

## **Report of Independent Accountants**

To the Board of Directors  
CVS Caremark Corporation

We have examined CVS Caremark Corporation's (CVS Caremark) RxConnect Pharmacy Management Application release 7.2 (PMA), installed at CVS Caremark in its IT environment described on page 3 of this report, to determine whether, at December 31, 2012, the CVS Caremark PMA met the criteria applicable to a pharmacy management application set forth in the *Code of Federal Regulations* Title 21, *Food and Drugs*, Parts 1300, 1304, 1306, and 1311, "Electronic Prescriptions for Controlled Substances; Final Rule," established by the Drug Enforcement Administration (DEA) of the U.S. Department of Justice (PMA criteria). The PMA criteria are listed in Attachment A. Management of CVS Caremark is responsible for the CVS Caremark PMA meeting the PMA criteria. Our responsibility is to express an opinion on whether the CVS Caremark PMA met the PMA criteria at December 31, 2012, based on our examination.

We also have examined the effectiveness of CVS Caremark's controls, described in Schedule A relevant to the processing integrity and security of the CVS Caremark PMA during the period January 1, 2012, through December 31, 2012, based on the American Institute of Certified Public Accountants (AICPA)-Canadian Institute of Chartered Accountants (CICA) Trust Services Criteria for processing integrity and security. Management of CVS Caremark is responsible for maintaining the effectiveness of these controls. Our responsibility is to express an opinion on whether management maintained effective controls during the period January 1, 2012 through December 31, 2012, based on our examination.

Our examination was conducted in accordance with attestation standards established by the AICPA. Our examination of whether the CVS Caremark PMA met the PMA criteria included examining, on a test basis, evidence about whether the CVS Caremark PMA met the PMA criteria and performing such other procedures as we considered necessary in the circumstances. In examining whether the CVS Caremark PMA met the AICPA-CICA Trust Services Criteria for processing integrity and security, our examination included (1) obtaining an understanding of CVS Caremark's controls over the processing integrity and security of the CVS Caremark PMA; (2) testing and evaluating the operating effectiveness of those controls; and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our examinations provides a reasonable basis for our opinion. Our examinations do not provide a legal determination regarding whether the CVS Caremark PMA met the PMA criteria.

To provide additional information about our examination of whether the CVS Caremark PMA met the PMA criteria, on page 3 of our report we have provided a description of certain aspects of the CVS Caremark PMA configuration and supporting IT environment in to which our tests were performed. The proper functioning of an application depends on the IT environment in which it operates, such as the physical hardware, system software, and software configuration settings. Because of the dependency of an application on the IT environment, an application may not function as designed due to changes in the IT environment or the failure to make needed changes. The proper functioning of an application also depends on the proper execution of the application and functioning of its supporting IT environment. Furthermore, the projection of any conclusions, based on our findings, to other releases of the PMA is subject to the risk that the validity of such conclusions may be altered because of changes made to the PMA in other releases.

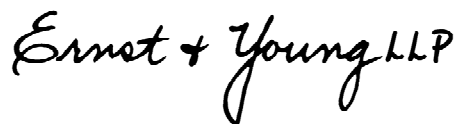
Because of the nature and inherent limitations of controls, CVS Caremark's ability for its PMA to meet the AICPA-CICA Trust Services Criteria for processing integrity and security may be affected. For example, controls may not prevent or detect and correct errors or fraud, unauthorized access to systems and information, and failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

In our opinion, as of December 31, 2012, the CVS Caremark PMA met the PMA criteria, in all material respects. Also, in our opinion, CVS Caremark maintained, in all material respects, effective controls over the processing integrity and security of the CVS Caremark PMA to provide reasonable assurance that

- the CVS Caremark PMA was protected against unauthorized access (both physical and logical) and
- the system processing was complete, accurate, timely, and authorized during the period January 1, 2012, through December 31, 2012,

based on the AICPA-CICA Trust Services Criteria for processing integrity and security criteria.

This report is intended solely for the information and use of CVS Caremark, the DEA, current customers using the CVS Caremark PMA, and prospective customers who are evaluating the CVS Caremark PMA for use in filling prescriptions for controlled substances and is not intended to be and should not be used by anyone other than these specified parties.

A handwritten signature in black ink that reads 'Ernst & Young LLP'.

January 17, 2013  
Boston, Massachusetts

**Description of Certain Aspects of the CVS Caremark PMA Configuration and IT Environment in which Ernst & Young, LLP Performed Tests of the CVS Caremark PMA**

The CVS Caremark RxConnect Pharmacy Management Application Release 7.2 (CVS Caremark PMA), developed in-house and managed by CVS Caremark (the Company), is used for supporting all aspects of the receipt and fulfillment of electronic prescriptions for controlled substances (EPCS) for the Company.

