2013

DEA 1311.205 Compliance Report for Pharmacy Application Providers as of September 21, 2013

Rx30 THE PHARMACY SYSTEM

ASSURANCE CONCEPTS
A SKODA MINOTTI ADVISORY FIRM

Table of Contents

SECTION 1: Independent Auditors Report on Applying Agreed-Upon Procedures

SECTION 2: Rx30 Pharmacy Application System Description

SECTION 1: Independent Auditors Report on Applying Agreed-Upon Procedures

To Management of Transaction Data Systems, Inc:

We have performed the procedures described below, which were agreed to by Transaction Data Systems, Inc. DBA Rx30, solely to assist in the identification of Compliance Assessment for DEA Part 1311.205 controls that were in place as of September 21, 2013, as set forth in the accompanying Schedule A. The maintenance of these controls is solely the responsibility of Rx30. Consequently, we make no representation regarding the sufficiency of the controls as a whole for Rx30 as described below either for the purpose for which this report has been requested or for any other purpose.

The controls and associated findings are as follows:

1. Compared Rx30's controls implemented in the pharmacy application Rx30 eScript 1.0 to applicable controls specified by the DEA Part 1311.205 pharmacy application requirements. Reviewed application operations and processes to verify that controls were in place and operating as of September 21, 2013.
   No exceptions were found as a result of this comparison.
2. Reviewed Rx30's controls implemented in the information security environment for the production system of Rx30's electronic prescription application services. Reviewed information security controls and processes to verify that controls were in place and operating as of September 21, 2013.
   No exceptions were found as a result of this comparison.
3. Reviewed Rx30's controls implemented in the physical security environment for the production system of Rx30's hosted electronic prescription application services. Reviewed physical security controls and processes to verify that controls were in place and operating as of September 21, 2013.
   No exceptions were found as a result of this comparison.

We were not engaged to and did not conduct an examination, the objective of which would be the expression of an opinion on the controls set forth in the accompanying Schedule A. Accordingly, we do not express such an opinion. Had we performed additional procedures, other matters might have come to our attention that would have been reported.

The description of controls at Rx30 is as of September 21, 2013, and any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the controls in existence. The potential effectiveness of specific controls at Rx30 is subject to inherent limitations and, accordingly, errors or fraud may occur and not be detected. Furthermore, 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.

We did not perform procedures to determine the operating effectiveness of controls for any period. Accordingly, we express no opinion on the operating effectiveness of any aspects of Rx30 controls, individually or in the aggregate.

This report is intended solely for the information of potential customer, existing customers, regulatory agencies and use by the management of Rx30 and is not intended to be and should not be used by anyone other than these specified parties.

Assurance Concepts, LLC

September 26, 2013

Company Overview and Services Provided

Transaction Data Systems ("TDS") was founded in January, 1977. Although the original focus was high end data communications software to the Airline reservation industry and Automated Teller Systems, TDS quickly found it's calling in the Pharmacy software dispensing market. In 1980, a local Florida pharmacy was looking to automate their daily processing activities and Rx30 was born.

For the past 34 years, Rx30 has been dedicated solely to the success of Independent Pharmacies. Today, Rx30 is proud to claim approximately 4,000 pharmacies that utilize our software for their prescription filling and management needs. With systems in all 50 states, ranging from Alaska to Hawaii and down to the Virgin Islands – Rx30 is an unquestioned leader in Independent Pharmacy Management Software.

The Rx30 Pharmacy System provides your pharmacy incomparable Prescription Filling, Nursing Home, Consulting, Accounts Receivable, Workflow Management, Signature Capture, IV processing, Compounding, Integrated POS Solutions and an abundance of value-added vendor interfaces to provide you a total turnkey dispensing solution. Whether you are a small independent start-up filling 30 prescriptions a day, or a 100+ independent chain operation filling 1,500 prescriptions a day.

Information Systems Overview

Rx30's information systems were built to facilitate the electronic dispensing of controlled substances used by a DEA registrant. Information systems contain prescription and dispensing information required by DEA regulations, digitally sign and verify digital signatures for the records of the prescription that is sent to the pharmacy, and maintain an internal audit trail of required auditable events. Rx30's information systems are comprised of an internal gateway managed by Rx30 and client server instances installed within the pharmacies.

