Independent Report on Compliance DEA 1311.120 for Application Service Providers as of April 29, 2019

ASSURANCE CONCEPTS

A SKODA MINOTTI ADVISORY FIRM

WENO – DEA 1311 Report on Compliance
Table of Contents

SECTION 1: INDEPENDENT AUDITORS REPORT ON COMPLIANCE FOR DEA 1311.120 FOR APPLICATION SERVICE PROVIDERS

Independent Auditors Report

To Management of WENO:

We have performed the procedures described below, which were agreed to by WENO Exchange, LLC (WENO) solely to assist in the identification of Compliance Assessment for DEA Part 1311.120 controls that were in place as of April 29, 2019 as set forth in the accompanying Schedule A. The maintenance of these controls is solely the responsibility of WENO. WENO uses Liquid Web ("subservice organization"), a third party managed IT infrastructure service provider that manages the Server Hosting where WENO deployed their electronic prescription application. The accompanying description includes only those controls and related control objectives of WENO and does not include control objectives and related controls of the subservice organization. Our examination did not extend to controls of the subservice organization. Consequently, we make no representation regarding the sufficiency of the controls as a whole for WENO as described below either for the purpose for which this report has been requested or for any other purpose.

The objectives and associated findings are as follows:

1. Compared WENO's controls implemented in the Electronic Prescription Application (EPA) (WENO Version 3) to the criteria applicable to EPA set forth in the Code of Federal Regulation 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 (EPA criteria). Management of WENO, is responsible for the EPA meeting the EPA criteria. Our responsibility was to perform procedures to determine if the EPA met the EPA criteria and that there was reasonable assurance that the processing integrity of the application was in place by the application provider to consistently and accurately recorded, stored, and transmitted information under this part as of April 29, 2019 based on our review procedures.
   See Section 3 | Table A - No exceptions were found as a result of this comparison.
2. Reviewed WENO's controls implemented in the information security environment for the production system of WENO's hosted electronic prescription application. Reviewed information security controls and processes to assess controls were in place and operating as of April 29, 2019.
   See Section 3 | Table B - No exceptions were found as a result of this comparison.

The description of controls at WENO is as of April 29, 2019, 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 WENO 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 WENO's 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 WENO and is not intended to be and should not be used by anyone other than these specified parties.

/S/ Assurance Concepts
April 29, 2019
Tampa, Florida

SECTION 2: WENO'S OVERVIEW

Company Overview and Services Provided

Weno Exchange LLC (WENO) is an electronic Prescribing (ePrescribing) network which routes standard ePrescribing messages, including controlled substances, between healthcare providers, payers, and pharmacies. This is accomplished when electronic health record (EHR) systems connect to WENO's network or when a healthcare provider uses WENO's web based ePrescribing application.

WENO is the only known competitor of Surescripts. WENO's super niche technology is focused on making ePrescribing easy and affordable for all. WENO is headquartered in Austin, Texas.

WENO has been hailed as an innovative competitor in an otherwise dominated e-prescribing network and benefit service market.

For more information, visit www.wenoexchange.com

Information Systems Overview

WENO information systems were built to facilitate the electronic prescriptions processes for controlled substances used by a DEA registrant. Information systems retain all prescription and dispensing information required by DEA regulations, digitally signatures of the records of the prescription that is sent to pharmacy and maintain an internal audit trail of any required auditable events. WENO's information systems are comprised of internal and external third party managed services.

WENO's custom developed application that healthcare providers utilize to process electronic prescriptions for controlled substance resides in a third party managed IT infrastructure service provider for Enterprise Hosting Services. WENO's third party managed IT infrastructure service provider (Liquid Web) goes under a reoccurring SOC 2 Type II audit every year. The SOC 2 Type II audit reports on the suitability and operating effectiveness of the Third Party Enterprise Hosting Services; where WENO deployed their electronic prescription application for their DEA Part 1311.120 compliance for hosted application service providers. WENO manages access to their electronic prescription application via a formal authorization process and limits the access to the application and data that resides in their systems to WENO personnel and clients. Physical security to the application service provider is maintained and monitored by the third party and therefore is not included in this report.

Scope and Summary of Report

This report describes the control criteria under the guidance of DEA Part 1311.120 for WENO as it relates to application and information security standard for their Electronic Prescription Application Services. It is intended to illustrate the validation procedures performed to verify that WENO's EPA WENO Rx version 4 met the criteria of Part 1311.120. In addition we verified that the application provider consistently and accurately recorded, stored, and transmitted information under this part. The criteria and results of testing are described in Section 3 Tables A & B below.

SECTION 3: TESTING MATRICES

Table A - DEA 1311.120 Electronic Prescription Application **Perform procedures to find reasonable assurance that the application functionality met the requirements of this part.**		
DEA Ref#	**DEA EPA Criteria Requirements**	**Procedures Performed and Results**
1311.105 (a)	(a) An individual practitioner must obtain a two-factor authentication credential from one of the following: (1) A credential service provider that has been approved by the General Services Administration Office of Technology Strategy/Division of Identity Management to conduct identity proofing that meets the requirements of Assurance Level 3 or above as specified in NIST SP 800–63–1 as incorporated by reference in Section 1311.08. (2) For digital certificates, a certification authority that is cross-certified with the Federal Bridge certification authority and that operates at a Federal Bridge Certification Authority basic assurance level or above. (b) The practitioner must submit identity proofing information to the credential service provider or certification authority as specified by the credential service provider or certification authority. (c) The credential service provider or certification authority must issue the authentication credential using two channels (e.g., e-mail, mail, or telephone call). If one of the factors used in the authentication protocol is a biometric, or if the practitioner has a hard token that is being enabled to sign controlled substances prescriptions, the credential service provider or certification authority must issue two pieces of information used to generate or activate the authentication credential using two channels.	Inquired of the CEO to verify that the EPA required users during the registration process to obtain their authentication credential from a credential service provider that was Assurance Level 3 or above. Inspected through observation that when registering on the EPA that they were required to go through identity proofing with inflection to obtain their authentication token. Upon completion of identity proofing instructions are provided on how to obtain the token from two methods of delivery. Once the token is obtained they were required to register the token through Duo. No relevant exceptions noted.
1311.120	**Electronic prescription application requirements.**	
1311.120 (b)	The electronic prescription application meets the requirements of this subpart including the following:	
1311.120 (b) (1)	The electronic prescription application does the following:	

