2013

DEA 1311.205 Compliance Report for Pharmacy Application Providers as of July 15, 2013

PioneerRx™
Pharmacy Software

assurance
CONCEPTS, LLC
think assurance. know compliance.

Table of Contents

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

To Management of New Tech Computer Systems, Inc:

We have performed the procedures described below, which were agreed to by New Tech Computer Systems, Inc. (“PioneerRx”) solely to assist in the identification of Compliance Assessment for DEA Part 1311.205 controls that were in place as of July 15, 2013, as set forth in the accompanying Schedule A. The maintenance of these controls is solely the responsibility of PioneerRx. Consequently, we make no representation regarding the sufficiency of the controls as a whole for PioneerRx 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 PioneerRx’s controls implemented in the pharmacy application PioneerRx V2.1.x 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 July 15, 2013.
   No exceptions were found as a result of this comparison.
2. Reviewed PioneerRx’s controls implemented in the information security environment for the production system of PioneerRx’s electronic prescription application services. Reviewed information security controls and processes to verify that controls were in place and operating as of July 15, 2013.
   No exceptions were found as a result of this comparison.
3. Reviewed PioneerRx’s controls implemented in the physical security environment for the production system of PioneerRx’s hosted electronic prescription application services. Reviewed physical security controls and processes to verify that controls were in place and operating as of July 15, 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 PioneerRx is as of July 15, 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 PioneerRx 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 PioneerRx 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 PioneerRx and is not intended to be and should not be used by anyone other than these specified parties.

Assurance Concepts, LLC

July 15, 2013

SECTION 2: PioneerRx Pharmacy Application System Description

Company Overview and Services Provided

With the experience of over 35 years of pharmacy software development and support, PioneerRx was built from scratch to provide the pharmacy community with a solution that can grow as the industry changes for the next 35 years. These features are designed to provide speed, simplicity, consistency and flexibility. However, the ultimate goal of development is to help pharmacies make more money.

PioneerRx provides customers with innovative, efficient, cost-effective solutions that meet their needs, conserve and enhance their resources, and maximize their profits. PioneerRx's commitment is to the traditional values of effective work, integrity, and customer satisfaction. This commitment, along with years of experience, a motivated management team, and staff of intelligent, creative problem solvers enables us to meet our business objectives and help our clients achieve their goals.

PioneerRx is headquartered in Shreveport, LA and was founded in 1983.

Information Systems Overview

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

PioneerRx is a custom developed application that healthcare providers utilize to dispense electronic prescriptions for controlled substance resides at the Pharmacies and prescriptions are routed from SureScripts to PioneerRx's gateway which digitally signs scripts upon receipt and then transmits to the designated pharmacy. PioneerRx's hosted gateway is used for the delivery of their electronic prescriptions to the individual pharmacies from SureScripts. Access is only granted to this gateway via a formal authorization process and access is limited to the application and data that resides its systems to authorized personnel. PioneerRx remotely manages and supports their Pharmacy Applications that are installed locally at each pharmacy customer location.

Scope and Summary of Report

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

SECTION 2: PioneerRx Pharmacy Application System Description

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 PioneerRx provides pharmacy application requirements to their customers described in DEA 1311.205 and throughout the remainder of this report pharmacies still have requirements to evaluated under DEA 1311.200. Additionally there are certain parts of the application services provided to pharmacies that PioneerRx alone is not able to provide by itself and users of the system are required to assess the User Control Considerations defined Throughout Section 2 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 reference 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 PioneerRx

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 PioneerRx. The following controls were identified:

- IT access requests are authorized prior to granting access to production systems.
- 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.
- The operating system audit settings are configured to log specific events.
- Access to the database is restricted via authorized accounts.
- Database access privileges are revoked as a component of the termination process.
- Application authentication is restricted via unique user account and passwords that required:
    - Minimum length of eight characters
    - Complexity requirements
    - Users are logged out upon a predetermine time interval
- The application required a security PIN to be entered to execute certain transactions within the pharmacy application.
- Access to administer the application is limited to personnel based on their job responsibilities.
- The application is configured to log certain user account application activities and is available for ad hoc review purposes.
- Network address translation (NAT) is utilized to manage internal IP addresses and routable IP addresses are not permitted on the internal network of the pharmacy services gateway.
- Administrative access to the firewall system is managed by network administrators.
- Firewall rulesets and configurations changes are authorized and requested changes are submitted to PioneerRx network administrators.