Rx30 is a custom developed application that healthcare providers utilize to dispense electronic prescriptions for controlled substances. It resides at the Pharmacies, and prescriptions are routed from Emdeon, SureScripts to Relay Health (an intermediary), and then to Rx30's gateway. The gateway then validates the prescription for required fields, and only accepts prescriptions with a Signature Indicator ("SI") flag. Once confirmed, the system then transmits the prescription to the designated pharmacy. Rx30's hosted gateway is used for the delivery of their electronic prescriptions to the individual pharmacies from SureScripts through RelayHealth. Access is only granted to this gateway via a formal authorization process, and access is limited to authorized personnel. Rx30 remotely manages and supports the Pharmacy Applications that are installed locally at each pharmacy customer location.

Rx30's gateway is a Linux Centos environment with a proprietary Ctree database used for prescription related information. Data from EPCS is never stored in this database and is not consider in scope for the EPCS Pharmacy Application review. EPCS transactions are only temporarily stored in memory prior to passing to the corresponding pharmacy location.

Scope and Summary of Report

This report describes the control structure under the guidance of DEA Part 1311.205 for Rx30 as it relates to application and information security standards for their Electronic Pharmacy Application Services at their Ocoee, Florida facility. It is intended to assist Rx30's customers and potential customers in determining the adequacy of Rx30's internal controls. The scope of this assessment included the evaluation of the DEA Part 1311.205 Pharmacy Application Requirements as it applies to Rx30's gateway and pharmacy software, processing integrity and physical security of the supporting system infrastructure. "SECTION 3: Schedule A | DEA Part 1311.205 Testing Matrices" of this report describes the procedures performed to verify Rx30's application features and information and physical security of their hosted gateway and pharmacy software services.

Pharmacies are required to adhere to requirements described in DEA Part 1311.200; this information can be access via http://www.deadiversion.usdoj.gov/21cfr/cfr/1311/subpart_c100.htm#200. Although Rx30 provides pharmacy application requirements to their customers described in DEA 1311.205 and throughout the remainder of this report, pharmacies still have requirements to be evaluated under DEA 1311.200. Additionally, there are certain parts of the application services provided to pharmacies that Rx30 alone is not able to provide by itself, which users of the system are required to assess the User Control Considerations defined Throughout Section 3 of this report.

SECTION 3: Schedule A | DEA Part 1311.205 Testing Matrices

DEA 1311.205 pharmacy applications control specifications:

Sec. 1311.205 Pharmacy Application Requirements are specified by the DEA and are required to be met, where applicable, to the system under review. The pharmacy application was evaluated for the following control specifications referenced in (a) and (b) 1 through 18:

(a) The pharmacy may only use a pharmacy application that meets the requirements in paragraph (b) of this section to process electronic controlled substance prescriptions.

(b) The pharmacy application must meet the following requirements:

(1) The pharmacy application must be 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 must be set by individual user name or role.

(3) The pharmacy application must digitally sign and archive 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 must meet the following requirements:

(i) The cryptographic module used to digitally sign the data elements required by part 1306 of this chapter must be at least FIPS 140–2 Security Level 1 validated. FIPS 140–2 is incorporated by reference in §1311.08.

(ii) The digital signature application and hash function must comply with FIPS 186–3 and FIPS 180–3, as incorporated by reference in §1311.08.

(iii) The pharmacy application's private key must be stored encrypted on a FIPS 140–2 Security Level 1 or higher validated cryptographic module using a FIPS-approved encryption algorithm. FIPS 140–2 is incorporated by reference in §1311.08.

(iv) For software implementations, when the signing module is deactivated, the pharmacy application must clear the plain text password from the application memory to prevent the unauthorized access to, or use of, the private key.

(v) The pharmacy application must have a time application that is within five minutes of the official National Institute of Standards and Technology time source.

(5) The pharmacy application must verify 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 must either:

(i) Verify that the practitioner signed the prescription by checking the data field that indicates the prescription was signed; or

(ii) Display the field for the pharmacist's verification.

(7) The pharmacy application must read and retain 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 must read and store, and be capable of displaying, all information required by part 1306 of this chapter.

SECTION 3: Schedule A | DEA Part 1311.205 Testing Matrices

(9) The pharmacy application must read and store in full the information required under §1306.05(a) of this chapter. The pharmacy application must either verify that such information is present or must display the information for the pharmacist's verification.

(10) The pharmacy application must provide 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 must be capable of retrieving controlled substance prescriptions by practitioner name, patient name, drug name, and date dispensed.

(12) The pharmacy application must allow downloading of prescription data into a database or spreadsheet that is readable and sortable.