Table A - DEA 1311.120 Electronic Prescription Application **Perform procedures to find reasonable assurance that the application functionality met the requirements of this part.**		
DEA Ref#	**DEA EPA Criteria Requirements**	**Procedures Performed and Results**
1311.120 (b) (1) (i)	Link each registrant, by name, to at least one DEA registration number.	Inquired of the CEO to verify that the application linked each registrant by name to at least one DEA registration number. Inspected through observation that when creating a registrant user the application required the registrant user to be linked to a DEA number or the application would not save the user profile. No relevant exceptions noted.
1311.120 (b) (1) (ii)	Link each practitioner exempt from registration under § 1301.22(c) of this chapter to the institutional practitioner's DEA registration number and the specific internal code number required under § 1301.22(c)(5) of this chapter.	Inquired of the CEO to verify application account users were linked to the primary institutional practitioner's DEA registration number. Inspected a listing of application users for the customer's DEA registration number to verify that application account users were linked to the primary institutional practitioner's DEA registration number. No relevant exceptions noted.
1311.120 (b) (2)	The electronic prescription application is capable of the setting of logical access controls to limit permissions for the following functions:	
1311.120 (b) (2) (i)	Indication that a prescription is ready for signing and signing controlled substance prescriptions.	Inquired of the CEO to verify that the application was configured to limit users' access permissions. Inspected the logical access control setup screen to verify that rolls were available to limit users' access permissions for the following functions: ➢ Administrator role ➢ ePrescribing Role ➢ ePrescribing role without EPCS ➢ ePrescribing role with EPCS No relevant exceptions noted.
1311.120 (b) (2) (ii)	Creating, updating, and executing the logical access controls for the functions specified in paragraph (b)(2)(i) of this section.	Inquired of the CEO to verify that the application was configured to limit users with the ability to administer application security to those users who were signed up and authorized to sign EPCS. Inspected application logical access control setup to verify that roles were available to limit users who can create, update and execute logical access permissions via the role Access Control Manager. No relevant exceptions noted.

Table A - DEA 1311.120 Electronic Prescription Application **Perform procedures to find reasonable assurance that the application functionality met the requirements of this part.**		
DEA Ref#	**DEA EPA Criteria Requirements**	**Procedures Performed and Results**
1311.120 (b) (3)	Logical access controls are set by individual user name or role. If the application sets logical access control by role, it does not allow an individual to be assigned the role of registrant unless that individual is linked to at least one DEA registration number as provided in paragraph (b)(1) of this section.	Inquired of the CEO to verify that the application security was controlled by role based security and users can't be assigned the role of sign and send unless tied to a DEA number. Inspected application security to verify that application security was controlled by role based security and that users were required to have a DEA number to be assigned permission to sign and send. No relevant exceptions noted.
1311.120 (b) (4)	The application requires that the setting and changing of logical access controls specified under paragraph (b)(2) of this section involve the actions of two individuals as specified in § 1311.125 or 1311.130. Except for institutional practitioners, a practitioner authorized to sign controlled substance prescriptions approves logical access control entries.	Inquired of the CEO to verify that assigning or modifying user's logical access required the actions of two individuals. Observed the CEO update security to a sample user and validated that 2 users were required to authenticate via their 2-factor credentials prior to updating logical security and that one of the users was required to have EPCS access. No relevant exceptions noted.
1311.120 (b) (5)	The electronic prescription application accepts two-factor authentication that meets the requirements of § 1311.115 and require its use for signing controlled substance prescriptions and for approving data that set or change logical access controls related to reviewing and signing controlled substance prescriptions.	Inquired of the CEO to verify that the application authentication for signing controlled substance prescriptions was restricted by two factor authentication, which required the practitioner's Duo token which was FIPS 140-2 Security Level 2 requirements. Inspected the application authentication requirements to verify that the application authentication for signing controlled substance prescriptions was restricted by two factor authentication, which required the practitioner's Duo token and password and met the criteria of FIPS 140-2 Security Level 2 requirements. No relevant exceptions noted.

Table A - DEA 1311.120 Electronic Prescription Application **Perform procedures to find reasonable assurance that the application functionality met the requirements of this part.**		
DEA Ref#	**DEA EPA Criteria Requirements**	**Procedures Performed and Results**
1311.120 (b) (6)	The electronic prescription application is capable of recording all of the applicable information required in part 1306 of this chapter for the controlled substance prescription.	Inquired of the CEO to verify that the application recorded the indication that the prescription was signed, the number of refills, special DEA identification number, the date before which a prescription may not be filled, and notes required for certain prescriptions. Inspected application logs to verify that the application recorded the indication that the prescription was signed, the number of refills, special DEA identification number, the date before which a prescription may not be filled, and notes required for certain prescriptions. No relevant exceptions noted.
1311.120 (b) (7)	If a practitioner has more than one DEA registration number, the electronic prescription application requires the practitioner or his agent to select the DEA registration number to be included on the prescription.	Inquired of the CEO to verify that the practitioner was restricted to one DEA registration number, which was included on the prescription, per user account. Inspected the user's details to verify that only one DEA must be selected when signing. Observed the prescription fulfillment process to verify that a practitioner's user account was restricted and required selecting one DEA number, which was included on the prescription. No relevant exceptions noted.
1311.120 (b) (8)	The electronic prescription application has a time application that is within five minutes of the official National Institute of Standards and Technology time source.	Inquired of the CEO to verify that the application internal time clock configuration was set to the NIST time source. Inspected the application internal time clock configuration to verify that the application time was set to synchronize with the time.nist.gov NIST time server. No relevant exceptions noted.
1311.120 (b) (9)	The electronic prescription application presents for the practitioner's review and approval all of the following data for each controlled substance prescription:	Inspected the practitioner's preapproval review screen in the application to verify that the application was configured to present for the practitioner's review and approval the following data for each controlled substance prescribed prior to signing: i. The date of issuance. ii. The full name of the patient. iii. The drug name.
1311.120 (b) (9) (i)	The date of issuance.	
1311.120 (b) (9) (ii)	The full name of the patient.	