The information technology (IT) infrastructure supporting the CVS Caremark PMA is hosted and managed from the Company’s corporate data center facility located in Woonsocket, Rhode Island. A digital certificate authority application (used only for digital certificate checking and verification) which is considered part of the CVS Caremark PMA, is hosted and managed by a third party service provider, Verizon Business Services, located in Miami, Florida and Culpepper, Virginia. As part of their internal control, CVS Caremark management has designed and implemented policies and procedures that monitor and investigate (as necessary) the digital certificate checking and verification activities performed at Verizon Business Services.

The architecture that comprises the CVS Caremark PMA includes the following layers of technology:

Application Software / Function	Operating System	Database	Network Infrastructure
RxConnect Release 7.2 application software - internally developed application using a java based programming language.	AIX Operating system software - running AIX 6/1 TL 5 Service Pack 1	Oracle Database software - running version 10.2.0.4	LDAP Sun-Directory-Server/11.1.1.3.0  Cisco ASA 5550 firewall running ASA OS 8.2(5)13
Digital Certificate Checking and Verification	Integrated nCipher Cryptographic Module	N/A	
Event Logging (internally referred to as RxDatawarehouse)	AIX Operating system software - running AIX 6/1 TL 7 Service Pack 5	Oracle database software version 11.2.0.3	

Access to the CVS Caremark PMA is restricted to authorized internal CVS Caremark personnel only. Authentication to the RxConnect application layer of the CVS Caremark PMA is controlled through role-based security and the use of unique username, password composition rules using a combination of application based security and LDAP network protocol security features. Operating system, database and network layer authentication relies on the use of unique username and password.

CVS Caremark receives EPCS transactions electronically from the sending prescriber which are then automatically directed into a CVS staging area where they pass through a CVS managed firewall and routed to the Integrated nCipher Cryptographic Module for digital certificate checking and verification before being loaded next into the RxConnect application layer for additional prescription validation checks. Invalid prescriptions (not passing the verification checks) are denied and transmitted back to the sending prescriber. Valid prescriptions (passing the verification checks) are then processed and filled. All EPCS transaction activity (from initial receipt through completion of processing), including any modifications or changes to data and rejected records, are logged within a centralized logging server (RxDatawarehouse) for tracking/monitoring and reporting purposes. Management has developed formalized monitoring and oversight procedures that includes producing and reviewing reports on a daily basis for auditable events of transaction processing related activities as well as the digital certificate validation checking performed by Verizon Business Services.

## Attachment A — Pharmacy Management Application Criteria

The following pharmacy management application (PMA) criteria have been excerpted from the *Code of Federal Regulations* (CFR) Title 21, *Food and Drugs*, Parts 1300, 1304, 1306, and 1311, “Electronic Prescriptions for Controlled Substances; Final Rule,” established by the Drug Enforcement Administration of the U.S. Department of Justice. For brevity, only those sections of the rule that contain the PMA criteria have been included. Text that does not address the PMA criteria has been omitted and is indicated by asterisks (\* \* \* \*). In addition, reference to the word *must* has been deleted from the text because the term *must* is considered prescriptive as criteria are statements of facts.

### § 1311.205(b) Pharmacy application requirements.

The pharmacy application meets the following requirements:

- (1) The pharmacy application is capable of setting logical access controls to limit access for the following functions:
  - (i) Annotation, alteration, or deletion of prescription information.
  - (ii) Setting and changing the logical access controls.
- (2) Logical access controls are set by individual user name or role.
- (3) The pharmacy application digitally signs and archives a prescription on receipt or be capable of receiving and archiving a digitally signed record.
- (4) For pharmacy applications that digitally sign prescription records upon receipt, the digital signature functionality meets the following requirements:
  - (i) The cryptographic module used to digitally sign the data elements required by part 1306 of this chapter is at least FIPS 140-2<sup>1</sup> Security Level 1 validated.
  - (ii) The digital signature application and hash function complies with FIPS 186-3<sup>2</sup> and FIPS 180-3.<sup>1</sup>
  - (iii) The pharmacy application's private key is stored encrypted on a FIPS 140-2 Security Level 1 or higher validated cryptographic module using a FIPS-approved encryption algorithm.
  - (iv) For software implementations, when the signing module is deactivated, the pharmacy application clears the plain text password from the application memory to prevent the unauthorized access to, or use of, the private key.
  - (v) The pharmacy application has a time application that is within five minutes of the official National Institute of Standards and Technology time source.
- (5) The pharmacy application verifies a practitioner's digital signature (if the pharmacy application accepts prescriptions that were digitally signed with an individual practitioner's private key and transmitted with the digital signature).
- (6) If the prescription received by the pharmacy application has not been digitally signed by the practitioner and transmitted with the digital signature, the pharmacy application either:
  - (i) Verifies that the practitioner signed the prescription by checking the data field that indicates the prescription was signed; or
  - (ii) Displays the field for the pharmacist's verification.
- (7) The pharmacy application reads and retains the full DEA number including the specific internal code number assigned to individual practitioners authorized to prescribe controlled substances by the hospital or other institution, as provided in § 1301.22(c) of this chapter.
- (8) The pharmacy application reads and stores, and is capable of displaying, all information required by part 1306 of this chapter.
- (9) The pharmacy application reads and stores in full the information required under § 1306.05(a)<sup>2</sup> of this chapter. The pharmacy application either verifies that such information is present or displays the information for the pharmacist's verification.