(13) The pharmacy application must maintain 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 must record 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 must conduct internal audits and generate 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 must protect the stored audit records from unauthorized deletion. The pharmacy application shall prevent modifications to the audit records.

(17) The pharmacy application must back up the controlled substance prescription records daily.

(18) The pharmacy application must retain 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**

SECTION 3: Schedule A | DEA Part 1311.205 Testing Matrices

Information Security controls implemented by Rx30

Review of the production hosted prescription gateway environment includes the following controls implemented and designed to support information security of the hosted pharmacy application services. These controls are implemented and performed by Rx30. The following controls were identified:

Information Security Policies and Procedures

- Formal information security policies and procedures are in place to establish organizational information security standards.
- IT access requests are authorized prior to granting access to production systems.

Active Directory / Network Access

- Active Directory authentication is restricted via unique user account and passwords that require:
    - Minimum length of eight characters
    - Maximum age of 183 days
    - Password history requirement of 11
    - Complexity requirement
    - Lockout threshold of five consecutive failed attempts
- Administrative access to the network domain is restricted to personnel with administration job responsibilities.
- Network accounts assigned to terminated personnel are deactivated upon notification of termination.
- The network domain audit settings are configured to log specific events.

Linux Access

- Administrative access to the server operating system is restricted to personnel with administration job responsibilities.
- User access to server operating systems is revoked upon notification of termination.

Operating System Logging

- The operating system audit settings are configured to log specific events.

Application Authentication

- Application authentication is restricted via unique user account and passwords that required:
    - Minimum password length nine
    - Maximum password age of 30 days
    - Minimum password age of seven days
    - History requirement of three previously used passwords
    - Complexity requirements

Application Access Controls

- Access to administer the application is limited to personnel based on their job responsibilities.

Application Logging Controls

- The application is configured to log certain user account application activities and is available for ad hoc review purposes.

Firewall Administration

- NAT is utilized to manage internal IP addresses and routable IP addresses are not permitted on the internal network.
- Administrative access to the firewall system is restricted via unique user account and password and limited to network administrator with firewall administration responsibilities.

Remote Access

- Remote access is performed over encrypted protocols to help ensure the privacy and integrity of the data passing over the public network.

User Control Considerations:

- Users of the pharmacy applications are responsible to issue new or changes to existing application accounts.

- Users of the pharmacy application are required to maintain the security of their account and password.
- Users of the pharmacy application are required to review Rx30’s security and determine if it is sufficient for their environment.
- Users of the pharmacy application are required to restrict logical access to their own internal networks.

SECTION 3: Schedule A | DEA Part 1311.205 Testing Matrices

Physical Security controls implemented by Rx30

Review of the production hosted prescription gateway environment includes the following controls implemented and designed to support physical security of the hosted pharmacy application services. These controls are implemented and performed by Rx30. The following controls were identified:

Physical Security

- A proximity card access control system restricts access to the perimeter, and within the facility, to those with the proximity card.
- Security cameras are in place to record activities within the facility. The security recordings are stored electronically for a minimum of 90 days.
- A security alarm system is installed and monitored by a third party alarm monitoring provider to detect unauthorized events.
- The proximity card access system logs access attempts to and within the facility premises. These logs are available for a minimum of 90 days for ad hoc review purposes.
- Proximity card access zone definitions are established and assigned to personnel based on their job responsibilities.
- Initial request for a proximity card and modification to existing proximity card access requires authorization.
- Access to administer the proximity card access system is limited to personnel based on their job responsibilities.
- Terminated employees’ proximity card access rights are revoked as a component of the termination process.
- A proximity card reader restricts access to the server room.
- Server room access is limited to appropriate personnel based on their job responsibilities.
- Surveillance cameras record activity to and within the server room. Recordings are available for 90 days.

User Control Considerations:

- Users are required to physically secure terminals, network devices and servers from unauthorized access.

SECTION 3: Schedule A | DEA Part 1311.205 Testing Matrices

Electronic Pharmacy Application

Control Objective 1: Control activities provide reasonable assurance that the electronic prescription application Software Version Rx30 eScript 1.0 (application) that processes the dispensing of received electronic prescriptions for controlled substances (EPCS) used by dispensing agents retains prescription and dispensing information required by DEA Part 1311.205.

