPE used by management in performance of controls, and IPE used in the performance of our examination procedures.

Based on the nature of the IPE, a combination of the following procedures were performed to address the completeness and accuracy of the data or reports used: (1) inspect source documentation relating to the IPE, (2) inspect the query, script, or parameters used to generate the IPE, (3) agree data between the IPE and the source, and/or (4) inspect the IPE for anomalous gaps in sequence or timing.

Client Configurations

Control Objective 1:			
Controls provide reasonable assurance that client configurations (i.e. drug list, fee schedule/pricing, and PA protocols) are implemented in the Novologix system based upon client directed parameters accurately.			
Description of Control Activity		**Test of Controls**	**Test Results**
1.01	Novologix configurations Team policies and procedures guide Prior Authorization protocol configuration including requirements, testing, approvals and deployment.	Inspected documentation to determine whether policies and procedures are in place to guide personnel through the prior authorization configuration process.	No deviations noted
1.02	Changes to client configurations (i.e., drug list, fee schedule/pricing, claims edits, and prior authorization protocols) are documented within a change support ticket and authorized by the client and/or authorized account representative.	For a sample of client configuration changes (i.e. drug list, fee schedule/pricing, claims edits, and PA protocols) made to the Novologix system, inspected change support tickets to determine whether the implemented change made was documented and authorized by the client or account representative.	No deviations noted
1.03	Configuration changes go through review and internal testing by Novologix (i.e., QA or Novologix Configurations Team) and/or the client, as applicable, prior to implementation in production.	For a sample of client configuration changes (i.e. drug list, fee schedule, claims edits, and prior authorization protocols) made to the Novologix system, inspected change support tickets and test results documentation to determine whether the configurations were tested by the QA team and client, if applicable, prior to implementation in production.	No deviations noted

Control Objective 1:			
Controls provide reasonable assurance that client configurations (i.e. drug list, fee schedule/pricing, and PA protocols) are implemented in the Novologix system based upon client directed parameters accurately.			
Description of Control Activity		**Test of Controls**	**Test Results**
1.04	Configuration changes to the Novologix system (fee schedules/pricing, claims edits, drug list, and prior authorization protocols) are reviewed and approved by Novologix Management and/or the client, as applicable, prior to implementation in production.	For a sample of configuration changes made to the Novologix system, inspected change support tickets to determine whether the change requests were documented, reviewed and approved by Novologix Management, and the client as applicable, prior to implementation in production.	No deviations noted
1.05	The ability to make changes to client configurations within the production system is restricted to appropriate Novologix Clinical Configurations personnel.	Inspected the Novologix system access privileges to determine whether access to modify client configurations within the production Novologix system was restricted to appropriate user accounts accessible by personnel within the Clinical Configurations team.	**Deviations noted** Refer to deviation number 1 within **Appendix A** below for further details and Management's response.

Data Transmission, Input and Administration

Control Objective 2:			
Control activities provide reasonable assurance that the data received from clients is transmitted and loaded to be processed, accurately and completely.			
Description of Control Activity		**Test of Controls**	**Test Results**
2.01	Policies, standards and procedures are documented and made available to guide personnel in data transfer/input and acknowledgement activities.	Inspected the relevant policies, standards and procedures to determine whether data transfer and input policies and procedures were documented to guide personnel in data transfer/ input and acknowledgement activities.	No deviations noted
2.02	A SecureTransport sFTP site exists for client use and is used for transmittal of files (i.e. claims, provider, and eligibility). Data sources are restricted to client-specific folders on the SecureTransport server.	Inspected the SecureTransport site configurations to determine whether a sFTP server was in place for transmittal of files from clients.	No deviations noted
		Observed the folder structure of the SecureTransport server to determine whether data sources were restricted to client-specific, logically separated folders on the SecureTransport server.	No deviations noted

Control Objective 2:		
Control activities provide reasonable assurance that the data received from clients is transmitted and loaded to be processed, accurately and completely.		
Description of Control Activity	**Test of Controls**	**Test Results**
2.03 Automated jobs are configured to retrieve client-specific EDI claims files (837 or approved proprietary file format) from the SecureTransport server and place them in client-specific file server directories. A second automated job then moves and renames the files from the client-specific directories into an Inbound Transactions directory. The program is configured to notify Novologix IT personnel if errors occur.	For a sample of client-related scheduled jobs, inspected the automated job configurations and job schedules to determine whether the automated file processing program was configured to: • move claim files from the sFTP server, or other specified client origin, to the client specific directories on the Novologix file server; • move and rename files from the client specific directories on the Novologix file server to an Inbound Transactions directory.	No deviations noted
	Inspected the folder structure of the Novologix file server to determine whether client-specific folders existed.	No deviations noted
	For a sample of client-related scheduled jobs, inspected the automated job program configurations to determine whether the automated jobs were configured to notify Novologix IT personnel if errors occurred.	No deviations noted