---

<sup>1</sup> Federal Information Processing Standards (FIPS) are incorporated in the rule by reference in Section 1311.08.

<sup>2</sup> See footnote 1.

<sup>1</sup> See footnote 1.

- (10)The pharmacy application provides for the following information to be added or linked to each electronic controlled substance prescription record for each dispensing:
  - (i) Number of units or volume of drug dispensed.
  - (ii) Date dispensed.
  - (iii) Name or initials of the person who dispensed the prescription.
- (11)The pharmacy application is capable of retrieving controlled substance prescriptions by practitioner name, patient name, drug name, and date dispensed.
- (12)The pharmacy application allows downloading of prescription data into a database or spreadsheet that is readable and sortable.
- (13)The pharmacy application maintains an audit trail of all actions related to the following:
  - (i) The receipt, annotation, alteration, or deletion of a controlled substance prescription.
  - (ii) Any setting or changing of logical access control permissions related to the dispensing of controlled substance prescriptions.
  - (iii) Auditable events as specified in § 1311.215.
- (14)The pharmacy application records within each audit record the following information:
  - (i) The date and time of the event.
  - (ii) The type of event.
  - (iii) The identity of the person taking the action, where applicable.
  - (iv) The outcome of the event (success or failure).
- (15)The pharmacy application conducts internal audits and generates reports on any of the events specified in § 1311.215 in a format that is readable by the pharmacist. Such an internal audit may be automated and need not require human intervention to be conducted.
- (16)The pharmacy application protects the stored audit records from unauthorized deletion. The pharmacy application shall prevent modifications to the audit records.
- (17)The pharmacy application backs up the controlled substance prescription records daily.
- (18)The pharmacy application retains all archived records electronically for at least two years from the date of their receipt or creation and comply with all other requirements of § 1311.305

**§ 1311.210 Archiving the initial record.**

- (a) Except as provided in paragraph (c) of this section, a copy of each electronic controlled substance prescription record that a pharmacy receives is digitally signed by one of the following:
  - (1) The last intermediary transmitting the record to the pharmacy immediately prior to transmission to the pharmacy.
  - (2) The first pharmacy application that receives the electronic prescription immediately upon receipt.
- (b) If the last intermediary digitally signs the record, it forwards the digitally signed copy to the pharmacy.
- (c) If a pharmacy receives a digitally signed prescription that includes the individual practitioner's digital signature, the pharmacy application:
  - (1) Verifies the digital signature as provided in FIPS 186–3, as incorporated by reference in § 1311.08.
  - (2) Checks the validity of the certificate holder's digital certificate by checking the certificate revocation list. The pharmacy may cache the CRL until it expires.
  - (3) Archives the digitally signed record. The pharmacy record retains an indication that the prescription was verified upon receipt. No additional digital signature is required.

**§ 1311.215 Internal audit trail.**

- (a) The pharmacy application provider establishes and implements a list of auditable events. The auditable events, at a minimum, includes the following:

---

<sup>2</sup> **§ 1306.05 Manner of issuance of prescriptions.**

- (a) All prescriptions for controlled substances shall be dated as of, and signed on, the day when issued and shall bear the full name and address of the patient, the drug name, strength, dosage form, quantity prescribed, directions for use, and the name, address and registration number of the practitioner.