#	Control Activity Specified by DEA Part 1311.205	Procedures Performed by the Independent Accountant	Results
1.1	(1) The pharmacy application must be 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.	Inspected the pharmacy application to verify that the application was capable of user security to enforce the following permissions: ➢ Annotation ➢ Alteration ➢ Deletion of prescription information ➢ User security administration	No relevant exceptions noted.
1.2	(2) Logical access controls must be set by individual user name or role.	Inspected the pharmacy application to verify that during user account creation, the application only permitted the assignment of a role during user creation. The application requires roles to be assigned to user accounts, and individual screen permission can be modified for user accounts.	No relevant exceptions noted.
1.3	(3) The pharmacy application must digitally sign and archive a prescription on receipt or be capable of receiving and archiving a digitally signed record.	Observed the application received a valid, digitally signed signature, and verified that the application rejected the script. Rx30 Pharmacy Application only accepts scripts with a Signature Indicator flag and their last intermediary signs and archives all scripts received.	No relevant exceptions noted.

SECTION 3: Schedule A | DEA Part 1311.205 Testing Matrices

#	Control Activity Specified by DEA Part 1311.205	Procedures Performed by the Independent Accountant	Results
1.4	(4) For pharmacy applications that digitally sign prescription records upon receipt, the digital signature functionality must meet the following requirements: (i) The cryptographic module used to digitally sign the data elements required by part 1306 of this chapter must be at least FIPS 140–2 Security Level 1 validated. FIPS 140–2 is incorporated by reference in §1311.08. (ii) The digital signature application and hash function must comply with FIPS 186–3 and FIPS 180–3, as incorporated by reference in §1311.08. (iii) The pharmacy application's private key must be stored encrypted on a FIPS 140–2 Security Level 1 or higher validated cryptographic module using a FIPS-approved encryption algorithm. FIPS 140–2 is incorporated by reference in §1311.08. (iv) For software implementations, when the signing module is deactivated, the pharmacy application must clear the plain text password from the application memory to prevent the unauthorized access to, or use of, the private key. (v) The pharmacy application must have a time application that is within five minutes of the official National Institute of Standards and Technology time source.	N/A, Rx30 does not digitally sign prescription records.	
1.5	(5) The pharmacy application must verify 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).	N/A, Rx30 does not accept digitally signed records with the practitioner’s private key.	

SECTION 3: Schedule A | DEA Part 1311.205 Testing Matrices

#	Control Activity Specified by DEA Part 1311.205	Procedures Performed by the Independent Accountant	Results
1.6	(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 must either: (i) Verify that the practitioner signed the prescription by checking the data field that indicates the prescription was signed; or (ii) Display the field for the pharmacist's verification.	Inspected prescriptions sent through the application with no digital signature to verify that the application checked for the signature indicator flag to verify the prescription was signed. Inspected prescriptions sent through the application with no digital signature and no signature indicator field to verify that prescriptions received with no digital signature or a signature indicator flag were rejected.	No relevant exceptions noted.
1.7	(7) The pharmacy application must read and retain 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.	Inspected prescriptions sent through the application to verify that the full DEA number and other internal codes were captured with the prescription.	No relevant exceptions noted.
1.8	(8) The pharmacy application must read and store, and be capable of displaying, all information required by part 1306 of this chapter.	Inspected the pharmacy application to verify that for each prescription the following was capable of being displayed and stored: ➢ full name and address of the patient ➢ the drug name, strength dosage form ➢ quantity prescribed ➢ directions for use ➢ name, address and registration number of the practitioner ➢ Transfers record the name of pharmacist and date of transfer	No relevant exceptions noted.
1.9	(9) The pharmacy application must read and store in full the information required under §1306.05(a) of this chapter. The pharmacy application must either verify that such information is present or must display the information for the pharmacist's verification.	Inspected the pharmacy application to verify that prescription information received, stored and displayed was available for the pharmacist's verification as follows: ➢ full name and address of the patient ➢ the drug name, strength dosage form ➢ quantity prescribed ➢ directions for use ➢ name, address and registration number of the practitioner	No relevant exceptions noted.
1.10	(10) The pharmacy application must provide 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.	Inspected the pharmacy application and a sample of dispensed prescriptions via the dispense log to verify that the following was linked in read only logs to the dispensed prescription records: - Description (included the type of drug and the number of units or volume dispensed) - Date/Time that drug was dispensed by the pharmacy user - User (unique identifier for person that dispensed the prescription)	No relevant exceptions noted.