Control Objective 2:			
Control activities provide reasonable assurance that the data received from clients is transmitted and loaded to be processed, accurately and completely.			
Description of Control Activity		**Test of Controls**	**Test Results**
2.04	An automated integration and connectivity server is configured to pull EDI claim files as they are moved to the Inbound Transactions directory, perform syntactical quality checks and process the file as individual claims. The program is configured to notify Novologix IT personnel if failures or errors occur.	Inspected configurations for the automated integration and connectivity server to determine whether it was configured to pull claim files from the Inbound Transactions directory on the file server as they were added, perform syntactical level checks and process the claims through the Novologix application engine.	No deviations noted
		For an example file movement/processing through the Novologix system, observed the following: • File was automatically pulled from the configured Inbound Transactions directory. • Syntactical level checks appropriately stopped the movement/processing of the claims file upon determination of error/issue, and routed the file to a separate file directory for resolution, where Novologix IT personnel are notified.	No deviations noted

Control Objective 2:			
Control activities provide reasonable assurance that the data received from clients is transmitted and loaded to be processed, accurately and completely.			
Description of Control Activity		**Test of Controls**	**Test Results**
2.05	If elected by the client, an automated acknowledgment file is sent to either the client-specific folders on the CVS SecureTransport server or directly to a client sFTP location, indicating acceptance or rejection.	For an example client who elected to receive acknowledgments, inspected the automated file processing program to corroborate that it was configured to send an acknowledgement file to the client-specific folder on the SecureTransport server upon receipt of the file.	No deviations noted
		For an example client file movement, observed the automatic generation and sending of the acknowledgement file upon successful receipt of the claims file.	No deviations noted
2.06	Production Support personnel monitor claim input and file processing information on a real-time basis.	Observed the processing of a sample of claims through the Novologix system to determine whether Production Support personnel monitored claim input and file processing results in real-time, and the accurate status was displayed in the monitoring tool.	No deviations noted
2.07	Automated jobs are configured to detect and retrieve member eligibility files from the SecureTransport server, or other approved secure method of transmission, and load into the Novologix platform.	Observed the member eligibility file load process to determine whether an automated file processing program was configured to run jobs to detect and retrieve the client-specific member eligibility file from the SecureTransport server, or other approved secure method of transmission, and load into the Novologix production eligibility database.	No deviations noted

Claims Edit Processing

Control Objective 3:		
Controls provide reasonable assurance that processing of claims files is completed accurately.		
Description of Control Activity	**Test of Controls**	**Test Results**
3.01 The Novologix system is configured to apply edit recommendations, assign a claim number, and add messaging (reject, warn, inform) to the original claim based on the following configured claims edit categories, as elected by the client: • Pricing Recommendations • Prior Authorization to Claim Matching • Administrative Edits • Clinical Edits • Quantity Edits	Observed the processing of claims and assigning of claim numbers for a sample of edit recommendations within each of the following claims edit categories and inspected the processing results (edit recommendations applied) to determine whether the Novologix system appropriately performed edit validation checks and applied messaging to the claims in accordance with client plan specifications: • Pricing Recommendations • Prior Authorization to Claim Matching • Administrative Edits • Clinical Edits • Quantity Edits	No deviations noted

Control Objective 3:		
Controls provide reasonable assurance that processing of claims files is completed accurately.		
Description of Control Activity	**Test of Controls**	**Test Results**
3.02 The Novologix system can be configured to make claim pricing recommendations based on fee schedules provided by the client and add messaging (reject, warn, inform) to each claim.	For a sample of claims for a client approved drug, inspected the claim edit recommendation results and compared the results to the client defined requirements/fee schedule to determine whether the Novologix system applied applicable edit recommendation checks and messaging accurately to the claim.	No deviations noted
	Recalculated the pricing/fee amount for a sample claim to determine whether the amount was properly calculated and applied based on the fee schedule and drug list provided by the client and setup in Novologix.	No deviations noted
	For a sample claim in which a corresponding fee schedule, based on drug HCPCS on the claim, was not configured or was not active, inspected the claim edit recommendation results and compared the results to the client defined requirements to determine whether rejection messaging was appropriately applied to the claim.	No deviations noted
3.03 After being processed through the Novologix system, claims response files are assembled and automated jobs are configured to move the files from the file server to the client-specific sFTP directories.	Inspected the automated file processing program configurations and job schedule to determine whether the automated file processing program was configured to move claims response files from the file server to the client-specific directories on the sFTP server.	No deviations noted

Control Objective 3:		
Controls provide reasonable assurance that processing of claims files is completed accurately.		
Description of Control Activity	**Test of Controls**	**Test Results**
3.04 Individual "processed" claims within the Novologix system are re-assembled within the original claims file ("response file"). Prior to assembly, the System is configured to perform a completeness validation check to ensure the claims processed matches the claims received.	Inspected configurations in the Novologix system to determine whether completeness validation checks were performed upon completion of claims processing and prior to re-assembly.	No deviations noted
	For a sample claims file processed through the Novologix System in which the claims output/processed amount did not tie to the claims input/received amount, observed that the System performed the completeness validation check and identified the discrepancy, and confirmed that assembly of the claims response file was not initiated as the completeness validation check was not passed.	No deviations noted
	For a sample claims file processed through the Novologix System in which the claims output/processed amount matched the claims input/received amount, observed that the System initiated assembly of the claims response file automatically indicating that the claims file passed the completeness validation check.	No deviations noted