Table A - DEA 1311.120 Electronic Prescription Application **Perform procedures to find reasonable assurance that the application functionality met the requirements of this part.**		
DEA Ref#	**DEA EPA Criteria Requirements**	**Procedures Performed and Results**
1311.120 (b) (9) (iii)	The drug name.	iv. The dosage strength and form, quantity prescribed, and directions for use. v. The number of refills authorized, if applicable, for prescriptions for Schedule III, IV, and V controlled substances. vi. The earliest date on which a pharmacy may fill the prescriptions of a Schedule II controlled substance. vii. The name, address, and DEA registration number of the prescribing practitioner. viii. Display the statement "By completing the two-factor authentication protocol at this time, you are legally signing the prescription(s) and authorizing the transmission of the above information to the pharmacy for dispensing. The two-factor authentication protocol may only be completed by the practitioner whose name and DEA registration number appear below." No relevant exceptions noted.
1311.120 (b) (9) (iv)	The dosage strength and form, quantity prescribed, and directions for use.	
1311.120 (b) (9) (v)	The number of refills authorized, if applicable, for prescriptions for Schedule III, IV, and V controlled substances.	
1311.120 (b) (9) (vi)	For prescriptions written in accordance with the requirements of § 1306.12(b) of this chapter, the earliest date on which a pharmacy may fill each prescription.	
1311.120 (b) (9) (vii)	The name, address, and DEA registration number of the prescribing practitioner.	
1311.120 (b) (9) (vii)	The statement required under § 1311.140(a)(3).	
1311.120 (b) (10)	The electronic prescription application requires the prescribing practitioner to indicate that each controlled substance prescription is ready for signing. The electronic prescription application does not permit alteration of the DEA elements after the practitioner has indicated that a controlled substance prescription is ready to be signed without requiring another review and indication of readiness for signing. Any controlled substance prescription not indicated as ready to be signed shall not be signed or transmitted.	Inspected the pending queue and preview page for a practitioner to verify that the application required the prescribing practitioner to indicate that each controlled substance prescription was ready for signing. Observed the prescription approval process to verify that the application did not permit alteration of the DEA elements after the practitioner had indicated that the prescription was ready to be signed without requiring another review and indication of readiness for signing. No relevant exceptions noted.

Table A - DEA 1311.120 Electronic Prescription Application **Perform procedures to find reasonable assurance that the application functionality met the requirements of this part.**		
DEA Ref#	**DEA EPA Criteria Requirements**	**Procedures Performed and Results**
1311.120 (b) (11)	While the information required by paragraph (b)(9) of this section and the statement required by § 1311.140(a)(3) remain displayed, the electronic prescription application prompts the prescribing practitioner to authenticate to the application, using two-factor authentication, as specified in § 1311.140(a)(4), which will constitute the signing of the prescription by the practitioner for purposes of § 1306.05(a) and (e) of this chapter.	Inspected the signing process for a sample of prescriptions to verify that the following statement was presented during signing “By completing the two-factor authentication protocol at this time, you are legally signing the prescription(s) and authorizing the transmission of the above information to the pharmacy for dispensing. The two-factor authentication protocol may only be completed by the practitioner whose name and DEA registration number appear below.” Inspected through observation of the signing process that two-factor authentication was required when signing. Observed the software developer attempt to sign without second credential and verified that authentication failed. Observed that the 2 factors were entered appropriately and prescription was indicated as signed. No relevant exceptions noted.
1311.120 (b) (12)	The electronic prescription application does not permit a practitioner other than the prescribing practitioner whose DEA number (or institutional practitioner DEA number and extension data for the individual practitioner) is listed on the prescription as the prescribing practitioner and who has indicated that the prescription is ready to be signed to sign the prescription.	Inspected through observation that the EPA would not permit authorized EPCS user to sign for a prescription that was previously prescribed by another practitioner. No relevant exceptions noted.

Table A - DEA 1311.120 Electronic Prescription Application **Perform procedures to find reasonable assurance that the application functionality met the requirements of this part.**		
DEA Ref#	**DEA EPA Criteria Requirements**	**Procedures Performed and Results**
1311.120 (b) (13)	Where a practitioner seeks to prescribe more than one controlled substance at one time for a particular patient, the electronic prescription application may allow the practitioner to sign multiple prescriptions for a single patient at one time using a single invocation of the two-factor authentication protocol provided the following has occurred: The practitioner has individually indicated that each controlled substance prescription is ready to be signed while the information required by paragraph (b)(9) of this section for each such prescription is displayed along with the statement required by § 1311.140(a)(3).	Inspected through observation of the prescribing process to verify that when signing multiple prescriptions for a single patient only prescriptions that were previously flagged as ready for signing would populate in the sign and send screen with the following statement displayed “By completing the two-factor authentication protocol at this time, you are legally signing the prescription(s) and authorizing the transmission of the above information to the pharmacy for dispensing. The two-factor authentication protocol may only be completed by the practitioner whose name and DEA registration number appear below.” when performing the two-factor authentication. No relevant exceptions noted.
1311.120 (b) (14)	The electronic prescription application time and date stamps the prescription when the signing function is used.	Inspected the log of signed prescription history to verify that the date, time, module, action, patient, Rx, description, outcome, digital signature hash and other elements were stored for each transaction. No relevant exceptions noted.
1311.120 (b) (15)	When the practitioner uses his two-factor authentication credential as specified in §1311.140(a)(4), the electronic prescription application digitally signs at least the information required by part 1306 of this chapter and electronically archive the digitally signed record. If the practitioner signs the prescription with his own private key, as provided in § 1311.145, the electronic prescription application electronically archives a copy of the digitally signed record, but need not apply the application's digital signature to the record.	Inspected the application logs for a sample of signed prescriptions and the code used for signing to verify that the following information was captured, stored and available upon retrieval: dated as of and signed on, the day when issued, 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. No relevant exceptions noted.
1311.120 (b) (16)	The digital signature functionality meets the following requirements:	