SECTION 3: Schedule A | DEA Part 1311.205 Testing Matrices

#	Control Activity Specified by DEA Part 1311.205	Procedures Performed by the Independent Accountant	Results
1.11	(11) The pharmacy application must be capable of retrieving controlled substance prescriptions by practitioner name, patient name, drug name, and date dispensed.	Inspected the pharmacy application search and reporting features to verify that a query and retrieval was capable for each of the following attributes: ➢ practitioner name ➢ patient name ➢ drug name ➢ date dispensed	No relevant exceptions noted.
1.12	(12) The pharmacy application must allow downloading of prescription data into a database or spreadsheet that is readable and sortable.	Observed the application's report export functionality to verify that reports were exportable to a .csv file.	No relevant exceptions noted.
1.13	(13) The pharmacy application must maintain 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.	Inspected the audit trail logs for a sample of prescriptions in the application to verify that the following were available, where applicable: ➢ the receipt, annotation, alteration, or deletion of a controlled substance prescription. ➢ any setting or changing of logical access control permissions related to the dispensing of controlled substance prescriptions. ➢ Auditable events as specified in 1311.215.	No relevant exceptions noted.
1.14	(14) The pharmacy application must record 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).	Inspected the audit logs for a sample of transactions in the application to verify that the following were recorded, where applicable: ➢ the date and time of the event. ➢ the type of event. ➢ the identity of the person taking the action, where applicable. ➢ the outcome of the event (success or failure).	No relevant exceptions noted.
1.15	(15) The pharmacy application must conduct internal audits and generate 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.	Inspected the audit reports to verify that daily reports were available and auditable events listed in 1311.215 applicable to the pharmacy application were presented in a readable structure.	No relevant exceptions noted.
1.16	(16) The pharmacy application must protect the stored audit records from unauthorized deletion. The pharmacy application shall prevent modifications to the audit records.	Inspected the pharmacy application and audit records to verify that audit records were read only through the application user interface.	No relevant exceptions noted.

SECTION 3: Schedule A | DEA Part 1311.205 Testing Matrices

#	Control Activity Specified by DEA Part 1311.205	Procedures Performed by the Independent Accountant	Results
1.17	(17) The pharmacy application must back up the controlled substance prescription records daily.	Inspected the backup configuration and logs of completed backups to verify that the controlled substance prescription records were backed up daily.	No relevant exceptions noted.
1.18	(18) The pharmacy application must retain 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.	Inspected the pharmacy application prescription records requirement settings and verified that the records were configured to be stored for a minimum of 24 months. Record retention cannot be set less than 24 months by an application user.	No relevant exceptions noted.

Information Security

Control Objective 2: Control activities provide reasonable assurance that logical access to critical systems and data is restricted to authorized individuals.

#	Control Activity	Testing Procedures and Results	Results
2.1	Formal information security policies and procedures are in place to establish organizational information security standards.	Inquired of the Systems Administrator to verify that information security policies and procedures were in place to establish organizational information security standards.	No relevant exceptions noted.
		Inspected the information security policies and procedures to verify that organizational information security standards were documented.	No relevant exceptions noted.
2.2	IT access requests are authorized prior to granting access to production systems.	Inquired of the Systems Administrator to verify that an approved IT access request was authorized prior to granting access to production systems.	No relevant exceptions noted.
2.3	Active Directory / Network Access Active Directory authentication is restricted via unique user account and passwords that required: ➢ Minimum length of eight characters ➢ Maximum age of 183 days ➢ Password history requirement of 11 ➢ Complexity requirement ➢ Lockout threshold of five consecutive failed attempts	Inquired of the Systems Administrator to verify that Active Directory was implemented on user machines and user account passwords required the following characteristics: ➢ Minimum length of eight characters ➢ Maximum age of 183 days ➢ Password history requirement of 11 ➢ Complexity requirement ➢ Lockout threshold of five consecutive failed attempts	No relevant exceptions noted.
		Inspected password settings to verify that Active Directory user account passwords required the following characteristics: ➢ Minimum length of eight characters ➢ Maximum age of 183 days ➢ Password history requirement of 11 ➢ Complexity requirement ➢ Lockout threshold of five consecutive failed attempts	No relevant exceptions noted.