- (1) Attempted unauthorized access to the pharmacy application, or successful unauthorized access to the pharmacy application where the determination of such is feasible.
  - (2) Attempted or successful unauthorized modification or destruction of any information or records required by this part, or successful unauthorized modification or destruction of any information or records required by this part where the determination of such is feasible.
  - (3) Interference with application operations of the pharmacy application.
  - (4) Any setting of or change to logical access controls related to the dispensing of controlled substance prescriptions.
  - (5) Attempted or successful interference with audit trail functions.
  - (6) For application service providers, attempted or successful annotation, alteration, or destruction of controlled substance prescriptions or logical access controls related to controlled substance prescriptions by any agent or employee of the application service provider.
- (b) The pharmacy application analyzes the audit trail at least once every calendar day and generates an incident report that identifies each auditable event.

\* \* \* \* \*

**§ 1311.305 Recordkeeping.**

- (a) If a prescription is created, signed, transmitted, and received electronically, all records related to that prescription are retained electronically.
- (b) Records required by this subpart are maintained electronically for two years from the date of their creation or receipt. This record retention requirement shall not pre-empt any longer period of retention which may be required now or in the future, by any other Federal or State law or regulation, applicable to practitioners, pharmacists, or pharmacies.
- (c) Records regarding controlled substances prescriptions are readily retrievable from all other records. Electronic records are easily readable or easily rendered into a format that a person can read.

\* \* \* \* \*

**§ 1311.145 Digitally signing the prescription with the individual practitioner's private key.**

\* \* \* \* \*

- (f) If the electronic prescription is transmitted without the digital signature, the electronic prescription application checks the certificate revocation list of the certification authority that issued the practitioner's digital certificate. If the digital certificate is not valid, the electronic prescription application does not transmit the prescription. The certificate revocation list may be cached until the certification authority issues a new certificate revocation list.
- (g) When the individual practitioner digitally signs a controlled substance prescription with the private key associated with his own digital certificate obtained as provided under § 1311.105, the electronic prescription application is not required to digitally sign the prescription using the application's private key.

**Schedule A – Trust Services Processing Integrity and Security Criteria and Controls**

<b>Processing Integrity Criteria</b>		<b>Security Criteria</b>		<b>CVS Caremark Control</b>
P1.1	The entity's processing integrity and related security policies are established and periodically reviewed and approved by a designated individual or group.	S1.1	The entity's security policies are established and periodically reviewed and approved by a designated individual or group.	Processing integrity and related security policies exist and are reviewed, approved, and updated, if needed, by the responsible Senior Management owner on an annual basis.
P1.2	The entity's system processing integrity and related security policies include, but may not be limited to, the matters listed in Schedule B.	S1.2	The entity's security policies include, but may not be limited to, the matters listed in Schedule B.	Policies exist that include matters relating to system processing integrity and related security in accordance with Schedule B.
P1.3	Responsibility and accountability for developing and maintaining entity's system processing integrity and related system security policies; changes, updates, and exceptions to those policies are assigned.	S1.3	Responsibility and accountability for the entity's system security policies, and changes and updates to those policies, are assigned.	Senior Management is responsible and accountable for developing, maintaining and communicating policies related to security and processing integrity (including changes, updates and exceptions to existing policies) that define the requirements, responsibilities, and expectations.
P2.1	The entity has prepared an objective description of the system and its boundaries and communicated such description to authorized users.	S2.1	The entity has prepared an objective description of the system and its boundaries and communicated such description to authorized users.	CVS has prepared an objective description of the system and its boundaries and communicated such description to authorized users.

Processing Integrity Criteria		Security Criteria		CVS Caremark Control
P2.2	The processing integrity and related security obligations of users and the entity's processing integrity and related security commitments to users are communicated to authorized users.	S2.2	The security obligations of users and the entity's security commitments to users are communicated to authorized users.	Policies and procedures related to the processing integrity and security of the system (including updates and changes to those policies and procedure) are published and communicated to personnel responsible for implementing them through an internal intranet site.
				The CVS Caremark Information Security & Privacy organization provides education and ongoing training programs to users that address and communicate user's processing integrity and security commitments and obligations.
P2.3	Responsibility and accountability for the entity's system processing integrity and related security policies, and changes and updates to those policies, are communicated to entity personnel responsible for implementing them.	S2.3	Responsibility and accountability for the entity's system security policies and changes and updates to those policies are communicated to entity personnel responsible for implementing them.	Policies and procedures related to the processing integrity and security of the system (including updates and changes to those policies and procedure) are published and communicated to personnel responsible for implementing them through an internal intranet site.
				The CVS Caremark Information Security & Privacy organization provides education and ongoing training programs to users that address and communicate user's processing integrity and security commitments and obligations.
P2.4	The process for obtaining support and informing the entity about system processing integrity issues, errors and omissions, and breaches of systems security and for submitting complaints is communicated to authorized users.	S2.4	The process for informing the entity about breaches of the system security and for submitting complaints is communicated to authorized users.	A ticketing system is in place for users to report errors or defects in processing integrity and security breaches for appropriate investigation and resolution.
				The CVS Caremark Information Security & Privacy organization provides education and ongoing training programs that address user's processing integrity and security obligations, including the process for informing and reporting potential violations.
				Documentation and reporting exists for the identification of security breaches and formal problem resolution procedures are in place for escalating and resolving identified breaches.
				Daily, Information Security monitors and logs security activity across the network, and identified security violations are reported