Table A - DEA 1311.120 Electronic Prescription Application **Perform procedures to find reasonable assurance that the application functionality met the requirements of this part.**		
DEA Ref#	**DEA EPA Criteria Requirements**	**Procedures Performed and Results**
1311.120 (b) (16) (i)	The cryptographic module used to digitally sign the data elements required by part 1306 of this chapter is at least FIPS 140-2 Security Level 1 validated. FIPS 140-21 is incorporated by reference in § 1311.08.	Inspected the digital signature implemented into the application to verify that they were utilizing RSA Crypto Service Provider which was FIPS 140-2 verified. Observed a test prescription to verify that the prescription data was signed and the SI flag indicated in message sent to Clearing House. Inspected the validated FIPS 140-2 certificates located at csrc.nist.gov to verify FIPS validation. No relevant exceptions noted.
1311.120 (b) (16) (ii)	(The digital signature application and hash function complies with FIPS 186-3 and FIPS 180-3, as incorporated by reference in § 1311.08.	Inspected the digital signature module implemented into the application to verify that they were utilizing RSA Crypto Service Provider which was FIPS 140-2 verified. No relevant exceptions noted.
1311.120 (b) (16) (iii)	The electronic prescription 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. FIPS 140-23 is incorporated by reference in § 1311.08.	Inspected the digital signature implemented into the application to verify that they were utilizing RSA Crypto Service Provider which was FIPS 140-2 verified and stored the private key encrypted. Inspected the validated FIPS 140-2 certificates located at csrc.nist.gov to verify FIPS validation. No relevant exceptions noted.
1311.120 (b) (16) (iv)	For software implementations, when the signing module is deactivated, the application clears the plain text password from the application memory to prevent the unauthorized access to, or use of, the private key.	N/A – the application is a hosted application. No relevant exceptions noted.
1311.120 (b) (17)	Unless the digital signature created by an individual practitioner's private key is being transmitted to the pharmacy with the prescription, the electronic prescription application includes in the data file transmitted an indication that the prescription was signed by the prescribing practitioner.	Inspected the message digest for a sample of transmitted prescriptions to verify that the message include the “SI” flag to indicate that the prescription had been signed by the prescribing practitioner. No relevant exceptions noted.
1311.120 (b) (18)	The electronic prescription application does not transmit a controlled substance prescription unless the signing function described in § 1311.140(a)(4) has been used.	Observed the prescribing process for EPCS to verify that prescriptions could not transmit until the validate two-factor authentication was completed. No relevant exceptions noted.

Table A - DEA 1311.120 Electronic Prescription Application **Perform procedures to find reasonable assurance that the application functionality met the requirements of this part.**		
DEA Ref#	**DEA EPA Criteria Requirements**	**Procedures Performed and Results**
1311.120 (b) (19)	The electronic prescription application does not allow alteration of any of the information required by part 1306 of this chapter after the prescription has been digitally signed. Any alteration of the information required by part 1306 of this chapter after the prescription is digitally signed cancels the prescription.	Inspected a sample of signed scripts to verify that signed scripts became read only in the system and were not modifiable. No relevant exceptions noted.
1311.120 (b) (20)	The electronic prescription application does not allow transmission of a prescription that has been printed.	Inspected a sample of printed electronic prescriptions to verify that there was not a transmission capability post printing. No relevant exceptions noted.
1311.120 (b) (21)	The electronic prescription application allows printing of a prescription after transmission only if the printed prescription is clearly labeled as a copy not for dispensing. The electronic prescription application may allow printing of prescription information if clearly labeled as being for informational purposes. The electronic prescription application may transfer such prescription information to medical records.	Inspected a sample of electronic prescriptions transmitted electronically to verify that there was no option to print these transmitted prescriptions. No relevant exceptions noted.
1311.120 (b) (22)	If the transmission of an electronic prescription fails, the electronic prescription application may print the prescription. The prescription indicates that it was originally transmitted electronically to, and provide the name of, a specific pharmacy, the date and time of transmission, and that the electronic transmission failed.	Inspected a sample failed transmission error to verify that a failed transmission had no printing options available in the application. No relevant exceptions noted.
1311.120 (b) (23)	The electronic prescription application maintains an audit trail of all actions related to the following:	
1311.120 (b) (23) (i)	The creation, alteration, indication of readiness for signing, signing, transmission, or deletion of a controlled substance prescription.	Inspected application audit logs to verify that transactions were recorded for the following events; ready to sign, signing, transmission, delete, open, view, create, save, and more. No relevant exceptions noted.

Table A - DEA 1311.120 Electronic Prescription Application **Perform procedures to find reasonable assurance that the application functionality met the requirements of this part.**		
DEA Ref#	**DEA EPA Criteria Requirements**	**Procedures Performed and Results**
1311.120 (b) (23) (ii)	Any setting or changing of logical access control permissions related to the issuance of controlled substance prescriptions.	Inspected application audit logs to verify that transactions were recorded for logical access modifications. No exception noted.
1311.120 (b) (23) (iii)	Notification of a failed transmission.	Inspected application audit logs to verify that transactions of failed transmissions or errors were recorded. No relevant exceptions noted.
1311.120 (b) (23) (iv)	Auditable events as specified in § 1311.150.	See testing for 1311.150 below.
1311.120 (b) (24)	The electronic prescription application records within each audit record the following information:	
1311.120 (b) (24) (i)	The date and time of the event.	Inspected application audit trails to verify the following was captured for each transaction; date and time of events. No relevant exceptions noted.
1311.120 (b) (24) (ii)	The type of event.	Inspected application audit trails to verify the following was captured for each transaction; type of event via descriptions. No relevant exceptions noted.
1311.120 (b) (24) (iii)	The identity of the person taking the action, where applicable.	Inspected application audit trails to verify the following was captured for each transaction; associated user ID of transactions. No relevant exceptions noted.
1311.120 (b) (24) (iv)	The outcome of the event (success or failure).	Inspected application audit trails to verify the following was captured for each transaction; success or failure in the outcome field. No relevant exceptions noted.
1311.120 (b) (25)	The electronic prescription application conducts internal audits and generate reports on any of the events specified in § 1311.150 in a format that is readable by the practitioner. Such internal audits may be automated and need not require human intervention to be conducted.	Inspected sample incident report that was available on demand every 24 hours to verify requirements from 1311.150 were reported on. This can be found in the alerts and messages menu. No relevant exceptions noted.
1311.120 (b) (26)	The electronic prescription application protects the stored audit records from unauthorized deletion. The electronic prescription application shall prevent modifications to the audit records.	Inspected the application logs to verify that application logs access via the application was read only, users have view access only. No relevant exceptions noted.

