Reporting on a Pharmacy Management Application or an Electronic Prescription Application Used for Electronically Prescribing Controlled Substances

The AICPA has developed illustrative reports to assist CPAs in reporting on

- whether a pharmacy management application (PMA) or an electronic prescription application (EPA) for electronically prescribing controlled substances meets the criteria established by the Drug Enforcement Administration of the U.S. Department of Justice set forth in the *Code of Federal Regulations* Title 21, *Food and Drugs*, Parts 1300, 1304, 1306, and 1311, "Electronic Prescriptions for Controlled Substances; Final Rule," and
- whether an entity's controls over the processing integrity and security of the PMA or EPA were operating effectively during the period covered by the report to meet the criteria for processing integrity and security included in TSP section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Technical Practice Aids*).

This engagement is performed under AT section 101, *Attest Engagements* (AICPA, *Professional Standards*), to meet the requirements in Part 1311.300 of the rule requiring that the application provider of an EPA or PMA undergo "a third-party audit of the application" to determine whether it meets specified requirements contained in the rule.

Reporting on a Pharmacy Management Application

Report of Independent Accountants

Board of Directors

XYZ Inc.

We have examined XYZ Inc.'s Pharmacy Management Application (PMA) Release XX.XXXX[1] to determine whether, at September 30, 20X2, the PMA met the criteria applicable to a PMA set forth in the *Code of Federal Regulations* Title 21, *Food and Drugs*, Parts 1300, 1304, 1306, and 1311, "Electronic Prescriptions for Controlled Substances; Final Rule," established by the Drug Enforcement Administration (DEA) of the U.S. Department of Justice (PMA criteria). The PMA criteria are listed in attachment A. Management of XYZ Inc. is responsible for the PMA meeting the PMA criteria. Our responsibility is to express an opinion on whether the PMA met the PMA criteria at September 30, 20X2, based on our examination.

We also have examined the effectiveness of XYZ Inc.'s controls, described in Schedule X, relevant to the processing integrity and security of the PMA during the period October 1, 20X1, through September 30, 20X2, based on the American Institute of Certified Public Accountants (AICPA)-Canadian Institute of Chartered Accountants (CICA) Trust Services Criteria for processing integrity and security. Management of XYZ Inc. is responsible for maintaining the effectiveness of these controls. Our responsibility is to express an opinion on whether management maintained effective controls during the period October 1, 20X1, through September 30, 20X2, based on our examination.

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

To provide additional information about our examination of whether the PMA met the PMA criteria, on page X of our report we have provided a description of certain aspects of the application configuration and IT environment in which we performed our tests of whether the PMA met the PMA criteria. The proper functioning of an application depends on the IT environment in which it operates, such as the physical hardware, system software, and software configuration settings. Because of the dependency of the application on the IT environment, the application may not function as designed in environments other than those in which it was developed or tested.[2] The proper functioning of the PMA also depends on the proper execution of the application and functioning of the IT environment. Furthermore, the projection of any conclusions, based on our findings, to other releases of the application is subject to the risk that the validity of such conclusions may be altered because of changes made to the application in other releases.

---

[1] When reporting on a single instance of installed software rather than a release for use by multiple customers, insert the words "installed at XYZ in the IT environment described on page X of this report."

[2] When reporting on a single instance of installed software rather than a release for use by multiple customers, delete this sentence and replace it with "Because of the dependency of the application on the IT environment, the application may not function as designed due to changes in the IT environment or the failure to make needed changes."

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

In our opinion, as of September 30, 20XX, the PMA met the PMA criteria, in all material respects. Also, in our opinion, XYZ Inc. maintained, in all material respects, effective controls over the processing integrity and security of the PMA to provide reasonable assurance that

- the PMA was protected against unauthorized access (both physical and logical) and
- the system processing was complete, accurate, timely, and authorized during the period October 1, 20X1, through September 30, 20X2,

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

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

October 31, 20X2

Description of Certain Aspects of the Application Configuration and IT Environment in Which Example CPA Firm Tested the XYZ Pharmacy Management Application Release XX.XXXX[3]