Processing Integrity Criteria		Security Criteria		CVS Caremark Control
P2.5	Changes that may affect system processing integrity and system security are communicated to management and users who will be affected.	S2.5	Changes that may affect system security are communicated to management and users who will be affected.	Formal policies and procedures are documented and followed for change implementation, database environment management, technology infrastructure management, and emergency changes.
				Appropriate authorization sign-off on the design and request for changes (including relevant security considerations) to in-scope systems are obtained from IT and/or Business management prior to development.
				System changes are approved for production by a Manager, and a VP/Director (Off-Cycle or Emergency changes) or an appropriate member of the CCB (Planned changes).
				Educational training is provided to users of the system (if needed) upon completion of a production change release to provide awareness of functionality changes.
P3.1	Procedures exist to (1) identify potential threats of disruptions to systems operation that would impair system processing integrity commitments and (2) assess the risks associated with the identified threats.	S3.1	Procedures exist to (1) identify potential threats of disruption to systems operation that would impair system security commitments and (2) assess the risks associated with the identified threats.	A risk assessment is performed periodically to identify threats of disruption to system operations that would impair processing integrity commitments and assess the risks from these threats.
P3.2	The procedures related to completeness, accuracy, timeliness, and authorization of inputs are consistent with the documented system processing integrity policies.			System transactions must go through a series of edit and validation checks (e.g., digital certificate checking, valid DEA number, drug information, patient data, and prescriber information) to confirm the completeness, accuracy and authorization in accordance with system processing integrity policies prior to being inputted into the system.

Processing Integrity Criteria		Security Criteria	CVS Caremark Control
P3.3	The procedures related to completeness, accuracy, timeliness, and authorization of system processing, including error correction and database management, are consistent with documented system processing integrity policies.		A development methodology exists and is followed for all system, hardware, database and application changes and data conversions that includes required procedures for user involvement, testing, and approvals of system processing integrity features.
			The system is configured with logical access controls to limit access to operating systems, databases, and applications, including information not deemed public.
			A ticketing system is in place for users to report errors or defects in processing integrity of system transaction for appropriate investigation and resolution.
P3.4	The procedures related to completeness, accuracy, timeliness, and authorization of outputs are consistent with the documented system processing integrity policies.		Output reports of system transaction activities are generated and reviewed daily, consistent with defined policies.
			System processing integrity incidents are logged by the Quality group. Incidents are then analyzed, classified and reported to the Steering Committee during which recommendations and decisions regarding system processing are raised.
			Changes to output reports follow a change management process requiring change requests to be documented and for changes to be tested and approved.
P3.5	There are procedures to enable tracing of information inputs from their source to their final disposition and vice versa.		System transactions are assigned a unique identifier that is used for tracing of transactions from initial input, during system processing and in their final disposition.

Processing Integrity Criteria		Security Criteria		CVS Caremark Control
P3.6	Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters: a. Logical access security measures to restrict access to information resources not deemed to be public. b. Identification and authentication of users. c. Registration and authorization of new users. d. The process to make changes and updates to user profiles. e. Distribution of output restricted to authorized users. f. Restriction of logical access to offline storage, backup data, systems, and media. g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).	S3.2	Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters: a. Logical access security measures to restrict access to information resources not deemed to be public. b. Identification and authentication of users. c. Registration and authorization of new users. d. The process to make changes and updates to user profiles. e. Distribution of output restricted to authorized users. f. Restriction of access to offline storage, backup data, systems, and media. g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).	A review of operating system software, network configuration and database software is performed to ensure configuration settings and patch levels are in compliance with the Corporate minimum security baselines and that out-of-compliance configurations are corrected appropriately.
				A user ID and password (requiring length, expiration, history, and lockout restrictions) are required to access in-scope systems.
				Access requests are communicated by HR to IT via e-mail, at which point IT sets up a standard network account for the new employee. If additional access is needed to in-scope systems, separate documentation (e-mail, request form, or help desk ticket) must be completed and approved by the appropriate manager. Upon granting user access, all documentation is retained.
				An access review is performed at least annually to review and confirm access rights and privileges (including administrative level access) to in-scope operating systems, databases, and applications.
				The system is capable of setting logical access controls to limit access to operating systems, databases, and applications.
				Backups are stored in a protective environment (i.e., locked container) in the data center facility prior to being transported offsite and data backed up to tape is restricted to authorized personnel.
				Virtual private networking (VPN) software is used to permit remote access by authorized users. Users are authenticated through specific approved authentication mechanisms.
				IT removes network, application, operating system and database login credentials for all terminated users based on direct notification from the HR system.