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, password and PIN.
- Users of the pharmacy application are required to review PioneerRx'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 PioneerRx

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 PioneerRx. The following controls were identified:

- The facility entrances are manned during business hours and locked during after hours.
- A security alarm system is installed and monitored by a third party alarm monitoring provider to detect unauthorized events
- Terminated employees' rights are revoked as a component of the termination process.
- A digital combination lock restricts access to the server room door. The lock is touch screen, supports 8 digit PINs which are unique per employee, audits PIN entry events via a network connection and website, and sends email notifications stating who\what\when the door opens. Server room access is limited to appropriate personnel based on their job responsibilities.
- Server room has motion activated video surveillance

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 7.9.10 (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 only allows rolls to be assigned to 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 receive a valid, digitally signed signature and verified that the application performed a validity check to ensure the authenticity of the signature was verified and archived. Observed the application receive an invalid digitally signed signature and verified that the application performed a validity check and marked the prescription as error invalid signature received and archived results. Observed the application receive a prescription without a digital signature to verify that the prescription was digitally signed by the gateway application, attached to the record and archived prior to transmitting to pharmacies.	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.	Inspected the deployed software module for digital signatures to verify that the deployed cryptographic module with a FIPS 140-2 Validation Certificate and FIPS 186-3 and FIPS 180-3 compliant hash functions were valid and approved and during the creation of the digital signature the prescription information (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) was included when signing. Inspected the time clock implemented in the application to ensure that a synchronization clock, approved from the National Institute of Standards and Technology, time source was utilized.	No relevant exceptions noted.
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).	Inspected a sample of prescriptions received with a valid digital signature in the pharmacy system and the results from the digital signature validation process to verify that the digital signature was validated upon receipt and status displayed. Inspected a sample of prescriptions received with an invalid digital signature in the pharmacy system and the results from the digital signature validation process to verify that the digital signature was validated as invalid upon receipt and status displayed.	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
1.6	(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 receive, store and display prescriptions to verify that the following was available for the pharmacist's verification: ➢ 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 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. (iii) 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, auditable events listed in 1311.215 applicable to the pharmacy application and 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 and verified that the records were available for a minimum of two years prior to the day of that the records were verified as available.	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	Procedures Performed by the Independent Accountant	Results
2.1	User Provisioning IT access requests are authorized prior to granting access to production systems.	Inquired of the system administrator to verify that access requests were authorized prior to granting access to production systems.	No relevant exceptions noted.
		Inspected IT production system accounts with the system administrator to verify that production system access was authorized.	No relevant exceptions noted.
2.2	Pharmacy Gateway Operating System Access Administrative access to the server operating system is restricted to personnel with administration job responsibilities.	Inquired of the system administrator to verify that administrative access to the server operating system was restricted to personnel with administrative job responsibilities.	No relevant exceptions noted.
		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.
2.3	User access to server operating systems is revoked upon notification of termination.	Inquired of the system administrator to verify that operating system accounts assigned to terminated personnel were deactivated upon notification of termination.	No relevant exceptions noted.
		Inspected users with access to the operating system to verify that access of terminated personnel was revoked.	No relevant exceptions noted.
2.4	Operating System Logging The operating system audit settings are configured to log specific events.	Inquired of the system administrator to verify that the operating system audit settings were configured to log specific events.	No relevant exceptions noted.

