McKesson Pharmacy Systems

IPPI Zadall ePrescribing Pharmacy Management Application version 1.8.0

Independent Application

Third Party Audit on Compliance with United States' Drug Enforcement Administration, Title 21, Code of Federal Regulations, Chapter II, Part 1311

February 12, 2013

Attestation and Compliance Services

BrightLine

Table of Contents

Section I

Certified Information Systems Auditor's Report on Compliance

February 19, 2013

To Whom It May Concern:

BrightLine CPAs & Associates, Inc. ("BrightLine") has completed an independent third party audit of the hosted IPPI Zadall ePrescribing Pharmacy Management Independent Application version 1.8.0 (the "Application") for controlled substances administered by McKesson Pharmacy Systems (the "Application Service Provider"). The objectives of our third party audit were to

i. determine whether the Application was capable of performing the relevant and requisite functions set forth in the United States Department of Justice Drug Enforcement Administration's requirements for pharmacy applications for controlled substances as defined in Title 21 of the Code of Federal Regulations, Parts 1300, 1304, 1306 and 1311 (the "Regulation") and dated April 1, 2010. Specific pharmacy application requirements are provided in section 2 ("Applicable Pharmacy Application Requirements") of this document.

ii. assess processing integrity and physical security as defined in requirement §1311.300(d) of the Regulation. The controls that address processing integrity and physical security are provided in section 3 ("Processing Integrity and Physical Security Controls").

We have determined that the Application accurately and consistently imported, stored, and displayed (i) the information required for a prescription by §1306.05(a), (ii) the number of refills as required by §1306.22, and (iii) the indication that the prescription was signed by a practitioner's digital signature as required by §1311.205(b)(6). Additionally, we have determined that the Application accepts prescriptions with the practitioner's digital signature and does accurately and consistently import, store, and verify the practitioner's digital signature.

Our third party audit, as that term is defined at 1300.03 and 1311.300 of the Regulation, is a determination of the Application's capability to satisfy the requirements set forth in the Regulation as of February 12, 2013. Per the Regulation, our determination should not be projected to future versions of the Application, whenever a functionality related to controlled substance prescription requirements is altered within the Application, or periods two calendar years after the date of this report, whichever occurs first. Our third party audit was not intended to detect errors or fraud that may have occurred during the course of our third party audit.

Although our organization is a licensed CPA firm, we did not conduct our third party audit in accordance with attestation standards established by the American Institute of Certified Public Accountants. Furthermore, we are not a law firm, and therefore, our third party audit is not a legal determination of compliance with the Regulation. This third party audit was conducted by a team of Certified Information Systems Auditors who perform compliance audits as a regular ongoing business activity, and as such, were qualified to conduct this third party audit per §1311.300(b) of the Regulation.

The sufficiency of the requirements is solely the responsibility of the United States Department of Justice Drug Enforcement Administration. Consequently, we make no representation regarding the sufficiency of the requirements of the Regulation either for the purpose for which this report has been requested or for any other purpose.

This report is intended solely for use by the management of the Application Service Provider and the current and prospective users of the Application.