Processing Integrity Criteria		Security Criteria		CVS Caremark Control
P3.7	Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.	S3.3	Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.	Technology equipment supporting the production environment (e.g., servers, firewalls, routers, etc) are stored within a secured data center facility protected by a badge access system.
				Corporate Security or designated facility personnel grant access to the data center facility based on request forms approved by management.
				A list of personnel with access to the data center facility is generated semi-annually and reviewed by designated IT management for ongoing appropriateness of access.
				Video cameras are used to monitor physical access to the data center facility where computer equipment is operating.
				Backups are stored in a protective environment (i.e., locked container) in the data center facility prior to being transported offsite and data backed up to tape is restricted to authorized personnel.

Processing Integrity Criteria		Security Criteria		CVS Caremark Control
P3.8	Procedures exist to protect against unauthorized access to system resources	S3.4	Procedures exist to protect against unauthorized access to system resources.	A user ID and password (requiring length, expiration, history, and lockout restrictions) are required to access the production environment.
				A review of operating system software, network configuration and database software is performed to ensure configuration settings and patch levels are in compliance with the Corporate minimum security baselines and that out-of-compliance configurations are corrected appropriately.
				Firewalls are used and configured to prevent unauthorized access.
				Virtual private networking (VPN) software is used to permit remote access by authorized users. Users are authenticated through specific approved authentication mechanisms.
				Access requests are communicated by HR to IT via e-mail, at which point IT sets up a standard network account for the new employee. If additional access is needed to in-scope systems, separate documentation (e-mail, request form, or help desk ticket) must be completed and approved by the appropriate manager. Upon granting user access, all documentation is retained.
				The system is configured with logical access controls to limit access to operating systems, databases, and applications, including information not deemed public.
				Pharmacy store client PCs are connected to the Corporate network and RxConnect application through dedicated secure lines.
P3.9	Procedures exist to protect against infection by computer viruses, malicious codes, and unauthorized software.	S3.5	Procedures exist to protect against infection by computer viruses, malicious codes, and unauthorized software.	Symantec Anti-virus software is installed on applicable production servers and personal computers (PCs).
				Daily, Information Security monitors and logs security activity across the network, and identified security violations are reported.

Processing Integrity Criteria		Security Criteria		CVS Caremark Control
P3.10	Encryption or other equivalent security techniques are used to protect user authentication information and the corresponding session transmitted over the Internet or other public networks.	S3.6	Encryption or other equivalent security techniques are used to protect user authentication information and the corresponding session transmitted over the Internet or other public networks.	Firewall routing rules and leased lines are used and configured to protect data transmitted over external networks.
				Virtual private networking (VPN) software is used to permit remote access by authorized users. Users are authenticated through specific approved authentication mechanisms.
P3.11	Procedures exist to identify, report, and act upon system processing integrity issues and related security breaches and other incidents.	S3.7	Procedures exist to identify, report, and act upon system security breaches and other incidents.	Standard procedures exist for the review, documentation, escalation, and resolution of system processing problems.
				Documentation and reporting exists for the identification of security breaches and formal problem resolution procedures are in place for escalating and resolving identified breaches.
				System processing integrity incidents are logged by the Quality group. Incidents are then analyzed, classified and reported to the Steering Committee during which recommendations and decisions regarding system processing are raised.
P3.12	Procedures exist to classify data in accordance with classification policies and periodically monitor and update such classifications as necessary.	S3.8	Procedures exist to classify data in accordance with classification policies and periodically monitor and update such classifications as necessary	CVS Caremark classifies data stored within the system in accordance with defined requirements and updates such classifications as necessary.