Report of Independent Accountants

Application Configuration

For testing, XYZ Pharmacy Management Application (PMA) Release XX.XXXX was configured as recommended by XYZ Inc., which included the following:

- Integrated ABC Cryptographic Module Release 2.5 installed
- "Role-based Security Enabled" = yes
- "Digital Signature Checking" = yes

IT Environment

Application testing procedures were performed using an IT environment provided by XYZ, which included the following components:

- Application server running on Windows x64 Service Pack 2
- Oracle Database 10*g* Release 2 running on a dedicated database server using Red Hat Enterprise Linux Server 6 for IBM Power
- Authentication to the application via two-factor authentication using RSA SecurID Token 4.1 for Microsoft Windows
- Internet Explorer 8 browser (release 8.0.6001.18702)
- Cisco ASA 5520 firewall running ASA OS 8.4 (external firewall restricting access to necessary ports)
- Cisco ASA 5520 firewall running ASA OS 8.4 (internal/DMZ firewall restricting access between database, middleware, external, and Web server zones)
- Big-IP application security manager application firewall running on 3900 series hardware

---

[3] The description of the IT environment would typically include, at a minimum, a list of the relevant application software in use (and middleware, as applicable), including the release number or name; the databases supporting the application functions, with release levels; the operating systems supporting the application software and databases, including the release number or name; and the hardware or desktop configurations (including browsers and virus software, as applicable) and related network architecture(s) used within the environment.

The description of the IT environment should also include the security mechanisms in use for the applications (for example, biometric authentication, and third-party certification authorities), the databases, operating systems, and networks. For data in transit or at rest, the description of the IT environment should include the data flows between all of the application components. The description may also include other elements, such as a list of the external inputs to the environment and outputs from the environment, as well as any related transmission protocols and security mechanisms. These external inputs should include any access or dependencies from other applications or systems that are received and processed by the application. For example, this could be in the form of a Web service call from a third-party application using the Application Programming Interface (API) to communicate information that is received and processed by the application.

Additionally the application's supporting components and infrastructure should be accounted for. Supporting components might include but are not limited to logging servers, SSL accelerators, reverse proxies, load balancers, and authentication servers (such as biometric or token servers) that the application and its environment depend upon. Other types of supporting infrastructure include the network and security devices that facilitate and protect communication within and external to the application environment. These devices might include routers and switches with associated access control lists and VLANs, network firewalls, Web application firewalls, or any other devices that encompass the application and its operating environment.

Attachment A — Pharmacy Management Application Criteria

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

§ 1311.205(b) Pharmacy application requirements.

The pharmacy application meets the following requirements:

(1) The pharmacy application is capable of setting logical access controls to limit access for the following functions:

(i) Annotation, alteration, or deletion of prescription information.

(ii) Setting and changing the logical access controls.

(2) Logical access controls are set by individual user name or role.

(3) The pharmacy application digitally signs and archives a prescription on receipt or be capable of receiving and archiving a digitally signed record.

(4) For pharmacy applications that digitally sign prescription records upon receipt, the digital signature functionality meets the following requirements:

(i) The cryptographic module used to digitally sign the data elements required by part 1306 of this chapter is at least FIPS 140-2[1] Security Level 1 validated.

(ii) The digital signature application and hash function complies with FIPS 186-3[2] and FIPS 180-3.[3]

(iii) The pharmacy application's private key is stored encrypted on a FIPS 140-2 Security Level 1 or higher validated cryptographic module using a FIPS-approved encryption algorithm.

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

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

(5) The pharmacy application verifies a practitioner's digital signature (if the pharmacy application accepts prescriptions that were digitally signed with an individual practitioner's private key and transmitted with the digital signature).

(6) If the prescription received by the pharmacy application has not been digitally signed by the practitioner and transmitted with the digital signature, the pharmacy application either:

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

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

(7) The pharmacy application reads and retains the full DEA number including the specific internal code number assigned to individual practitioners authorized to prescribe

---

[1] Federal Information Processing Standards (FIPS) are incorporated in the rule by reference in Section 1311.08.

[2] See footnote 1.

[3] See footnote 1.

controlled substances by the hospital or other institution, as provided in § 1301.22(c) of this chapter.