2.4	Administrative access to the network domain is restricted to personnel with administration job responsibilities.	Inquired of the Systems Administrator to verify that network domain administrative access was restricted to personnel with administration job responsibilities. Inspected administrative access to the network domain to verify that access was restricted to personnel with administration job responsibilities.	No relevant exceptions noted. No relevant exceptions noted.
2.5	Network accounts assigned to terminated personnel are deactivated upon notification of termination.	Inquired of the Systems Administrator to verify that network accounts were only assigned to active and current personnel with administration job responsibilities. Inspected network user access for personnel terminated during the audit period to verify that network accounts were only assigned to active and current personnel.	No relevant exceptions noted. No relevant exceptions noted.
2.6	The network domain audit settings are configured to log specific events.	Inquired of the Systems Administrator to verify that network domain audit settings were configured to log specific events. Inspected network domain audit log configurations to verify that network domain audit settings were configured to log specific events.	No relevant exceptions noted. No relevant exceptions noted.
	Linux Access		
2.7	Administrative access to the server operating system is restricted to personnel with administration job responsibilities.	Inquired of the Systems Administrator to verify that administrative access to the server operating system was restricted to personnel with administrative job responsibilities. Inspected users with administrative access to the server operating system to verify that administrative access was restricted to IT personnel with administrative job responsibilities.	No relevant exceptions noted. No relevant exceptions noted.
2.8	User access to server operating systems is revoked upon notification of termination.	Inquired of the Systems Administrator to verify that operating system accounts assigned to terminated personnel were deactivated upon notification of termination. Inspected user with access to the operating system to verify that access was only assigned to current authorized personnel.	No relevant exceptions noted. No relevant exceptions noted.
	Operating System Logging		
2.9	The operating system audit settings are configured to log specific events.	Inquired of the Systems Administrator to verify that the operating system audit settings were configured to log specific events. Inspected the operating system audit settings to verify that certain operating system events were logged.	No relevant exceptions noted. No relevant exceptions noted.

2.10	Application Authentication Application authentication is restricted via unique user account and passwords that required: ➢ Minimum password length nine ➢ Maximum password age of 30 days ➢ Minimum password age of seven days ➢ History requirement of three previously used passwords ➢ Complexity requirements	Inquired of the Systems Administrator to verify that application authentication user account passwords required the following characteristics: ➢ Minimum password length nine ➢ Maximum password age of 30 days ➢ Minimum password age of seven days ➢ History requirement of three previously used passwords ➢ Complexity requirements	No relevant exceptions noted.
		Inspected the application password authentications to verify that application authentication user account passwords required the following characteristics: ➢ Minimum password length nine ➢ Maximum password age of 30 days ➢ Minimum password age of seven days ➢ History requirement of three previously used passwords ➢ Complexity requirements	No relevant exceptions noted.
2.11	Application Access Controls Access to administer the application is limited to personnel based on their job responsibilities.	Inquired of the Systems Administrator to verify that access to administer the application was limited to certain personnel with application administration responsibilities.	No relevant exceptions noted.
		Inspected the application access user listing to verify that access to administer the application was limited to certain IT personnel based on their job responsibilities.	No relevant exceptions noted.
2.12	Application Logging Controls The application is configured to log certain user account application activities and is available for ad hoc review purposes.	Inquired of the Systems Administrator to verify that the application was configured to log certain user account application activities and was available for ad hoc review purposes.	No relevant exceptions noted.
		Inspected a sample of application logs to verify that application activities were logged and available for ad hoc review.	No relevant exceptions noted.
2.13	Firewall Administration NAT is utilized to manage internal IP addresses and routable IP addresses are not permitted on the internal network.	Inquired of the Systems Administrator to verify that NAT was utilized to manage internal IP address and that routable IP addresses were not permitted on the internal network.	No relevant exceptions noted.
		Inspected the NAT setting and internal IP address ranges to verify that NAT was utilized to mask internal IP addresses and routable IP address ranges were not permitted on the internal network.	No relevant exceptions noted.

2.14	Administrative access to the firewall system is restricted via unique user account and password and limited to network administrator with firewall administration responsibilities.	Inquired of the Systems Administrator to verify that administrative access to the firewall system was restricted via unique user account and password, and account was limited to personnel with firewall administration responsibilities.	No relevant exceptions noted.
		Inspected the third party managed services providers letter to verify that access was limited to personnel with firewall administration responsibilities.	No relevant exceptions noted.
	Remote Access		
2.15	Remote access is performed over encrypted protocols to help ensure the privacy and integrity of the data passing over the public network.	Inquired of the Systems Administrator to verify that encrypted protocols were utilized for remote access to help ensure the privacy and integrity of the data passing over the public network.	No relevant exceptions noted.
		Inspected the encryption settings to verify that remote access was encrypted.	No relevant exceptions noted.
2.16	Access to customer installed environments is limited to authorized Rx30 personnel.	Inquired of the system administrator to verify that only authorized Rx30 personnel had remote access to installed pharmacy application.	No relevant exceptions noted.
		Inspected listing of personnel with access to customer environments to verify access was limited to authorized personnel.	No relevant exceptions noted.