Table A - DEA 1311.120 Electronic Prescription Application **Perform procedures to find reasonable assurance that the application functionality met the requirements of this part.**		
DEA Ref#	**DEA EPA Criteria Requirements**	**Procedures Performed and Results**
1311.120 (b) (27)	The electronic prescription application does the following:	
1311.120 (b) (27) (i)	Generate a log of all controlled substance prescriptions issued by a practitioner during the previous calendar month and provide the log to the practitioner no later than seven calendar days after that month.	Inspected the application logs to verify that application logs were capable of the following; generating report of all controlled substance prescriptions issues during previous calendar month. No relevant exceptions noted.
1311.120 (b) (27) (ii)	Be capable of generating a log of all controlled substance prescriptions issued by a practitioner for a period specified by the practitioner upon request. Prescription information available from which to generate the log spans at least the previous two years.	Inspected the application logs to verify that application logs were capable of the following; running date range reports for log of all controlled substances prescriptions, and was available for at least two years. No relevant exceptions noted.
1311.120 (b) (27) (iii)	Archive all logs generated.	Inspected the application logs to verify that application logs were capable of the following; logs were backed up and archived hourly. No relevant exceptions noted.
1311.120 (b) (27) (iv)	Ensure that all logs are easily readable or easily rendered into a format that a person can read.	Inspected the application logs to verify that application logs were capable of the following; logs were presented in a readable presentation. No relevant exceptions noted.
1311.120 (b) (27) (v)	Ensure that all logs are sortable by patient name, drug name, and date of issuance of the prescription.	Inspected the application logs to verify that application logs were capable of the following; logs were sortable by date, patient last name, first name, drug type, directions schedule, routed, pharmacy, routed date, and status. No relevant exceptions noted.
1311.120 (b) (28)	(28) Where the electronic prescription application is required by this part to archive or otherwise maintain records, it retains such records electronically for two years from the date of the record's creation and comply with all other requirements of § 1311.305.	Inspected the log retention policy to verify that WENO policy required the retention of logs indefinitely and required a minimum of 2 years to be readily available. No relevant exceptions noted.
1311.135	**Requirements for creating a controlled substance prescription.**	

Table A - DEA 1311.120 Electronic Prescription Application **Perform procedures to find reasonable assurance that the application functionality met the requirements of this part.**		
DEA Ref#	**DEA EPA Criteria Requirements**	**Procedures Performed and Results**
1311.135 (a)	The electronic prescription application may allow the registrant or his agent to enter data for a controlled substance prescription, provided that only the registrant may sign the prescription in accordance with §§ 1311.120(b)(11) and 1311.140.	See testing results above under DEA 1311.120 (b) (11). It is the responsibility of the practitioner to secure their credentials to restrict who can sign prescriptions. No relevant exceptions noted.
1311.135 (b)	If a practitioner holds multiple DEA registrations, the practitioner or his agent selects the appropriate registration number for the prescription being issued in accordance with the requirements of § 1301.12 of this chapter.	Inspected the application to verify that only one DEA registration number was permitted per user account. It is the practitioner's responsibility to log into the correct account when creating and signing prescriptions. No relevant exceptions noted.
1311.135 (c)	If required by State law, a supervisor's name and DEA number may be listed on a prescription, provided the prescription clearly indicates who is the supervisor and who is the prescribing practitioner.	N/A – the application does not have the functionality of a supervisor role. No relevant exceptions noted.
1311.140	**Requirements for signing a controlled substance prescription.**	
1311.140 (a)	For a practitioner to sign an electronic prescription for a controlled substance the following occurs:	
1311.140 (a) (1)	The practitioner accesses a list of one or more controlled substance prescriptions for a single patient. The list displays the information required by § 1311.120(b)(9).	See testing results above under DEA 1311.120 (b) (9). No relevant exceptions noted.
1311.140 (a) (2)	The practitioner indicates the prescriptions that are ready to be signed.	See testing results above under DEA 1311.120 (b) (9). No relevant exceptions noted.