Ryan J. Buckner, Certified Information Systems Auditor
Principal

SECTION 2

APPLICABLE PHARMACY APPLICATION REQUIREMENTS

PART 1311.205

Applicable Pharmacy Application Requirements

Point No.	DEA Regulatory Reference	DEA Regulatory Requirement
1.	1311.205 (b) (1) (i)	The pharmacy application must be capable of setting logical access controls to limit access for the following function: (i) Annotation, alteration, or deletion of prescription information.
2.	1311.205 (b) (1) (ii)	The pharmacy application must be capable of setting logical access controls to limit access for the following function: (ii) Setting and changing the logical access controls.
3.	1311.205 (b) (2)	Logical access controls must be set by individual user name or role.
4.	1311.205 (b) (3)	The pharmacy application must digitally sign and archive a prescription on receipt or be capable of receiving and archiving a digitally signed record.
5.	1311.205 (b) (4) (i)	For pharmacy applications that digitally sign prescription records upon receipt, the digital signature functionality must meet the following requirement: (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.
6.	1311.205 (b) (4) (ii)	For pharmacy applications that digitally sign prescription records upon receipt, the digital signature functionality must meet the following requirement: (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.
7.	1311.205 (b) (4) (iii)	For pharmacy applications that digitally sign prescription records upon receipt, the digital signature functionality must meet the following requirement: (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.
8.	1311.205 (b) (4) (iv)	For pharmacy applications that digitally sign prescription records upon receipt, the digital signature functionality must meet the following requirement: (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.
9.	1311.205 (b) (4) (v)	For pharmacy applications that digitally sign prescription records upon receipt, the digital signature functionality must meet the following requirement: (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.
10.	1311.205 (b) (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).

Point No.	DEA Regulatory Reference	DEA Regulatory Requirement
11.	1311.205 (b) (6) (i)	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
12.	1311.205 (b) (6) (ii)	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: (ii) Display the field for the pharmacist's verification.
13.	1311.205 (b) (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.
14.	1311.205 (b) (8)	The pharmacy application must read and store, and be capable of displaying, all information required by part 1306 of this chapter.
15.	1311.205 (b) (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.
16.	1311.205 (b) (10) (i)	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.
17.	1311.205 (b) (10) (ii)	The pharmacy application must provide for the following information to be added or linked to each electronic controlled substance prescription record for each dispensing: (ii) Date dispensed.
18.	1311.205 (b) (10) (iii)	The pharmacy application must provide for the following information to be added or linked to each electronic controlled substance prescription record for each dispensing: (iii) Name or initials of the person who dispensed the prescription.
19.	1311.205 (b) (11)	The pharmacy application must be capable of retrieving controlled substance prescriptions by practitioner name, patient name, drug name, and date dispensed.
20.	1311.205 (b) (12)	The pharmacy application must allow downloading of prescription data into a database or spreadsheet that is readable and sortable.
21.	1311.205 (b) (13) (i)	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.
22.	1311.205 (b) (13) (ii)	The pharmacy application must maintain an audit trail of all actions related to the following: (ii) Any setting or changing of logical access control permissions related to the dispensing of controlled substance prescriptions.
23.	1311.205 (b) (13) (iii)	The pharmacy application must maintain an audit trail of all actions related to the following: (iii) Auditable events as specified in § 1311.215.
24.	1311.205 (b) (14) (i)	The pharmacy application must record within each audit record the following information: (i) The date and time of the event.

Point No.	DEA Regulatory Reference	DEA Regulatory Requirement
25.	1311.205 (b) (14) (ii)	The pharmacy application must record within each audit record the following information: (ii) The type of event.
26.	1311.205 (b) (14) (iii)	The pharmacy application must record within each audit record the following information: (iii) The identity of the person taking the action, where applicable.
27.	1311.205 (b) (14) (iv)	The pharmacy application must record within each audit record the following information: (iv) The outcome of the event (success or failure).
28.	1311.205 (b) (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.
29.	1311.205 (b) (16)	The pharmacy application must protect the stored audit records from unauthorized deletion. The pharmacy application shall prevent modifications to the audit records.
30.	1311.205 (b) (17)	The pharmacy application must back up the controlled substance prescription records daily.
31.	1311.205 (b) (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.

PART 1311.300

Applicable Provider Requirements – Third Party Audits or Certifications

Point No.	DEA Regulatory Reference	DEA Regulatory Requirement
1.	1311.300 (d)	An audit for application service providers must address processing integrity and physical security and determine that the application meets the requirements of Part 1311.