SECTION 3: Schedule A | DEA Part 1311.205 Testing Matrices

Physical Security

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

#	Control Activity	Procedures Performed by the Independent Accountant	Results
3.1	A proximity card access control system restricts access to the perimeter and within the facility to those with the proximity card.	Inquired of the system administrator to verify that a proximity card reader restricted the perimeter, and certain rooms within the facility.	No relevant exceptions noted.
		Observe the access to and within the facility to verify that a proximity card access control system restricted the perimeter, and certain rooms within the facility.	No relevant exceptions noted.
3.2	Security cameras are in place to record activities to and within the facility. The security recordings are stored electronically for a minimum of 90 days.	Inquired of the Systems Administrator to verify that activities to and within the facility were recorded and available for review during the past 90 days.	No relevant exceptions noted.
		Inspected video surveillance recordings to verify that activities to and within the facility were recorded and available for review during the past 90 days.	No relevant exceptions noted.
3.3	A security alarm system is installed and monitored by a third party alarm monitoring provider to detect unauthorized events.	Inquired of the Systems Administrator to verify that a third party monitored the facilities alarm system.	No relevant exceptions noted.
		Inspected the monitoring agreement to verify that the security alarm system was monitored by a third party provider.	No relevant exceptions noted.
3.4	The proximity card access system logs access attempts to and within the facility premises. These logs are available for a minimum of 90 days for ad hoc review purposes.	Inquired of the Director of Operations to verify that logs were available for a minimum of 90 days for ad hoc review purposes, and that unsuccessful attempts were reviewed monthly.	No relevant exceptions noted.
		Inspected the access logs to verify that the security logs were available for the past 90 days.	No relevant exceptions noted.
3.5	Proximity card access zone definitions are established and assigned to personnel based on their job responsibilities.	Inquired of the Systems Administrator to verify that proximity card access zone definitions were established and assigned to personnel based on their job responsibilities.	No relevant exceptions noted.
		Inspected the proximity card access zone assignments to verify that personnel were assigned access based on their job responsibilities.	No relevant exceptions noted.
3.6	Initial request for a proximity card and modification to existing proximity card access requires authorization.	Inquired of the Systems Administrator to verify that proximity card access initial request and modification to existing proximity cards required authorization.	No relevant exceptions noted.

SECTION 3: Schedule A | DEA Part 1311.205 Testing Matrices

#	Control Activity	Procedures Performed by the Independent Accountant	Results
3.7	Access to administer the proximity card access system is limited to personnel based on their job responsibilities.	Inquired of the Systems Administrator to verify that access to administer the proximity card access system was limited to personnel based on their job responsibilities.	No relevant exceptions noted.
		Inspected user access report to verify that access to administer the badge access system was limited to personnel based on their job responsibilities.	No relevant exceptions noted.
3.8	Terminated employees' proximity card access rights are revoked as a component of the termination process.	Inquired of the Systems Administrator to verify that terminated employees' proximity card access rights were revoked as a component of the termination process.	No relevant exceptions noted.
		Inspected badge access user report for and current employee listing to verify that terminated personnel proximity card access rights were revoked.	No relevant exceptions noted.
3.9	A proximity card reader restricts access to the server room door.	Observed server room proximity card reader and personnel access the server room to verify that a proximity card reader restricted access to the server room door.	No relevant exceptions noted.
3.10	Server room access is limited to appropriate personnel based on their job responsibilities.	Inquired of the Systems Administrator to verify that server room access was limited to appropriate personnel based on their job responsibilities.	No relevant exceptions noted.
		Inspected the personnel listing that had access to the server room to verify that server room access was limited to appropriate personnel based on their job responsibilities.	No relevant exceptions noted.
3.11	Surveillance cameras record activity to and within the server room. Recordings are available for 90 days.	Inquired of the Systems Administrator to verify that activities to and within the facility were recorded and available for review during the past 90 days.	No relevant exceptions noted.