Table A - DEA 1311.120 Electronic Prescription Application **Perform procedures to find reasonable assurance that the application functionality met the requirements of this part.**		
DEA Ref#	**DEA EPA Criteria Requirements**	**Procedures Performed and Results**
1311.140 (a) (3)	While the prescription information required in § 1311.120(b)(9) is displayed, the following statement or its substantial equivalent is displayed: "By completing the two-factor authentication protocol at this time, you are legally signing the prescription(s) and authorizing the transmission of the above information to the pharmacy for dispensing. The two-factor authentication protocol may only be completed by the practitioner whose name and DEA registration number appear above."	See testing results above under DEA 1311.120 (b) (9). No relevant exceptions noted.
1311.140 (a) (4)	While the prescription information required in § 1311.120(b)(9) and the statement required by paragraph (a)(3) of this section remain displayed, the practitioner is prompted to complete the two-factor authentication protocol.	See testing results above under DEA 1311.120 (b) (9). No relevant exceptions noted.
1311.140 (a) (5)	The completion by the practitioner of the two-factor authentication protocol in the manner provided in paragraph (a)(4) of this section will constitute the signing of the prescription by the practitioner for purposes of § 1306.05(a) and (e) of this chapter.	See testing results above under DEA 1311.120 (b) (9). No relevant exceptions noted.
1311.140 (a) (6)	Except as provided under § 1311.145, the practitioner's completion of the two-factor authentication protocol causes the application to digitally sign and electronically archive the information required under part 1306 of this chapter.	See testing results above under DEA 1311.120 (b) (9). No relevant exceptions noted.
1311.140 (b)	(b) The electronic prescription application clearly labels as the signing function the function that prompts the practitioner to execute the two-factor authentication protocol using his credential.	See testing results above under DEA 1311.120 (b) (9). No relevant exceptions noted.
1311.140 (c)	(c) Any prescription not signed in the manner required by this section shall not be transmitted.	See testing results above under DEA 1311.120 (b) (9). No relevant exceptions noted.

Table A - DEA 1311.120 Electronic Prescription Application **Perform procedures to find reasonable assurance that the application functionality met the requirements of this part.**		
DEA Ref#	**DEA EPA Criteria Requirements**	**Procedures Performed and Results**
1311.145	**Digitally signing the prescription with the individual practitioner's private key.**	
1311.145 (a)	An individual practitioner who has obtained a digital certificate as provided in § 1311.105 may digitally sign a controlled substance prescription using the private key associated with his digital certificate.	N/A, does not sign with private key.
1311.145 (b)	The electronic prescription application requires the individual practitioner to complete a two-factor authentication protocol as specified in § 1311.140(a)(4) to use his private key.	N/A, does not sign with private key.
1311.145 (c)	The electronic prescription application digitally signs at least all information required under part 1306 of this chapter.	N/A, does not sign with private key.
1311.145 (d)	The electronic prescription application electronically archives the digitally signed record.	N/A, does not sign with private key.
1311.145 (e)	A prescription that is digitally signed with a practitioner's private key may be transmitted to a pharmacy without the digital signature.	N/A, does not sign with private key.
1311.145 (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.	N/A, does not sign with private key.

Table A - DEA 1311.120 Electronic Prescription Application **Perform procedures to find reasonable assurance that the application functionality met the requirements of this part.**		
DEA Ref#	**DEA EPA Criteria Requirements**	**Procedures Performed and Results**
1311.145 (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.	N/A, does not sign with private key.
1311.150	**Additional requirements for internal application audits.**	
1311.150 (a)	The application provider establishes and implements a list of auditable events. Auditable events, at a minimum, include the following:	
1311.150 (a) (1)	Attempted unauthorized access to the electronic prescription application or successful unauthorized access where the determination of such is feasible.	Inspected application logs to verify the application logged the following events; successful and failed authorization of account access. No relevant exceptions noted.
1311.150 (a) (2)	Attempted 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.	Inspected the application to verify that users without permission were restricted from access unauthorized fields or objects and therefore no unauthorized activity was permissible. All events were recorded in application logs. No relevant exceptions noted.
1311.150 (a) (3)	Interference with application operations of the prescription application.	Inspected application logs to verify that interruption of application operations were logged for failed actions. No relevant exceptions noted.
1311.150 (a) (4)	Any setting of or change to logical access controls related to the issuance of controlled substance prescriptions.	Inspected application logs to verify that logical security to user profiles were logged and available. No relevant exceptions noted.
1311.150 (a) (5)	Attempted or successful interference with audit trail functions.	Inspected audit trail functionality to verify audit trail functionality was based on the application software compiled code and was not accessible via the application user interface and therefore was not possible to turn on/off without changing the application code. Logical security controls (see logical security section below) were in place to prevent unauthorized changes to the production code. No relevant exceptions noted.

Table A - DEA 1311.120 Electronic Prescription Application **Perform procedures to find reasonable assurance that the application functionality met the requirements of this part.**		
DEA Ref#	**DEA EPA Criteria Requirements**	**Procedures Performed and Results**
1311.150 (a) (6)	For application service providers, attempted or successful creation, modification, 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.	All users of the application, included application service provider personnel or agents were logged in the same manner as the other users of the application. Support staff does not have logins to the provider's data. No relevant exceptions noted.
1311.150 (b)	The electronic prescription application analyzes the audit trail at least once every calendar day and generate an incident report that identifies each auditable event.	Inspected the daily report that was generated and any identified auditable events 1311.150 (a)(1-6) created an alert in the application that remained an open task until viewed. No relevant exceptions noted.
1311.170	**Transmission requirements.**	
1311.170 (a)	The electronic prescription application transmits the electronic prescription as soon as possible after signature by the practitioner.	Inspected the signing process to verify that prescriptions were scheduled for transmission upon signature. No relevant exceptions noted.
1311.170 (b)	The electronic prescription application may print a prescription that has been transmitted only if an intermediary or the designated pharmacy notifies a practitioner that an electronic prescription was not successfully delivered to the designated pharmacy. If this occurs, the electronic prescription application may print the prescription for the practitioner's manual signature. The printed prescription includes information noting that the prescription was originally transmitted electronically to [name of the specific pharmacy] on [date/time] and that transmission failed.	See testing results above under DEA 1311.120 (b) (21). No relevant exceptions noted.
1311.170 (c)	The electronic prescription application may print copies of the transmitted prescription if they are clearly labeled: "Copy only--not valid for dispensing." Data on the prescription may be electronically transferred to medical records, and a list of prescriptions written may be printed for patients if the list indicates that it is for informational purposes only and not for dispensing.	See testing results above under DEA 1311.120 (b) (21). No relevant exceptions noted.