(8) The pharmacy application reads and stores, and is capable of displaying, all information required by part 1306 of this chapter.

(9) The pharmacy application reads and stores in full the information required under § 1306.05(a)[4] of this chapter. The pharmacy application either verifies that such information is present or displays the information for the pharmacist's verification.

(10) The pharmacy application provides for the following information to be added or linked to each electronic controlled substance prescription record for each dispensing:

(i) Number of units or volume of drug dispensed.

(ii) Date dispensed.

(iii) Name or initials of the person who dispensed the prescription.

(11) The pharmacy application is capable of retrieving controlled substance prescriptions by practitioner name, patient name, drug name, and date dispensed.

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

(13) The pharmacy application maintains an audit trail of all actions related to the following:

(i) The receipt, annotation, alteration, or deletion of a controlled substance prescription.

(ii) Any setting or changing of logical access control permissions related to the dispensing of controlled substance prescriptions.

(iii) Auditable events as specified in § 1311.215.

(14) The pharmacy application records within each audit record the following information:

(i) The date and time of the event.

(ii) The type of event.

(iii) The identity of the person taking the action, where applicable.

(iv) The outcome of the event (success or failure).

(15) The pharmacy application conducts internal audits and generates reports on any of the events specified in § 1311.215 in a format that is readable by the pharmacist. Such an internal audit may be automated and need not require human intervention to be conducted.

(16) The pharmacy application protects the stored audit records from unauthorized deletion. The pharmacy application shall prevent modifications to the audit records.

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

(18) The pharmacy application retains all archived records electronically for at least two years from the date of their receipt or creation and comply with all other requirements of § 1311.305

[4] **§ 1306.05 Manner of issuance of prescriptions.**

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

§ 1311.210 Archiving the initial record.

(a) Except as provided in paragraph (c) of this section, a copy of each electronic controlled substance prescription record that a pharmacy receives is digitally signed by one of the following:

(1) The last intermediary transmitting the record to the pharmacy immediately prior to transmission to the pharmacy.

(2) The first pharmacy application that receives the electronic prescription immediately upon receipt.

(b) If the last intermediary digitally signs the record, it forwards the digitally signed copy to the pharmacy.

(c) If a pharmacy receives a digitally signed prescription that includes the individual practitioner's digital signature, the pharmacy application:

(1) Verifies the digital signature as provided in FIPS 186–3, as incorporated by reference in § 1311.08.

(2) Checks the validity of the certificate holder's digital certificate by checking the certificate revocation list. The pharmacy may cache the CRL until it expires.

(3) Archives the digitally signed record. The pharmacy record retains an indication that the prescription was verified upon receipt. No additional digital signature is required.

§ 1311.215 Internal audit trail.

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

(1) Attempted unauthorized access to the pharmacy application, or successful unauthorized access to the pharmacy application where the determination of such is feasible.

(2) Attempted or successful unauthorized modification or destruction of any information or records required by this part, or successful unauthorized modification or destruction of any information or records required by this part where the determination of such is feasible.

(3) Interference with application operations of the pharmacy application.

(4) Any setting of or change to logical access controls related to the dispensing of controlled substance prescriptions.

(5) Attempted or successful interference with audit trail functions.

(6) For application service providers, attempted or successful annotation, alteration, or destruction of controlled substance prescriptions or logical access controls related to controlled substance prescriptions by any agent or employee of the application service provider.

(b) The pharmacy application analyzes the audit trail at least once every calendar day and generates an incident report that identifies each auditable event.

* * * * *

§ 1311.305 Recordkeeping.

(a) If a prescription is created, signed, transmitted, and received electronically, all records related to that prescription are retained electronically.

(b) Records required by this subpart are maintained electronically for two years from the date of their creation or receipt. This record retention requirement shall not pre-empt any longer

period of retention which may be required now or in the future, by any other Federal or State law or regulation, applicable to practitioners, pharmacists, or pharmacies.

(c) Records regarding controlled substances prescriptions are readily retrievable from all other records. Electronic records are easily readable or easily rendered into a format that a person can read.