Prior Authorization Processing

Control Objective 4:			
Controls provide reasonable assurance that prior authorizations are processed accurately based on the client configured protocols, business rules and workflow.			
Description of Control Activity		**Test of Controls**	**Test Results**
4.01	The Novologix system is configured to perform a duplication check to prevent duplicate prior authorizations from being created for a member/patient based on drug, date of service and NPI (if elected).	Inspected the Novologix Prior Authorization default system configurations to determine whether the system was configured to perform a duplication check on the following data fields within a prior authorization form, per member/patient: • Drug • Date of service • NPI (if elected)	No deviations noted
		[Drug + Date of Service] For an example prior authorization, observed the Novologix system prevented the submission of the prior authorization for a drug with overlapping dates of service as that of a previously submitted prior authorization for the same member. Upon submission, also observed the system displayed an error message indicating the prior authorization submission attempt was a duplicate.	No deviations noted
		[Drug + Date of Service + NPI] For an example prior authorization, observed the Novologix system prevented the submission of the prior authorization for a drug with overlapping dates of service as that of a previously submitted prior authorization for the same member and same provider (NPI). Upon submission, also observed the system displayed an error message indicating the prior authorization submission attempt was a duplicate.	No deviations noted

Control Objective 4:			
Controls provide reasonable assurance that prior authorizations are processed accurately based on the client configured protocols, business rules and workflow.			
Description of Control Activity		**Test of Controls**	**Test Results**
4.02	The Novologix system is configured to prevent the creation of a prior authorization for a member or provider that is not setup or is deactivated within the system.	Observed a user attempt to create an example prior authorization and confirmed that the Novologix System prevented the creation of a prior authorization for a member and provider that were not setup (loaded) in the system.	No deviations noted
		Observed a user attempt to create an example prior authorization and confirmed that the Novologix System prevented the creation of a prior authorization for a deactivated/terminated member and provider within the system.	No deviations noted
		Observed a user attempt to create an example prior authorization for an active/valid member and provider and confirmed that the Novologix System successfully created a prior authorization for the member and provider selected.	No deviations noted
4.03	The Novologix system is configured to restrict updating of member demographic and eligibility information (member name, date of birth, gender, group #, effective and term dates) within the application directly.	Observed the Novologix system was configured to restrict users from modifying member demographic and eligibility information directly within the application.	No deviations noted

Control Objective 4:			
Controls provide reasonable assurance that prior authorizations are processed accurately based on the client configured protocols, business rules and workflow.			
Description of Control Activity		**Test of Controls**	**Test Results**
4.04	Upon completion of the protocol question set, a prior authorization request is evaluated using the Novologix clinical algorithm and can result in the following status: • Approved • Require additional clinical review • Pend for clinical validation of medical records • Denied	Inquired of management regarding the prior authorization process to determine whether the Novologix system was configured to process prior authorizations according to parameters that included client specific business rule parameters, criteria and protocol question sets.	No deviations noted
		Inspected the Novologix prior authorization workflow configurations for an example client to corroborate that the system was configured to generate a prior authorization status in accordance with the results of the prior authorization form submission based on the information entries and protocol question set responses.	No deviations noted
		For a sample prior authorization submission, observed the accurate status resulted based on the information entries and protocol question set responses, in accordance with client configurations (decision tree established for drug).	No deviations noted
4.05	The Novologix system displays the prior authorization status during the course of the prior authorization process. Once a prior authorization request is in an approved or denied status, an automated job routes the information to a	Inspected the Novologix system for an example prior authorization to determine whether the application displayed the prior authorization status during the course of the submission/review.	No deviations noted

Control Objective 4:			
Controls provide reasonable assurance that prior authorizations are processed accurately based on the client configured protocols, business rules and workflow.			
	Description of Control Activity	**Test of Controls**	**Test Results**
	subsystem for letter notifications.	Inspected the Novologix system prior authorization queues to determine whether the application displayed the prior authorization status during the course of the submission/review and that errors noted or requiring action noted during the prior authorization submission/review process were flagged and moved into an exception queue for additional review, based on the defined workflow.	No deviations noted
4.06	The Novologix System automatically routes prior authorizations that do not result in auto-approval and require further clinical review to the appropriate clinical review team based on the established workflow. For delegated clients, the PA is routed to the Case Review Unit (CRU) queue based on role assignment.	For an example prior authorization that resulted in a status of "Requires Clinical Review", observed that the prior authorization was automatically moved into the "Case Review Unit" workflow queue. Additionally, observed that only users assigned to the applicable "Case Review" role in the Novologix system were able to modify the prior authorization to change the status to approved or denied.	No deviations noted
	For non-delegated clients, the PA is routed to the appropriate queue based on role assignment, as determined by the client during implementation. Following the client's clinical review, a decision is rendered and entered into the Novologix System (Approved or Denied).	Observed users with access to modify the workflow configuration and determined the users were appropriate and restricted to areas defined by their role.	No deviations noted

Control Objective 4:			
Controls provide reasonable assurance that prior authorizations are processed accurately based on the client configured protocols, business rules and workflow.			
Description of Control Activity		**Test of Controls**	**Test Results**
4.07	Denied PAs are only able to be modified (i.e. change in result/decision based on inputs or via clinical review) by going through the appeal process within the Novologix System, in which a PA is notated as an appeal to the original PA.	Observed the configuration within the Novologix System to determine that denied PAs are only able to be modified by going through the appeal process.	No deviations noted