Table A - DEA 1311.120 Electronic Prescription Application **Perform procedures to find reasonable assurance that the application functionality met the requirements of this part.**		
DEA Ref#	**DEA EPA Criteria Requirements**	**Procedures Performed and Results**
1311.170 (d)	The electronic prescription application does not allow the transmission of an electronic prescription if an original prescription was printed prior to attempted transmission.	See testing results above under DEA 1311.120 (b) (20). No relevant exceptions noted.
1311.305	**Recordkeeping.**	
1311.305 (a)	If a prescription is created, signed, transmitted, and received electronically, all records related to that prescription are retained electronically.	See testing results above under DEA 1311.120 (b) (28). No relevant exceptions noted.
1311.305 (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.	See testing results above under DEA 1311.120 (b) (28). No relevant exceptions noted.
1311.305 (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.	See testing results above under DEA 1311.120 (b) (28). No relevant exceptions noted.
1311.305 (d)	Records required by this part are made available to the Administration upon request.	See testing results above under DEA 1311.120 (b) (28). No relevant exceptions noted.
1306.05	**Manner of issuance of prescriptions.**	
1306.05 (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.	See testing results above under DEA 1311.120 (b) (15). No relevant exceptions noted.

Table A - DEA 1311.120 Electronic Prescription Application **Perform procedures to find reasonable assurance that the application functionality met the requirements of this part.**		
DEA Ref#	**DEA EPA Criteria Requirements**	**Procedures Performed and Results**
1306.05 (e)	Electronic prescriptions shall be created and signed using an application that meets the requirements of **part 1311 of this chapter**.	See testing results above under DEA 1311.120 (b) (1-28). No relevant exceptions noted.
1311.115	**Additional requirements for two-factor authentication.**	
1311.115 (a)	To sign a controlled substance prescription, the electronic prescription application requires the practitioner to authenticate to the application using an authentication protocol that uses two of the following three factors:	Observed the authentication procedure to validate the application required a pass code with hard or soft token device which meets requirement 1311.115 (a) (1) and 1311.115 (a) (3). No relevant exceptions noted.
1311.115 (a) (1)	Something only the practitioner knows, such as a password or response to a challenge question.	
1311.115 (a) (2)	Something the practitioner is, biometric data such as a fingerprint or iris scan.	
1311.115 (a) (3)	Something the practitioner has, a device (hard token) separate from the computer to which the practitioner is gaining access.	
1311.115 (b)	If one factor is a hard token, it is separate from the computer to which it is gaining access and meets at least the criteria of FIPS 140-2 Security Level 1, as incorporated by reference in § 1311.08, for cryptographic modules or one-time-password devices.	See testing results above under DEA 1311.120 (b) (9). No relevant exceptions noted.
1311.115 (c)	If one factor is a biometric, the biometric subsystem complies with the requirements of § 1311.116.	N/A – no biometric devices w used for WENO.
1311.116	**Additional requirements for biometrics.**	
1311.116 (a)	If one of the factors used to authenticate to the electronic prescription application is a biometric as described in § 1311.115, it complies with the following requirements.	N/A – no biometric devices are used for WENO.
1311.116 (b)	The biometric subsystem operates at a false match rate of 0.001 or lower.	N/A – no biometric devices are used for WENO.

Table A - DEA 1311.120 Electronic Prescription Application **Perform procedures to find reasonable assurance that the application functionality met the requirements of this part.**		
DEA Ref#	**DEA EPA Criteria Requirements**	**Procedures Performed and Results**
1311.116 (c)	The biometric subsystem uses matching software that has demonstrated performance at the operating point corresponding with the false match rate described in paragraph (b) of this section, or a lower false match rate. Testing to demonstrate performance is conducted by the National Institute of Standards and Technology or another DEA- approved government or nongovernment laboratory. Such testing complies with the requirements of paragraph (h) of this section.	N/A – no biometric devices are used for WENO.
1311.116 (d)	The biometric subsystem conforms to Personal Identity Verification authentication biometric acquisition specifications, pursuant to NIST SP 800-76-1 as incorporated by reference in § 1311.08, if they exist for the biometric modality of choice.	N/A – no biometric devices are used for WENO.
1311.116 (e)	The biometric subsystem is either co-located with a computer or PDA that the practitioner uses to issue electronic prescriptions for controlled substances, where the computer or PDA is located in a known, controlled location, or built directly into the practitioner's computer or PDA that he uses to issue electronic prescriptions for controlled substances.	N/A – no biometric devices are used for WENO.
1311.116 (f)	The biometric subsystem stores device ID data at enrollment (i.e., biometric registration) with the biometric data and verify the device ID at the time of authentication to the electronic prescription application.	N/A – no biometric devices are used for WENO.
1311.116 (g)	The biometric subsystem protects the biometric data (raw data or templates), match results, and/or non-match results when authentication is not local. If sent over an open network, biometric data (raw data or templates), match results, and/or non-match results are:	

Table A - DEA 1311.120 Electronic Prescription Application **Perform procedures to find reasonable assurance that the application functionality met the requirements of this part.**		
DEA Ref#	**DEA EPA Criteria Requirements**	**Procedures Performed and Results**
1311.116 (g) (1)	Cryptographically source authenticated;	N/A – no biometric devices are used for WENO.
1311.116 (g) (2)	Combined with a random challenge, a nonce, or a time stamp to prevent replay;	N/A – no biometric devices are used for WENO.
1311.116 (g) (3)	Cryptographically protected for integrity and confidentiality; and	N/A – no biometric devices are used for WENO.
1311.116 (g) (4)	Sent only to authorized systems.	N/A – no biometric devices are used for WENO.
1311.116 (h)	Testing of the biometric subsystem has the following characteristics:	N/A – no biometric devices are used for WENO.
1311.116 (h) (1)	The test is conducted by a laboratory that does not have an interest in the outcome (positive or negative) of performance of a submission or biometric.	N/A – no biometric devices are used for WENO.
1311.116 (h) (2)	Test data are sequestered.	N/A – no biometric devices are used for WENO.
1311.116 (h) (3)	Algorithms are provided to the testing laboratory (as opposed to scores or other information).	N/A – no biometric devices are used for WENO.
1311.116 (h) (4)	The operating point(s) corresponding with the false match rate described in paragraph (b) of this section, or a lower false match rate, is tested so that there is at least 95% confidence that the false match and non-match rates are equal to or less than the observed value.	N/A – no biometric devices are used for WENO.
1311.116 (h) (5)	Results of the testing are made publicly available.	N/A – no biometric devices are used for WENO.