* * * * *

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

* * * * *

(f) If the electronic prescription is transmitted without the digital signature, the electronic prescription application checks the certificate revocation list of the certification authority that issued the practitioner's digital certificate. If the digital certificate is not valid, the electronic prescription application does not transmit the prescription. The certificate revocation list may be cached until the certification authority issues a new certificate revocation list.

(g) When the individual practitioner digitally signs a controlled substance prescription with the private key associated with his own digital certificate obtained as provided under § 1311.105, the electronic prescription application is not required to digitally sign the prescription using the application's private key.

Reporting on an Electronic Prescription Application

Report of Independent Accountants

Board of Directors

XYZ Inc.

We have examined XYZ Inc.'s Electronic Prescription Application (EPA) Release XX.XXXX[1] to determine whether, at September 30, 20X2, the EPA met the criteria applicable to EPA set forth in the *Code of Federal Regulations* Title 21, *Food and Drugs*, Parts 1300, 1304, 1306, and 1311, "Electronic Prescriptions for Controlled Substances; Final Rule," established by the Drug Enforcement Administration (DEA) of the U.S. Department of Justice (EPA criteria). The EPA criteria are listed in attachment A. Management of XYZ Inc. is responsible for the EPA meeting the EPA criteria. Our responsibility is to express an opinion on whether the EPA met the EPA criteria at September 30, 20X2, based on our examination.

We also have examined the effectiveness of XYZ Inc.'s controls, described in Schedule X, relevant to the processing integrity and security of the EPA during the period October 1, 20X1, through September 30, 20X2, based on the American Institute of Certified Public Accountants (AICPA)-Canadian Institute of Chartered Accountants (CICA) Trust Services Criteria for processing integrity and security. Management of XYZ Inc. is responsible for maintaining the effectiveness of these controls. Our responsibility is to express an opinion on whether management maintained effective controls during the period October 1, 20X1, through September 30, 20X2, based on our examination.

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

To provide additional information about our examination of whether the EPA met the EPA criteria, on page X of our report we have provided a description of certain aspects of the application configuration and IT environment in which we performed our tests of whether the EPA met the EPA criteria. The proper functioning of an application depends on the IT environment in which it operates, such as the physical hardware, system software, and software configuration settings. Because of the dependency of the application on the IT environment, the application may not function as designed in environments other than those in which it was developed or tested.[2] The proper functioning of the EPA also depends on the proper execution of the application and functioning of the IT environment. Furthermore, the projection of any conclusions, based on our findings, to other releases of the application is subject to the risk that the validity of such conclusions may be altered because of changes made to the application in other releases.

Because of the nature and inherent limitations of controls, XYZ Inc.'s ability to meet the AICPA-CICA Trust Services Criteria for processing integrity and security may be affected. For example, controls may not prevent or detect and correct error or fraud, unauthorized access to systems and

---

[1] When reporting on a single instance of installed software rather than a release for use by multiple customers, insert the words "installed at XYZ in the IT environment described on page X of this report."

[2] When reporting on a single instance of installed software rather than a release for use by multiple customers, delete this sentence and replace it with "Because of the dependency of the application on the IT environment, the application may not function as designed due to changes in the IT environment or the failure to make needed changes."

information, and failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

In our opinion, as of September 30, 20XX, the EPA met the EPA criteria, in all material respects.

Also, in our opinion, XYZ Inc. maintained, in all material respects, effective controls over the processing integrity and security of the EPA to provide reasonable assurance that

- the EPA was protected against unauthorized access (both physical and logical) and
- the system processing was complete, accurate, timely, and authorized during the period October 1, 20X1, through September 30, 20X2,

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

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

October 31, 20X2

Description of Certain Aspects of the Application Configuration and IT Environment in Which Example CPA Firm Tested the Electronic Prescription Application Release XX.XXXX[3]

Report of Independent Accountants

Application Configuration

For testing, XYZ Electronic Prescription Application (EPA) Release XX.XXXX was configured as recommended by XYZ Inc., which included the following:

- Integrated ABC Cryptographic Module Release 2.5 installed
- "Role-based Security Enabled" = yes
- "Digital Signature Checking" = yes

IT Environment

Application testing procedures were performed using an IT environment provided by XYZ, which included the following components:

- Application server running Windows x64 Service Pack 2
- Oracle Database 10*g* Release 2 running on a dedicated database server using Red Hat Enterprise Linux Server 6 for IBM Power
- Authentication to the application via two-factor authentication using RSA SecurID Token 4.1 for Microsoft Windows
- Internet Explorer 8 browser (release 8.0.6001.18702)
- Cisco ASA 5520 firewall running ASA OS 8.4 (external firewall restricting access to necessary ports)
- Cisco ASA 5520 firewall running ASA OS 8.4 (internal/DMZ firewall restricting access between database, middleware, external, and Web server zones)
- Big-IP application security manager application firewall running on 3900 series hardware

[3] The description of the IT environment would typically include, at a minimum, a list of the relevant application software in use (and middleware, as applicable), including the release number or name; the databases supporting the application functions, including the release levels; the operating systems supporting the application software and databases, including the release number or name; and the hardware or desktop configurations (including browsers and virus software, as applicable) and related network architecture(s) used within the environment.

The description of the IT environment should also include the security mechanisms in use for the applications (for example, biometric authentication, and third-party certification authorities), the databases, operating systems, and networks. For data in transit or at rest, the description of the IT environment should include the data flows between all of the application components. The description may also include other elements, such as a list of the external inputs to the environment and outputs from the environment, as well as any related transmission protocols and security mechanisms. These external inputs should include any access or dependencies from other applications or systems that are received and processed by the application. For example, this could be in the form of a Web service call from a third-party application using the Application Programming Interface (API) to communicate information that is received and processed by the application.

Additionally the application's supporting components and infrastructure should be accounted for. Supporting components might include, but are not limited to, logging servers, SSL accelerators, reverse proxies, load balancers, and authentication servers (such as biometric or token servers) that the application and its environment depend on. Other types of supporting infrastructure include the network and security devices that facilitate and protect communication within and external to the application environment. These devices might include routers and switches with associated access control lists and VLANs, network firewalls, Web application firewalls, or any other devices that encompass the application and its operating environment.

Attachment A — Electronic Prescription Application Criteria

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

§ 1311.120(b) Electronic prescription application requirements.

The electronic prescription application meets the requirements of this subpart including the following:

(1) The electronic prescription application does the following:

(i) Link each registrant, by name, to at least one DEA registration number.

(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.

(2) The electronic prescription application is capable of the setting of logical access controls to limit permissions for the following functions:

(i) Indication that a prescription is ready for signing and signing controlled substance prescriptions.

(ii) Creating, updating, and executing the logical access controls for the functions specified in paragraph (b)(2)(i) of this section.

(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.

(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.

(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.

(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.

(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.

(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.

(9) The electronic prescription application presents for the practitioner's review and approval all of the following data for each controlled substance prescription:

(i) The date of issuance.

(ii) The full name of the patient.

(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) 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.

(vii) The name, address, and DEA registration number of the prescribing practitioner.

(viii) The statement required under § 1311.140(a)(3).

(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.

(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.

(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.

(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).

(14) The electronic prescription application time and date stamps the prescription when the signing function is used.

(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.

(16) The digital signature functionality meets the following requirements:

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

[1] Federal Information Processing Standards (FIPS) are incorporated in the rule by reference in Section 1311.08.

(ii) The digital signature application and hash function complies with FIPS 186-3 and FIPS 180-3,[2] as incorporated by reference in § 1311.08.

(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 140-2[3] is incorporated by reference in § 1311.08.

(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.

(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.

(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.

(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.

(20) The electronic prescription application does not allow transmission of a prescription that has been printed.

(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.

(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.

(23) The electronic prescription application maintains an audit trail of all actions related to the following:

(i) The creation, alteration, indication of readiness for signing, signing, transmission, or deletion of a controlled substance prescription.

(ii) Any setting or changing of logical access control permissions related to the issuance of controlled substance prescriptions.

(iii) Notification of a failed transmission.

(iv) Auditable events as specified in § 1311.150.

(24) The electronic prescription application records within each audit record the following information:

(i) The date and time of the event.

(ii) The type of event.

[2] See footnote 1.

[3] See footnote 1.

(iii) The identity of the person taking the action, where applicable.

(iv) The outcome of the event (success or failure).