Logical Security

Control Objective 5:			
Controls provide reasonable assurance that logical access to data, programs, and computer resources is restricted to authorized and appropriate individuals.			
	Description of Control Activity	**Test of Controls**	**Test Results**
5.01	Information Security has documented and communicated security policies that define the requirements, responsibilities, and expectations of individuals that have been granted access to Information Security resources.	Inspected information security policies to determine whether requirements, responsibilities, and expectations of individuals with access to Information Security resources exist and were communicated through the corporate intranet site.	No deviations noted
5.02	Procedures exist to govern timely actions related to requesting, establishing, issuing, suspending, and disabling user accounts.	Inspected the User Access Management Procedure for Information Security Identity Access Management policy governing user access to determine whether they were documented, reviewed, and approved.	No deviations noted
5.03	Novologix User Provisioning (NUP) requires the completion of User Access Request forms for adding, modifying or removing user access. The forms are required to be approved by the user's functional leader and when applicable by the NUP Supervisor before access is granted. Upon granting user access, forms are retained as documentation within the ticketing system.	For a sample of users granted or modified access to the Novologix system, inspected user access request forms to determine whether the forms were approved by the user's functional leader, and NUP Supervisor as applicable, and access was provisioned as requested.	No deviations noted

Control Objective 5:			
Controls provide reasonable assurance that logical access to data, programs, and computer resources is restricted to authorized and appropriate individuals.			
Description of Control Activity		**Test of Controls**	**Test Results**
5.04	Access to the Novologix system is removed for terminated employees and/or any user no longer requiring access to the Novologix system upon notification of termination/access removal request.	For a sample of terminated employees with access to the Novologix system, inspected system evidence to determine whether access was removed promptly.	No deviations noted
5.05	Access to the corporate network for terminated employees is removed through an automated script within 72 hours based on notification from HR or Strategic Procurement.	Inspected the script configuration settings to determine whether the script identified terminated employees automatically disabled the associated corporate network account upon receipt of termination notification.	No deviations noted
		For a sample of terminated employees, inspected system evidence to determine whether network accounts were revoked or disabled within 72 hours of notification from HR or Strategic Procurement.	No deviations noted
5.06	Access to the network for terminated contractors is set to automatically expire at a specific end date approved as part of the access request or extension process. The end date cannot be set beyond the date of the contractor agreement.	For a sample of contractors, inspected the account expiration within Oracle Identity Manager (OIM) to determine whether the user IDs were set to automatically expire at a specific end date approved by the user's manager. If a selected contractor's account expired during the period, inspected the Active Directory listing to confirm their access was revoked.	No deviations noted

Control Objective 5:			
Controls provide reasonable assurance that logical access to data, programs, and computer resources is restricted to authorized and appropriate individuals.			
Description of Control Activity		**Test of Controls**	**Test Results**
5.07	A user ID and password are required to authenticate to the in-scope applications and network, including supporting operating systems and databases. Password composition and lockout settings are in place, as defined in Caremark's logical access policies and standards.	Observed that a user ID and password were required to authenticate to the Caremark network and Novologix production systems (application, database, operating system).	No deviations noted
		Inspected the password configurations for the Caremark network and Novologix production systems (operating system, database and application) to determine whether settings were appropriate and in compliance within Caremark's logical access policies and standards.	No deviations noted
5.08	Application, database, and operating system access is reviewed at least annually, based on risk, to assess and confirm whether rights and privileges (greater than read-only) are restricted to appropriate personnel based on job responsibilities.	For the Novologix production systems (applications, databases, and operating systems), inspected supporting evidence to determine whether a review over the related application, database, and operating system levels of access was scheduled and performed by Application Management in accordance with defined frequencies.	No deviations noted
		Inspected supporting evidence for the Novologix production systems (applications, databases, and operating systems) to determine whether the review over the related application, database, and operating system levels of access was performed with the appropriate level of precision, and whether any access that was found to be unnecessary was revoked.	No deviations noted

Control Objective 5:			
Controls provide reasonable assurance that logical access to data, programs, and computer resources is restricted to authorized and appropriate individuals.			
Description of Control Activity		**Test of Controls**	**Test Results**
5.09	Formal security standards and minimum-security baselines have been developed for the in-scope operating systems and databases. The security standards and minimum-security baselines are reviewed at least biennially and updated (if needed) by Information Security and sent to the relevant system owner for final approval.	Inspected the security standards and minimum security baselines for in-scope operating systems and databases to determine whether they existed.	No deviations noted
		Inspected the security standards and minimum-security baselines developed for in scope operating systems and databases to determine whether they have been reviewed and updated (if needed) by Information Security, and approved on a biennial basis by the system owners.	No deviations noted
5.10	Management performs an annual review of operating systems and databases to ensure configuration settings for in-scope production systems are in compliance with the defined Corporate minimum security baselines and that out-of-compliance configurations are corrected appropriately.	For a sample of operating system and database servers, inspected the corresponding annual review documentation and configuration settings to determine whether IT Management completed their review of the configuration settings for compliance with minimum security baselines and that any out-of-compliance configurations identified were remediated.	No deviations noted