SECTION 3: Schedule A | DEA Part 1311.205 Testing Matrices

#	Control Activity	Procedures Performed by the Independent Accountant	Results
		Inspected the operating system audit settings to verify that certain operating system events were logged.	No relevant exceptions noted.
2.5	Database Access Access to the database is restricted via authorized accounts.	Inquired of the system administrator to verify that access to the database was restricted via authorized accounts.	No relevant exceptions noted.
		Inspected access to the database to verify access was restricted via authorized accounts.	No relevant exceptions noted.
2.6	Database access privileges are revoked as a component of the termination process.	Inquired of the system administrator to verify that database access privileges were revoked upon notification of termination.	No relevant exceptions noted.
		Inspected the accounts with the system administrator to verify that database access was current and authorized.	No relevant exceptions noted.
2.7	Application Authentication Application authentication is restricted via unique user account and passwords that required: ➢ Minimum length of eight characters ➢ Complexity requirements ➢ Users are logged out upon a predetermine time interval	Inquired of the system administrator to verify that application authentication user account passwords required the following characteristics: ➢ Minimum length ➢ Complexity requirements ➢ Cannot use previous password ➢ Users are logged out upon a predetermine time interval	No relevant exceptions noted.
		Inspected the application password authentication to verify that application authentication user account passwords required the following characteristics: ➢ Minimum length ➢ Complexity requirements ➢ Cannot use previous password ➢ Users are logged out upon a predetermine time interval	No relevant exceptions noted.
2.8	Application Access Controls Access to administer the application is limited to personnel based on their job responsibilities.	Inquired of the system 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.

SECTION 3: Schedule A | DEA Part 1311.205 Testing Matrices

#	Control Activity	Procedures Performed by the Independent Accountant	Results
2.9	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 system 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.
2.10	Firewall Administration NAT is utilized to manage internal IP addresses and routable IP addresses are not permitted on the internal network.	Inquired of the system administrator to verify that NAT was utilized to mange internal IP addresses and that routable IP addresses were not permitted on the internal network.	No relevant exceptions noted.
		Inspected the 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.
2.11	Administrative access to the firewall system is managed by network administrators.	Inquired of the system administrator to verify that administrative access to the firewall system was managed by network administrators.	No relevant exceptions noted.
		Observed firewall users to verify access to administrate the firewall was restricted to network administrators.	
2.12	Firewall rulesets and configuration changes are authorized and requested changes are submitted to PioneerRx network administrators.	Inquired of the system administrator to verify that fire rulesets and configuration changes were authorized and requested changes were submitted to PioneerRx network administrators for implementation.	No relevant exceptions noted.
2.13	Remote Access Access to customer installed environments is limited to authorized PioneerRx personnel.	Inquired of the system administrator to verify that only authorized PioneerRx 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	The facility entrances are manned during business hours and locked during after hours.	Observed access while on the premises to verify physical access to the facility required was locked after hours.	No relevant exceptions noted.
3.2	A security alarm system is installed and monitored by a third party alarm monitoring provider to detect unauthorized events.	Inquired of the system administrator to verify that the security alarm system was monitored by a third party provider.	No relevant exceptions noted.
		Observed the security alarm system to verify that a security alarm system was in place at the facility.	No relevant exceptions noted.
3.3	Terminated employees' rights are revoked as a component of the termination process.	Inquired of the system administrator to verify that terminated personnel physical access was revoked during the termination process.	No relevant exceptions noted.
3.4	A digital combination lock restricts access to the server room door. The lock is touch screen, supports 8 digit PINs which are unique per employee, audits PIN entry events via a network connection and website, and sends email notifications stating who\what\when the door opens. Server room access is limited to appropriate personnel based on their job responsibilities.	Inquired of the system administrator to verify that the digital combination lock restricted access to the server room, required an 8 digit pin, unique account were assign and logging of users was recorded.	No relevant exceptions noted.
		Observed access to the server room to verify that digital combination lock restricted access to the server room.	No relevant exceptions noted.
3.5	Server room has motion activated video surveillance.	Inquired of the system administrator to verify that the server room had motion activated video surveillance.	No relevant exceptions noted.