(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.

(26) The electronic prescription application protects the stored audit records from unauthorized deletion. The electronic prescription application shall prevent modifications to the audit records.

(27) The electronic prescription application does the following:

(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.

(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.

(iii) Archive all logs generated.

(iv) Ensure that all logs are easily readable or easily rendered into a format that a person can read.

(v) Ensure that all logs are sortable by patient name, drug name, and date of issuance of the prescription.

(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.

§ 1311.125 Requirements for establishing logical access control—Individual practitioner.

(a) At each registered location where one or more individual practitioners wish to use an electronic prescription application meeting the requirements of this subpart to issue controlled substance prescriptions, the registrant(s) designates at least two individuals to manage access control to the application. At least one of the designated individuals is a registrant who is authorized to issue controlled substance prescriptions and who has obtained a two- factor authentication credential as provided in § 1311.105.

(b) At least one of the individuals designated under paragraph (a) of this sectionverifies that the DEA registration and State authorization(s) to practice and, where applicable, State authorization(s) to dispense controlled substances of each registrant being granted permission to sign electronic prescriptions for controlled substances are current and in good standing.

(c) After one individual designated under paragraph (a) of this section enters data that grants permission for individual practitioners to have access to the prescription functions that indicate readiness for signature and signing or revokes such authorization, a second individual designated under paragraph (a) of this section uses his two-factor authentication credential to satisfy the logical access controls. The second individual is a DEA registrant.

* * * * *

§ 1311.130 Requirements for establishing logical access control—Institutional practitioner.

(a) The entity within an institutional practitioner that conducts the identity proofing under § 1311.110 develops a list of individual practitioners who are permitted to use the institutional practitioner's electronic prescription application to indicate that controlled

substances prescriptions are ready to be signed and to sign controlled substance prescriptions. The list is approved by two individuals.

(b) After the list is approved, it is sent to a separate entity within the institutional practitioner that enters permissions for logical access controls into the application. The institutional practitioner authorizes at least two individuals or a role filled by at least two individuals to enter the logical access control data. One individual in the separate entity authenticates to the application and enter the data to grant permissions to individual practitioners to indicate that controlled substances prescriptions are ready to be signed and to sign controlled substance prescriptions. A second individual authenticates to the application to execute the logical access controls.

* * * * *

§ 1311.135 Requirements for creating a controlled substance prescription.

(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.

(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.

(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.

§ 1311.140 Requirements for signing a controlled substance prescription.

(a) For a practitioner to sign an electronic prescription for a controlled substance the following occurs:

(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).

(2) The practitioner indicates the prescriptions that are ready to be signed.

(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.''

(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.

(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.

(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.

(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.

(c) Any prescription not signed in the manner required by this section shall not be transmitted.

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

(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.

(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.

(c) The electronic prescription application digitally signs at least all information required under part 1306 of this chapter.

(d) The electronic prescription application electronically archives the digitally signed record.

(e) A prescription that is digitally signed with a practitioner's private key may be transmitted to a pharmacy without the digital signature.

(f) If the electronic prescription is transmitted without the digital signature, the electronic prescription application checks the certificate revocation list of the certification authority that issued the practitioner's digital certificate. If the digital certificate is not valid, the electronic prescription application does not transmit the prescription. The certificate revocation list may be cached until the certification authority issues a new certificate revocation list.

(g) When the individual practitioner digitally signs a controlled substance prescription with the private key associated with his own digital certificate obtained as provided under § 1311.105, the electronic prescription application is not required to digitally sign the prescription using the application's private key.

§ 1311.150 Additional requirements for internal application audits.

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

(1) Attempted unauthorized access to the electronic prescription application, or successful unauthorized access where the determination of such is feasible.

(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.

(3) Interference with application operations of the prescription application.

(4) Any setting of or change to logical access controls related to the issuance of controlled substance prescriptions.

(5) Attempted or successful interference with audit trail functions.

(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.

(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.

* * * * *

§ 1311.170 Transmission requirements.

(a) The electronic prescription application transmits the electronic prescription as soon as possible after signature by the practitioner.

(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.

(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.

(d) The electronic prescription application does not allow the transmission of an electronic prescription if an original prescription was printed prior to attempted transmission.