Program Change

Control Objective 6:		
Controls provide reasonable assurance that: ***(a) changes to application programs and related data management systems are authorized, tested, documented, approved and implemented to result in complete, accurate, and timely processing and reporting of transactions and balances; and*** ***(b) changes to infrastructure (i.e., system software and hardware configuration) are authorized to enable applications and application controls to operate effectively, protect data from unauthorized changes and support segregation of duties.***		
Description of Control Activity	**Test of Controls**	**Test Results**
6.01 Formal policies and procedures have been developed to guide application development and support personnel in the development and modification of application, database, and infrastructure systems including requirements around emergency changes, approvals, and release schedules.	Inspected policies and procedures to determine whether documented procedures governing changes to production systems existed and included requirements around the development of changes, emergency change requirements, approvals, and release schedules.	No deviations noted
6.02 A change record for routine and emergency changes is documented for all in-scope systems (i.e. applications, operating systems, and databases).	For a sample of routine and emergency changes, inspected the change record to determine whether the implemented change was documented.	No deviations noted
6.03 Testing, including User Acceptance Testing (UAT) where applicable, is performed prior to implementing a change to production.	For a sample of changes, inspected relevant ticket and testing documentation to determine whether changes were tested prior to implementation into production.	No deviations noted
6.04 Changes to application, operating system, and database are approved by appropriate business and/or	For a sample of changes, inspected the relevant tracking records (HPSM and/or TFS) to determine whether manager, CAB, and/or senior	No deviations noted

Control Objective 6:

Controls provide reasonable assurance that:

(a) changes to application programs and related data management systems are authorized, tested, documented, approved and implemented to result in complete, accurate, and timely processing and reporting of transactions and balances; and

(b) changes to infrastructure (i.e., system software and hardware configuration) are authorized to enable applications and application controls to operate effectively, protect data from unauthorized changes and support segregation of duties.

	Description of Control Activity	Test of Controls	Test Results
	system owners in accordance with Caremark policy.	management approvals were provided, as applicable.	
6.05	Testing is performed by independent testers on system infrastructure upgrades and patches in a test environment and authorized by the CAB before changes are migrated to production.	For a sample of system infrastructure (i.e., operating system and database) upgrades and patches, inspected ticket support to determine whether they were independently tested and authorized by the CAB prior to deployment into production environments.	No deviations noted
6.06	Regression tests follow code changes in the Novologix application prior to a monthly major//minor release. Any differences between previous code cycle execution and the next code push that are identified by the QA Team, are then reported to the development team to validate the code and to remediate any identified problems/errors. Differences noted as a result of regression testing are communicated to system owners for resolution.	For a sample of releases, inspected the regression tests for the Novologix program changes to determine whether regression testing was performed, results were properly documented and communicated to system owners, and errors were appropriately investigated and resolved by the system owners.	No deviations noted
6.07	Segregation of duties has been established between the assigned Change Executor, responsible for enforcing the change management process	Inspected the system generated user listings within the in-scope applications and change management tools and inquired of IS Management to determine	No deviations noted

Control Objective 6:			
Controls provide reasonable assurance that: ***(a) changes to application programs and related data management systems are authorized, tested, documented, approved and implemented to result in complete, accurate, and timely processing and reporting of transactions and balances; and*** ***(b) changes to infrastructure (i.e., system software and hardware configuration) are authorized to enable applications and application controls to operate effectively, protect data from unauthorized changes and support segregation of duties.***			
Description of Control Activity		**Test of Controls**	**Test Results**
	and moving the change to production, and the individuals responsible for coding and testing the change.	whether segregation of duties was established between those users with the ability to migrate changes into the production environment and those responsible for coding and testing of changes.	
6.08	Development and production environments are logically separated.	Inquired of Management regarding the separation between development, QA, and production environments to determine whether the environments were logically separated.	No deviations noted
		Inspected the listing of production, QA, and development servers to determine whether the environments were logically separated.	No deviations noted
6.09	Application file modification reports are generated by the File Integrity Monitoring (FIM) tool, or manually for servers not compatible with FIM, and reviewed for appropriateness by Application Managers, as per CVS Health policy.	Inspected the configuration of the FIM tool to determine whether the tool was configured to scan critical production libraries and directories for the Novologix system.	No deviations noted
		For a sample change captured in the FIM tool, inspected FIM tool and supporting evidence to determine whether the review was performed timely and appropriately.	No deviations noted
		Inspected the listing of users with administrative account access to modify and update the FIM tool and inquired of Application	No deviations noted

Control Objective 6:		
Controls provide reasonable assurance that: ***(a) changes to application programs and related data management systems are authorized, tested, documented, approved and implemented to result in complete, accurate, and timely processing and reporting of transactions and balances; and*** ***(b) changes to infrastructure (i.e., system software and hardware configuration) are authorized to enable applications and application controls to operate effectively, protect data from unauthorized changes and support segregation of duties.***		
Description of Control Activity	**Test of Controls**	**Test Results**
	Management to determine whether access was restricted to appropriate users based on their job responsibilities.	