Processing Integrity Criteria		Security Criteria		CVS Caremark Control
P3.13	Procedures exist to provide that issues of noncompliance with system processing integrity and related security policies are promptly addressed and that corrective measures are taken on a timely basis.	S3.9	Procedures exist to provide that issues of noncompliance with system security policies are promptly addressed and that corrective measures are taken on a timely basis.	System processing integrity incidents are logged by the Quality group. Incidents are then analyzed, classified and reported to the Steering Committee during which recommendations and decisions regarding system processing are raised, including corrective measures.
				Reporting exists for security breaches and formal problem resolution procedures are in place for escalating and resolving identified breaches.
				Standard procedures exist for the review, documentation, escalation, and resolution of system processing problems.
P3.14	Design, acquisition, implementation, configuration, modification, and management of infrastructure and software related to processing integrity and security are consistent with defined processing integrity and related security policies.	S3.10	Design, acquisition, implementation, configuration, modification, and management of infrastructure and software related to system security are consistent with defined system security policies to enable authorized access and to prevent unauthorized access.	Formal policies and procedures are documented and followed for change implementation, database environment management, technology infrastructure management, and emergency changes.
				A development methodology exists and is followed for all system, hardware, and application changes and data conversions that includes proper approval and communication of changes effecting the production environment.
				A review of operating system software, network configuration and database software is performed to ensure configuration settings and patch levels are in compliance with the Corporate minimum security baselines and that out-of-compliance configurations are corrected appropriately.
				System changes are approved for production by a Manager, and a VP/Director (Off-Cycle or Emergency changes) or an appropriate member of the CCB (Planned changes)

Processing Integrity Criteria		Security Criteria		CVS Caremark Control
P3.15	Procedures exist to provide that personnel responsible for the design, development, implementation, and operation of systems affecting processing integrity and security have the qualifications and resources to fulfill their responsibilities.	S3.11	Procedures exist to provide that personnel responsible for the design, development, implementation, and operation of systems affecting security have the qualifications and resources to fulfill their responsibilities.	Hiring procedures include a comprehensive screening of candidates for key positions and consideration of whether the verified credentials and experienced levels are commensurate with the proposed position and responsibility.
				New personnel are offered employment subject to background checks.
P3.16	Procedures exist to maintain system components, including configurations consistent with the defined system processing integrity and related security policies.	S3.12	Procedures exist to maintain system components, including configurations consistent with the defined system security policies.	Formal security standards and minimum security baselines have been developed for operating systems, databases and the network which support the objectives of the Security Policy. The security standards and minimum security baselines are reviewed at least annually and updated (if needed).
				A review of operating system software, network configuration and database software is performed to ensure configuration settings and patch levels are in compliance with the Corporate minimum security baselines and that out-of-compliance configurations are corrected appropriately.
P3.17	Procedures exist to provide that only authorized, tested, and documented changes are made to the system.	S3.13	Procedures exist to provide that only authorized, tested, and documented changes are made to the system.	Change requests (including emergency changes) are documented and authorized by IT and/or Business management prior to development.
				Testing, including user-acceptance testing where applicable, is performed prior to implementing a change to production.
				System changes are approved for production by a Manager, and a VP/Director (Off-Cycle or Emergency changes) or an appropriate member of the CCB (Planned changes).



Processing Integrity Criteria		Security Criteria		CVS Caremark Control
P3.18	Procedures exist to provide that emergency changes are documented and authorized (including after-the-fact approval).	S3.14	Procedures exist to provide that emergency changes are documented and authorized timely.	Appropriate authorization sign-off on the design and request for changes (including relevant security considerations) to in-scope systems are obtained from IT and/or Business management prior to development.
				System changes are approved for production by a Manager, and a VP/Director (Off-Cycle or Emergency changes) or an appropriate member of the CCB (Planned changes).
P3.19	Procedures exist to protect the system against potential risks (for example, environmental risks, natural disasters, and routine operational errors and omissions) that might impair system processing integrity.			The entity site is protected against a disruption in power supply to the processing environment by both uninterruptible power supplies and emergency power supplies. This equipment is tested semiannually.
				Preventive maintenance agreements and scheduled maintenance procedures are in place for key system hardware components.
				Environmental safeguards, including fire suppression equipment, separate HVAC systems to control temperature and humidity, and uninterruptible power supply (UPS) devices are in place where computer equipment is operating.
				Disaster recovery and contingency plans have been documented and are tested on a periodic basis. Testing results and recommendations are documented.
P3.20	Procedures exist to provide for restoration and disaster recovery consistent with the entity's defined processing integrity policies.			Disaster recovery and contingency plans have been documented and are tested on a periodic basis. Testing results and recommendations are documented.
P3.21	Procedures exist to provide for the completeness, accuracy, and timeliness of backup data and systems.			Data and systems are backed in a timely manner and backup failures are monitored by the Operations group.