(e) The contents of the prescription required by part 1306 of this chapter is not altered during transmission between the practitioner and pharmacy. Any change to the content during transmission, including truncation or removal of data, will render the electronic prescription invalid. The electronic prescription data may be converted from one software version to another between the electronic prescription application and the pharmacy application; conversion includes altering the structure of fields or machine language so that the receiving pharmacy application can read the prescription and import the data.

(f) An electronic prescription is transmitted from the practitioner to the pharmacy in its electronic form. At no time may an intermediary convert an electronic prescription to another form (e.g., facsimile) for transmission.

§ 1311.305 Recordkeeping.

(a) If a prescription is created, signed, transmitted, and received electronically, all records related to that prescription are retained electronically.

(b) Records required by this subpart are maintained electronically for two years from the date of their creation or receipt. This record retention requirement shall not pre-empt any longer period of retention which may be required now or in the future, by any other Federal or State law or regulation, applicable to practitioners, pharmacists, or pharmacies.

(c) Records regarding controlled substances prescriptions are readily retrievable from all other records. Electronic records are easily readable or easily rendered into a format that a person can read.

(d) Records required by this part are made available to the Administration upon request.

* * * * *

§ 1306.05 Manner of issuance of prescriptions.

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

(b) A prescription for a Schedule III, IV, or V narcotic drug approved by FDA specifically for ''detoxification treatment'' or ''maintenance treatment'' includes the identification number issued by the Administrator under § 1301.28 (d) of this chapter or a written notice stating that the practitioner is acting under the good faith exception of § 1301.28 (e) of this chapter.

(c) Where a prescription is for gammahydroxybutyric acid, the practitioner shall note on the face of the prescription the medical need of the patient for the prescription.

* * * * *

(g) An individual practitioner exempted from registration under § 1301.22 (c) of this chapter shall include on all prescriptions issued by him the registration number of the hospital or other institution and the special internal code number assigned to him by the hospital or other institution as provided in § 1301.22 (c) of this chapter, in lieu of the registration number of the practitioner required by this section.

* * * * *

(h) An official exempted from registration under § 1301.23 (a) of this chapter includes on all prescriptions issued by him his branch of service or agency (e.g., ''U.S. Army'' or ''Public Health Service'') and his service identification number, in lieu of the registration number of the practitioner required by this section. The service identification number for a Public Health Service employee is his Social Security identification number.

* * * * *

§ 1311.115 Additional requirements for two-factor authentication.

(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:

(1) Something only the practitioner knows, such as a password or response to a challenge question.

(2) Something the practitioner is, biometric data such as a fingerprint or iris scan.

(3) Something the practitioner has, a device (hard token) separate from the computer to which the practitioner is gaining access.

(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.

(c) If one factor is a biometric, the biometric subsystem complies with the requirements of § 1311.116.

§ 1311.116 Additional requirements for biometrics.

(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.

(b) The biometric subsystem operates at a false match rate of 0.001 or lower.

(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.

(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.

(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.

(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.

(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:

(1) Cryptographically source authenticated;

(2) Combined with a random challenge, a nonce, or a time stamp to prevent replay;

(3) Cryptographically protected for integrity and confidentiality; and

(4) Sent only to authorized systems.

(h) Testing of the biometric subsystem has the following characteristics:

(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.

(2) Test data are sequestered.

(3) Algorithms are provided to the testing laboratory (as opposed to scores or other information).

(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.

(5) Results of the testing are made publicly available.

DISCLAIMER: This publication has not been approved, disapproved or otherwise acted upon by any senior technical committees of, and does not represent an official position of, the American Institute of Certified Public Accountants. It is distributed with the understanding that the contributing authors and editors, and the publisher, are not rendering legal, accounting, or other professional services in this publication. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

Copyright © 2012 by American Institute of Certified Public Accountants, Inc. New York, NY 10036-8775. All rights reserved. For information about the procedure for requesting permission to make copies of any part of this work, please email copyright@aicpa.org with your request. Otherwise, requests should be written and mailed to the Permissions Department, AICPA, 220 Leigh Farm Road, Durham, NC 27707-8110.