Job Scheduling

Control Objective 7:			
Controls provide reasonable assurance that application and system processing are authorized and executed in a complete, accurate, and timely manner, and processing interruptions are identified, documented and resolved.			
Description of Control Activity		**Test of Controls**	**Test Results**
7.01	Policies and procedures exist for the processes (i.e. monitoring, back-ups, support, and incident management) within Computer Operations.	Inspected the Quality System Process and Procedures to determine whether documented procedures governing Computer Operations existed.	No deviations noted
7.02	Production Support monitor batch jobs for exceptions / failures. Failed jobs are detected through real time notification by the systems or though daily review of logs of job completion, as instructed/requested. Job failures are investigated and re-run as instructed if necessary by Production Support.	For a sample of scheduled production jobs, inspected the job scheduling tool to determine whether scheduled production jobs were configured to automatically notify Production Support personnel upon failure.	No deviations noted
		For a sample of failed jobs, inspected evidence to ascertain that failed jobs were investigated and rerun or escalated for resolution.	No deviations noted
7.03	The ability to create, modify, and delete job schedules are restricted to appropriate personal based on job responsibilities.	Inspected the users listing for the in-scope job schedulers and inquired of IT Management to determine whether the ability to create, modify, and delete job schedules was restricted to appropriate IT and Operations personnel based on job responsibilities.	No deviations noted
7.04	Production issues are escalated to the appropriate support team and an accompanying ticket is completed that identifies the problem and action taken. The tickets are investigated and tracked through to resolution.	For a sample of job failures (i.e., production issues), inspected the associated tickets and supporting documentation to determine whether issues were documented, communicated to necessary parties, and resolved.	No deviations noted

System Backup

Control Objective 8:			
Controls provide reasonable assurance that program and data are backed up to permit restoration of applications and processing in the event of the destruction of the applications or data.			
Description of Control Activity		**Test of Controls**	**Test Results**
8.01	Backups are conducted in a timely manner for applicable in-scope applications and supporting databases and operating systems.	Inspected the backup policies and procedures to determine whether documented procedures governing applicable applications, databases and operating systems existed.	No deviations noted
		Inspected the configuration settings within the backup software tools to determine whether the relevant in-scope application, database and operating systems were configured to backup appropriately. *Refer to Control Objective 7 for controls related to monitoring and resolution of job failures.*	No deviations noted
8.02	Backup data is replicated real time to the Woonsocket, Rhode Island, Data Center.	Inspected the real-time replication system configuration and the most recent disaster recovery test results to determine whether production data for relevant in-scope applications was replicated real time to the Woonsocket, Rhode Island, Data Center.	No deviations noted

Physical Security

Control Objective 9:			
Controls provide reasonable assurance that physical access to computer equipment, and other resources, are adequately controlled and restricted to authorized and appropriate individuals.			
Description of Control Activity		**Test of Controls**	**Test Results**
9.01	A badge access system is used to control and restrict access to Caremark Data Centers. Each user is assigned an access badge with a unique identification number that is recorded each time the badge is used. The system's control panel is secured in a locked cabinet.	Observed the entry points to the in-scope Data Centers were restricted with badge readers and required a valid badge for entry.	No deviations noted
		Observed the badge access system log to determine whether users' activities were recorded with their corresponding unique identification numbers.	No deviations noted
		Observed the access control panel for the card access control application to determine whether the control access panel was stored within a secured and locked cabinet.	No deviations noted
9.02	Asset Protection or designated facility personnel grants access to sensitive Caremark facilities (e.g., Data Centers, server rooms) based on request forms approved by Operations and Information Systems (IS) Management.	For a sample of personnel granted access to the in-scope Data Centers and server rooms, inspected request forms to determine whether access was approved by Operations and IS Management and granted as approved.	**Deviations noted** Refer to deviation number 2 within **Appendix A** below for further details and Management's response.

Control Objective 9:			
Controls provide reasonable assurance that physical access to computer equipment, and other resources, are adequately controlled and restricted to authorized and appropriate individuals.			
Description of Control Activity		**Test of Controls**	**Test Results**
9.03	A list of personnel with access to Data Centers and/or server rooms is generated monthly and reviewed by designated IT Management for ongoing appropriateness of access. Discrepancies are followed up and resolved.	For a sample of months, inspected access review documentation for each of the in-scope Data Centers and server rooms to determine whether the reviews were performed by designated IT Management and any discrepancies were followed up on and resolved.	**Deviations noted** Refer to deviation number 3 within **Appendix A** below for further details and Management's response.
9.04	Security guards and video cameras are used to monitor physical access to sensitive areas.	For each of the in-scope facilities, observed that security guards and video cameras were present and used to monitor physical access to sensitive areas.	No deviations noted
9.05	Termination details for full-time employees and contract workers are sent to Asset Protection and other individuals responsible for deactivating badges. These documents are used to confirm all terminated employee and contractor physical access has been deactivated in a timely manner.	For a sample of full-time employee and contractor terminations, inspected termination requests and the physical badge system to determine whether the termination notification was sent to Asset Protection and physical access was deactivated in a timely manner.	No deviations noted