Processing Integrity Criteria		Security Criteria		CVS Caremark Control
P4.1	System processing integrity and security performance is periodically reviewed and compared with the defined system processing integrity and related security policies.	S4.1	The entity's system security is periodically reviewed and compared with the defined system security policies.	Formal security standards and minimum security baselines have been developed for operating systems, databases and the network which support the objectives of the Security Policy. The security standards and minimum security baselines are reviewed at least annually and updated (if needed).
				A review of operating system software, network configuration and database software is performed to ensure configuration settings and patch levels are in compliance with the Corporate minimum security baselines and that out-of-compliance configurations are corrected appropriately.
				A review of EPCS transactions is performed on a daily basis to monitor activity by store and to identify any abnormalities in the processing of transactions.

Processing Integrity Criteria		Security Criteria		CVS Caremark Control
P4.2	There is a process to identify and address potential impairments to the entity's ongoing ability to achieve its objectives in accordance with its defined system processing integrity and related security policies.	S4.2	There is a process to identify and address potential impairments to the entity's ongoing ability to achieve its objectives in accordance with its defined system security policies.	Standard procedures exist for the review, documentation, escalation, and resolution of system processing problems.
				Reporting exists for security breaches and formal problem resolution procedures are in place for escalating and resolving identified breaches.
				System processing integrity incidents are logged by the Quality group. Incidents are then analyzed, classified and reported to the Steering Committee during which recommendations and decisions regarding system processing are raised.
				Daily monitoring is performed over defined auditable events which are reviewed for indication of breach or potential breach and identified issues are investigated and resolved.
P4.3	Environmental, regulatory, and technological changes are monitored, and their effect on system processing integrity and security is assessed on a timely basis; policies are updated for that assessment.	S4.3	Environmental, regulatory, and technological changes are monitored and their effect on system security is assessed on a timely basis and policies are updated for that assessment.	The entity's compliance group monitors the impact of applicable laws or regulations on the entity's processing integrity and related security policies and updates as necessary.
				Senior IT management reviews developments in technology and the impact on the entity's processing integrity and related security policies.
				Processing integrity and related security policies exist and are reviewed, approved, and updated, if needed, by the responsible Senior Management owner on an annual basis.
				Senior Management is responsible and accountable for developing, maintaining and communicating policies related to security and processing integrity (including changes, updates and exceptions to existing policies) that define the requirements, responsibilities, and expectations.

## Schedule B – Required Policy Components

Criteria Number	Security Component Description
S1.2.a	Identifying and documenting the security requirements of authorized users.
S1.2.b	Classifying data based on its criticality and sensitivity and that classification is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements.
S1.2.c	Assessing risks on a periodic basis.
S1.2.d	Preventing unauthorized access.
S1.2.e	Adding new users, modifying the access levels of existing users, and removing users who no longer need access.
S1.2.f	Assigning responsibility and accountability for system security.
S1.2.g	Assigning responsibility and accountability for system changes and maintenance.
S1.2.h	Testing, evaluating, and authorizing system components before implementation.
S1.2.i	Addressing how complaints and requests relating to security issues are resolved.
S1.2.j	Identifying and mitigating security breaches and other incidents.
S1.2.k	Providing for training and other resources to support its system security policies.
S1.2.l	Providing for the handling of exceptions and situations not specifically addressed in its system security policies.
S1.2.m	Providing for the identification of and consistency with applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements.
S1.2.n	Providing for sharing information with third parties.

<b>Criteria Number</b>	<b>Processing Integrity Component Description</b>
P1.2a	Identifying and documenting the system processing integrity and related security requirements of authorized users
P1.2b	Classifying data based on their criticality and sensitivity; that classification is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements
P1.2c	Assessing risks on a periodic basis
P1.2d	Preventing unauthorized access
P1.2e	Adding new users, modifying the access levels of existing users, and removing users who no longer need access
P1.2f	Assigning responsibility and accountability for system processing integrity and related security
P1.2g	Assigning responsibility and accountability for system changes and maintenance
P1.2h	Testing, evaluating, and authorizing system components before implementation
P1.2i	Addressing how complaints and requests relating to system processing integrity and related security issues are resolved
P1.2j	Identifying and mitigating errors and omissions and other system processing integrity and related security breaches and other incidents
P1.2k	Providing for training and other resources to support its system processing integrity and related system security policies
P1.2l	Providing for the handling of exceptions and situations not specifically addressed in its system processing integrity and related system security policies
P1.2m	Providing for the identification of and consistency with applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements
P1.2n	Providing for sharing information with third parties