SECTION 3

PROCESSING INTEGRITY AND PHYSICAL SECURITY CONTROLS

PROCESSING INTEGRITY

Control No.	Control Activity Implemented by the Application Service Provider
	Policies and Procedures
1.	Documented change control procedures are in place to guide application development, maintenance and documentation activities.
	Version Control
2.	Application development personnel utilize version control software to manage application development and maintenance activities.
3.	The version control software maintains a history log of code check-in/out and the user account associated with the activity.
4.	Changes to source code results in the creation of a new version of the application code. Changes are capable of being rolled back to prior versions of the application code on an as needed basis.
	Change Control
5.	A ticketing system is used to track, review and prioritize emergency and non-emergency change requests.
6.	Documented change requests are completed for bug fixes, enhancements and new development.
7.	Quality assurance testing is performed on application changes prior to implementation into the production environment.
8.	Application changes are approved prior to migration to the production environment. Approval is documented in a ticketing system.
9.	A documented emergency change request is required to be completed prior to implementation to the production environment.
10.	Write access to the version control software is restricted to user accounts accessible by authorized personnel (10).
11.	The ability to promote application code into the application production environment is restricted to user accounts accessible by authorized personnel (3).
12.	A file integrity monitoring tool is configured to monitor production executables when production files and directories are modified.
	Network Monitoring
13.	Internal personnel utilize a third party application to perform scans of the production network on at least a monthly basis.
14.	A formal risk assessment is performed on at least an annual basis. Risks that are identified are formally documented for management review.
15.	Security personnel utilize a monitoring application for manual reviews to monitor and analyze the production systems for possible or actual security breaches.
	Antivirus
16.	A central antivirus server is configured to manage antivirus software clients installed on production servers.
17.	The central antivirus server software is configured to check for updates to antivirus definitions and distribute updates to registered clients on a daily basis.

Control No.	Control Activity Implemented by the Application Service Provider
18.	The central antivirus server software is configured to perform a full scan on managed desktops and servers on a weekly basis.
	Intrusion Detection and Prevention
19.	Internal personnel utilize an intrusion detection and prevention system to analyze network events and report possible or actual network security breaches.
20.	The intrusion detection and prevention system is configured to alert IT security personnel of network events.
	Enterprise Monitoring
21.	An enterprise monitoring application is utilized to monitor the performance and availability of production servers.
22.	The enterprise monitoring application generates on screen alert notifications of monitored production servers.
23.	The enterprise monitoring application sends alert notifications to operations personnel via e-mail when predefined thresholds are exceeded on monitored production servers.
	Security Advisory
24.	Management is periodically advised on information security regulatory and industry changes affecting services provided.
25.	Periodic security advisory alerts from industry resources regarding information security are provided to internal personnel for review.
	Logical Access
26.	Domain administration privileges are restricted to user accounts accessible authorized personnel (9).
27.	Operating system administration privileges are restricted to user accounts accessible by authorized personnel (6).
28.	Administration privileges to the application are restricted to user accounts accessible by authorized personnel (6).

PHYSICAL SECURITY

Control No.	Control Activity Implemented by the Application Service Provider
	Policies and Procedures
1.	Policies and procedures are in place to govern the issuance and maintenance of physical access privileges.
	Physical Access
2.	Access privileges to the data center are restricted to badge access cards assigned to authorized personnel (79).
3.	Badge access card access rights are restricted to predefined access groups.
4.	Badge access system administration privileges are restricted to shared and individual user accounts accessible by authorized personnel (2).

Control No.	Control Activity Implemented by the Application Service Provider
5.	The badge access system logs both successful and unsuccessful access attempts. Access attempts are traceable to specific badge access cards.
6.	Corporate and third party security personnel monitor the corporate facility ingress and egress points, including elevators, service elevators and stairwells utilizing a closed circuit video monitoring system.
7.	Corporate and third party security personnel monitor the data center utilizing a closed circuit video monitoring system.
8.	Logs of surveillance recordings from the closed circuit video monitoring system are retained for 30 days.
9.	Visitors are required to sign a visitors log at the reception desk upon entrance to the corporate facility.
10.	Visitors are required to wear visitor badges while within the corporate facility.
11.	Visitors are required to be escorted by an authorized employee when accessing the data center.
12.	Data center visitors are required to sign a visitors log before being granted access to the data center.