Management Response to Testing Deviations – Appendix A

Ref #	Control Objective	Deviation Information
1	Client Configuration Changes	**Control specified by Caremark** 1.05 - The ability to make changes to client clinical configurations within the production system is restricted to appropriate Novologix Clinical Configurations personnel. **Results of testing performed** For 2 of 35 users (representing the full population) with access to make configuration changes, the access was identified as inappropriate due to the users' job roles. For the two users, we performed the following procedures: 1) inquired of the employee's Supervisor to confirm that the employee's access to the role in the system was authorized; 2) inquired of Management to validate that the access was authorized at one point due to business justification; 3) inspected the periodic access review performed to validate that the user's access was confirmed as authorized at one point and had a valid business justification at the time of the review; 4) inspected system change logs to validate that the two users did not inappropriately utilize the access to make configuration changes during the period; 5) inspected system evidence to validate the user access was revoked following Management determination of alternative solution. **Management's response** For the users noted within the deviation, Management agrees that the two users were granted access to one user role that had the capability to make configuration changes within the system. This user role also allows approved users to "view" specific configurations or changes in the system that may not have been promoted to Production and/or are suppressed on the user interface (e.g., back-end system NDC and mapping updates). The users were authorized and granted the role to perform monitoring duties of their respective client environment configurations. Due to system limitations, a view-only sub-role to perform the necessary activities was not available in the system. Management accepted the risk of granting the role to the two users for the intermediary period until a more formal and permanent solution was developed to allow the users to carry out their business duties, on the basis that the following procedures, processes, controls and factors reduce and mitigate the risk: • Documented procedures exist and are enforced for the configuration change process (as described in controls 1.02 – 1.04), and a multi-level testing/QA process is established within Novologix to control changes from being promoted to the Production environment by unauthorized individuals.

Ref #	Control Objective	Deviation Information
		• Management performed a periodic review of change and access logs to validate that the users did not make any inappropriate configuration changes to the system. • For both users noted within the deviation, Management developed an alternative solution to allow the business monitoring activity to be performed without this role assignment, and their access was immediately revoked by Novologix User Provisioning thereafter.
2	Physical Security	**Control specified by Caremark** 9.02 - Asset Protection or designated facility personnel grants access to sensitive Caremark facilities (e.g., Data Centers, server rooms) based on request forms approved by Operations and Information Systems (IS) Management. **Results of testing performed** For 1 of 43 new physical access roles tested, the new role granted to the Shea data center did not have formal approval. Further, the access was determined to be inappropriate based on the employee's job responsibilities. Per inspection of the data center access listing generated on 3/1/2019, the access was subsequently revoked. **Management's response** Management agrees that formal approval and related documentation of approval over access requests should have been followed and maintained. Access was inappropriately provisioned as a result of human error. The employee's provisioned access was limited to the check cage room within the Data Center, which can only be reached through additional access levels through the initial doors to enter the data center that the employee was not provisioned with. The access for this individual was also for an area that is staffed 24x7x365 and monitored by surveillance cameras. Management has since re-enforced the physical access provisioning procedures with relevant personnel.

Ref #	Control Objective	Deviation Information
3	Physical Security	**Control specified by Caremark** 9.03 - A list of personnel with access to Data Centers and/or server rooms is generated monthly and reviewed by designated IT Management for ongoing appropriateness of access. Discrepancies are followed up and resolved. **Results of testing performed** For 2 of 4 months tested, the reviews were not completed in a precise manner as not all roles granted access to the Shea data center were reviewed. **Management's response** Management agrees that the review over physical access to the data center should have captured the inappropriate access to the check cage. This impacted one (1) CVS employee of the 138 users with access to the Shea Data Center. The employee not identified was an individual whose access was limited to the check cage room within the Data Center, which can only be reached through additional access levels through the initial doors to enter the data center that the employee did not possess. The access for this individual was also for an area that is staffed 24x7x365 and monitored by surveillance cameras. Management has since re-enforced the physical access provisioning procedures with relevant personnel.

Section V. Other Information Provided by Novologix, L.L.C.

Other Information Provided by Novologix, L.L.C.

The information in this section is presented by Novologix to provide additional information and is not a part of Novologix's Description that may be relevant to the user organization's internal control. This information has not been subject to the procedures applied in the examination of the description. Novologix, LLC is a wholly owned indirect subsidiary of CVS Health. Caremark, L.L.C. is the entity that directly owns 100% of Novologix, L.L.C. which means Novologix is required to follow all HIPAA, disaster recovery, business continuity, emergency management and other information governance, privacy, risk standards, policies, procedures, methodologies and compliance regulations as defined by the CVS Health and Caremark enterprise.

5.1 Health Insurance Portability and Accountability Act (HIPAA)

5.1.1 General Compliance Statement

Caremark has developed and implemented policies and procedures to be in compliance with the regulations promulgated under HIPAA Privacy & Security Rules (effective for the CVS Health organization April 13, 2003), the statutory amendments under the Health Information Technology for Economic and Clinical Heath Ace (the HITECH Act or the act), and the HIPAA Transaction and Code Sets (effective for the CVS Health organization October 16, 2002).

5.1.2 Transactions and Code Sets

Caremark started accepting National Council for Prescription Drug Programs (NCPDP) Version D.0 transactions for the Retail Processing in July 2011. By March 2012, 100% of these transactions were received in this format. Novologix accepts NCPDP transactions.

5.1.3 Information Governance & Privacy

Our existing role code structure utilized to control data access is reviewed at least annually. Role codes for applications that possess PHI are designed with the HIPAA "minimum necessary" principle embedded throughout. Role codes are also subjected to a segregation of duties analysis and annual period access review exercise. The process by which system and application access is granted is managed by the Information Security's User Provisioning Team.