Table B - Information Security

Control Objective 2: Control activities provide reasonable assurance that logical access to critical systems and data is restricted to authorized individuals and to foster system processing is complete, accurate, timely and authorized.

Control #	Control Activity	Testing Procedures and Results
IS.1	Formal information security policies and procedures are in place to establish organizational information security standards.	Inquired of the CEO to verify that information security policies and procedures were in place to establish organizational information security standards. Inspected the information security policies and procedures to verify that organizational information security standards were documented. No relevant exceptions noted.
IS.2	IT access requests are approved prior to granting access to production systems.	Inquired of the CEO to verify that an approved IT access request was required prior to granting access to production systems. Inspected IT authorization procedures for new production system accounts to verify that production system access was required to be authorized. No relevant exceptions noted.
IS.3	<u>Windows Operating System Access</u> Server operating system authentication is restricted via unique user account and passwords that required: ➢ Minimum length of eight characters ➢ Maximum age of 180 days ➢ Password history requirement of three ➢ Complexity requirement ➢ Lockout threshold of 5 consecutive failed attempts	Inquired of the CEO to verify that server operating system authentication user account passwords required the following characteristics: ➢ Minimum length of eight characters ➢ Maximum age of 180 days ➢ Password history requirement of three ➢ Complexity requirement ➢ Lockout threshold of 5 consecutive failed attempts Inspected the application password authentications to verify that application authentication user account passwords required the following characteristics: ➢ Minimum length of eight characters ➢ Maximum age of 180 days ➢ Password history requirement of three ➢ Complexity requirement ➢ Lockout threshold of 5 consecutive failed attempts No relevant exceptions noted.
IS.4	Administrative access to the server operating system is restricted to personnel with administration job responsibilities.	Inquired of the CEO 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.

Table B - Information Security

Control Objective 2: Control activities provide reasonable assurance that logical access to critical systems and data is restricted to authorized individuals and to foster system processing is complete, accurate, timely and authorized.

Control #	Control Activity	Testing Procedures and Results
IS.5	User access to server operating systems is revoked upon notification of termination.	Inquired of the CEO 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.
IS.6	Operating System Logging The operating system audit settings are configured to log specific events.	Inquired of the CEO 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.
IS.7	Database Access Database authentication is restricted via unique user account, service accounts and data center hosting accounts and based on windows authentication.	Inquired of the CEO to verify that database authentication was restricted to unique user account, service accounts and data center hosting accounts and based on windows authentication. Inspected the application password authentications to verify that database authentication was based on windows authentication. No relevant exceptions noted.
IS.8	Access to the database is restricted via authorized application, administrator accounts, and data center hosting accounts.	Inquired of the CEO to verify that access to the database was restricted via authorized application, administrator accounts, and data center hosting accounts. Inspected the database user accounts and roles permissions to verify that access to the databases was restricted to IT personnel with administrative job responsibilities. No relevant exceptions noted.
IS.9	Database access privileges are revoked as a component of the termination process.	Inquired of the CEO to verify that database access privileges were revoked upon notification of termination. Inspected the database user access to verify that access of terminated personnel was revoked. No relevant exceptions noted.
IS.10	Database Logging The database records certain user account activity that is available for ad hoc review.	Inquired of the CEO to verify that the database logs record certain user activity that was available for adhoc review. Inspected the database configurations and email alert notification to verify that database logs records certain user account activity that was available for ad hoc review. No relevant exceptions noted.

Table B - Information Security

Control Objective 2: Control activities provide reasonable assurance that logical access to critical systems and data is restricted to authorized individuals and to foster system processing is complete, accurate, timely and authorized.

Control #	Control Activity	Testing Procedures and Results
IS.11	Application Authentication Application authentication is restricted via unique user account and passwords that required: ➢ Minimum length of six characters ➢ Alpha and numeric ➢ Complexity requirements of one number and one symbol	Inquired of the CEO to verify that application authentication user account passwords required the following characteristics: ➢ Minimum length of six characters ➢ Alpha and numeric ➢ Complexity requirements of one number and one symbol Inspected the application password authentications to verify that application authentication user account passwords required the following characteristics: ➢ Minimum length of six characters ➢ Alpha and numeric ➢ Complexity requirements of one number and one symbol No relevant exceptions noted.
IS.12	Application Access Controls Access to administer the application is limited to personnel based on their job responsibilities.	Inquired of the CEO to verify that access to administer the application was limited to certain personnel with application administration responsibilities. 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.
IS.13	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 CEO to verify that the application was configured to log certain user account application activities and was available for ad hoc review purposes. Inspected a sample of application logs to verify that application activities were logged and available for ad hoc review. No relevant exceptions noted.
IS.14	Firewall Administration A firewall and web application firewall are in place to help prevent unauthorized access.	Inspected the firewall and web application firewall settings to verify they were in place. No relevant exceptions noted.
IS.15	Firewall rulesets and configurations have documented business justifications and changes to firewall rules required management approval.	Inquired of the CEO to verify that fire rulesets and configurations had documented business justifications and changes to rules required Management approval. No relevant exceptions noted.

Table B - Information Security

Control Objective 2: Control activities provide reasonable assurance that logical access to critical systems and data is restricted to authorized individuals and to foster system processing is complete, accurate, timely and authorized.

Control #	Control Activity	Testing Procedures and Results
		Inspected the documented business justifications and change control procedures to verify that firewall rulesets and configurations were documented and changes required management approval. No relevant exceptions noted.
IS.16	Remote Access Customer web sessions are encrypted using a certification authority.	Inquired of the CEO to verify that customer web sessions were encrypted. Inspected the approved certificates to verify web sessions were encrypted.
IS.17	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 CEO 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. Inspected the encryption settings to verify that remote access was encrypted. No relevant exceptions noted.