All disclosures involving PHI are logged by the Privacy Office in a disclosure reporting database (Archer). Investigations and assessments are also performed for each disclosure incident and centrally documented in the disclosure reporting database (Archer) as well. Disclosure accounting and risk assessment processes and procedures are compliant with both HIPAA and HITECH requirements.

5.1.4 Privacy Regulations

Caremark has developed and implemented privacy policies and procedures ensuring compliance with the requirement of the HIPAA Privacy Rule, including policies and procedures covering the use and disclosure of PHI, the minimum necessary requirement, safeguarding PHI, handling of individual requests, training of its workforce, and sanctions. Caremark has appointed a privacy officer to oversee its compliance with the HIPAA Privacy Rule, which also applies to the Novologix business unit.

5.1.5 HIPAA Security Standards

The goal of these standards is to address the uniform protection of health information that is either housed or transmitted electronically that pertains to an individual. Caremark's Information Security Organization is responsible for aligning Caremark and all its business entities (including Novologix) security standards to help ensure compliance with these regulations. The security regulations address 18 required standards categorized into three separate areas: (1) Administrative, (2) Physical, and (3) Technical.

5.1.6 HIPAA Unique Identifier Standards

The goal of these standards is to standardize the manner in which an entity identifies various individuals and/or groups. There are four types of identifiers anticipated by these standards: (1) Identifiers for employers (compliance date of July 30, 2004), (2) Provider identifiers (compliance date in May 2007), (3) Health plan identifiers (October 5, 2014), and (4) Individual identifiers (guidelines and compliance date pending).

5.1.7 Going Forward

Caremark is committed to integrating the ongoing review of rules and regulations related to HIPAA as part of their daily operations and ensuring that Caremark employees receive appropriate training necessary to perform necessary job functions with the end goal being the protection of its Participants' PHI.

5.2 Disaster Recovery (DR)

CVS Health recognized many years ago the importance of DR planning in the data centers that support our pharmacies, call centers, clients, and their members. DR plans have been in place since the late 1990's with continual exercising and updating as the environment changes.

CVS Health utilizes both an internal site and alternate site recovery strategy for the Shea Data Center, located in Scottsdale, Arizona. Critical business functions running in the Shea Data Center are being replicated real time to the CVS Health Woonsocket, Rhode Island Data Center and the SunGard Carlstadt, New Jersey, Data Center. Caremark contracts with SunGard Availability Services in Carlstadt, New Jersey, for use of their hot site (alternate site) of similar equipment in the event a disaster is declared.

The Shea Data Center is a critical part of the day-to-day business for Caremark. The computer hardware and software resident in the data center process well over three million claims each day from member pharmacies. The data center is a "hardened" facility designed to protect the computer systems and minimize any disruption to normal processing.

5.3 Business Continuity Plan(s)

Caremark and its business entities including Novologix have a comprehensive Business Continuity Management (BCM) program in place to ensure those commitments can be met during events or situations that may impact the ability to deliver products and services. The Caremark Business Continuity Plans provide activation criteria and procedures, implementation procedures, roles and responsibilities, communication requirements, call lists and procedures, recovery scenarios (loss of workplace, loss of technology, loss of staff, and loss of critical third party), dependencies resource requirements, and work around procedures. Caremark maintains redundant locations for Mail Service Pharmacy, Specialty Pharmacy, Customer Care Call Center, and Data Centers to ensure that client support functions are not interrupted in the event of a disaster.

5.4 Emergency Management Plan

Caremark established an Incident Management Program to provide a process to respond to an event (such as a drug recall, disruption of supply chain, or a natural disaster) that could impact clients, Plan Participants, or Caremark's Operations, including Novologix. The site Incident Management Program provides a clear and organized response and recovery framework for site leaders to effectively manage emergencies, disruptions, or situations that introduce risk to employees, business operations, information, and assets. In addition, a dedicated emergency management war room has been setup at the Northbrook, IL, facility (as well as a dedicated area in the Woonsocket, RI, facility) with an alternate war room established at the Bannockburn, IL, facility in case the Northbrook facility is not available. A dedicated 800 number and an on-call schedule have also been established.

5.5 Vendor Approval Process

To ensure authenticity of drugs from its suppliers, Caremark purchased prescription products directly from FDA licensed pharmaceutical companies or drug wholesalers licensed in the United States to distribute these prescription drugs. It is the responsibility of the drug wholesalers to ensure that drugs are purchased only from FDA licensed pharmaceutical companies or the manufacturer's Authorized Distributor of Record and sold/distributed to Caremark. Caremark's wholesalers certify that procured drugs have been purchased directly from the pharmaceutical manufacturer of from an Authorized Distributor of Record. If counterfeit drugs are identified, the suspected counterfeit drugs are quarantined until a full investigation is conducted.

5.6 Trademarks

Microsoft® and Windows® are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

Novologix and other products or Company names are used for identification purposes only and may be trademarks or service marks of their respective owners.

DB2® is a registered trademark of International Business Machines Corporation in the United States, other countries, or both.

Other products or Company names are used for identification purposes only and may be trademarks or service marks of their respective owners.