OMC
ORGANIZACIÓN MÉDICA COLEGIAL DE ESPAÑA | CONSEJO GENERAL DE COLEGIOS OFICIALES DE MEDICOS

Plaza de las Cortes, 11
28014 Madrid
Tel. +34 914 317 780
cgcom@cgcom.es
www.cgcom.es

Requerimientos para la auditoría de certificación del sistema de receta médica privada electrónica

CGCOM
Septiembre de 2017

Índice

1. Introducción

En este documento se presentan los requerimientos relacionados con el proceso de auditoría de certificación del sistema de receta médica privada electrónica.

El documento contiene los objetivos de control que deben cumplir los sistemas de receta médica privada electrónica candidatos a la certificación por el organismo de certificación, y los criterios para la auditoría.

Los objetivos de control se han agrupado en las siguientes categorías:

- Controles funcionales y técnicos.
- Controles de formalización documental.
- Controles de interoperabilidad.
- Controles de protección de datos de carácter personal.
- Controles de seguridad y confidencialidad.

Por su parte, los criterios desarrollan los anteriores objetivos de control, indicando:

- Una descripción detallada del control, incluyendo, en su caso, descripción de mejores prácticas para el cumplimiento del control.
- La documentación acreditativa a presentar en la justificación del cumplimiento.
- El contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles.

2. Objetivos de control de los sistemas de receta médica privada electrónica

2.1. Controles funcionales y técnicos

Esta sección identifica los controles funcionales y técnicos mínimos aplicables a sistemas de receta médica privada electrónica.

FT01	Posibilidad de prescribir, en cada receta electrónica, uno o varios medicamentos y productos sanitarios.
FT02	Generación de la relación de medicamentos y productos sanitarios prescritos al paciente.
FT03	Posibilidad de establecer un plan terapéutico en soporte de la prescripción, en base a intervalos de tratamiento

	definidos no superiores a un año.
FT04	Control de la periodicidad de la dispensación, en prescripción en base a plan terapéutico a intervalos definidos.
FT05	Medidas de control en relación con la prescripción de medicamentes estupefacientes.
FT06	Verificación, cuando resulte procedente, del aseguramiento privado del paciente, y registro de dicha información, para su posterior uso en el acceso a la historia.
FT07	Seguimiento de las dispensaciones del tratamiento prescrito, con posibilidad de su modificación o anulación, atendiendo a cualquier evento o circunstancia sobrevenida en la situación clínica del paciente, así como a criterios de cumplimiento terapéutico, que deberán ser registradas.
FT08	Mecanismos de protección y confidencialidad del paciente en la dispensación de los tratamientos, cuando el mismo lo solicite.
FT09	Posibilidad de realizar la impresión de la hoja de información al paciente y/o de medicación activa, en función de las características del sistema implantado.
FT10	Posibilidad de remisión telemática de la hoja de información al paciente y/o de medicación activa, al menos para los pacientes con discapacidades que imposibilite o dificulte el acceso a los mismos.

2.2. Controles de formalización documental

Esta sección identifica los controles mínimos de formalización documental aplicables a los sistemas de receta médica privada electrónica.

• FD01	• Emisión de la receta en soporte electrónico, con los datos básicos obligatorios, relativos a paciente, medicamento, prescriptor y fecha de prescripción. En su caso, el visado por la Administración sanitaria correspondiente. • Inclusión del código o número de identificación de la

	prescripción de cada medicamento y producto sanitario, asignado por el sistema electrónico con carácter único e irrepetible; y de la información de la relación activa de medicamentos correspondiente a los tratamientos en curso.
• FD02	• Firma electrónica avanzada basada en certificado electrónico cualificado de la receta electrónica, en su caso empleando el carné oficial del Colegio de Médicos correspondiente, y de acuerdo con las reglas de la política de firma electrónica publicada por el CGCOM.
• FD03	• Emisión y entrega de hoja de información al paciente, en soporte papel, que recogerá los datos básicos obligatorios de la receta, así como información del tratamiento necesaria para facilitar el uso adecuado de los medicamentos o productos sanitarios prescritos.

2.3. Controles de interoperabilidad.

Esta sección identifica los controles mínimos en relación con la interoperabilidad de los sistemas de receta médica privada electrónica con otros agentes y sistemas.

• IN01	• Normas de interconexión de sistemas de receta médica electrónica privada entre los diferentes agentes funcionales (prescriptor, dispensador, etc).
• IN02	• Consumo de servicios de autenticación delegada, en caso de sistemas basados en federación de identidad médica (SINCERT).
• IN03	• Verificación interoperable de certificados de médico colegiado y de pacientes, incluyendo DNI electrónico y otros certificados electrónicos de firma reconocida.
• IN04	• Modelos de datos para el acceso al sistema de receta médica privada del prescriptor.
• IN05	• Empleo del esquema de intercambio de recetas médicas privadas electrónicas.
• IN06	• Modelo de integración de las recetas en la historia clínica del paciente.
• IN07	• En su caso, cumplimiento de las normas de

	interoperabilidad aplicables al procedimiento electrónico de visado por la Administración sanitaria correspondiente.

2.4. Controles de protección de datos de carácter personal

Esta sección identifica los controles mínimos a aplicar en relación con los datos de carácter personal gestionados por los sistemas de receta médica privada electrónica.

• PD01	• Existencia de cláusula de información de protección de datos personales en la hoja de información al paciente.
• PD02	• Cumplimiento de todas las medidas de seguridad de ficheros de datos personales de nivel alto, previstas en el reglamento de desarrollo de la ley reguladora.

2.5. Controles de seguridad y confidencialidad

Esta sección identifica los controles mínimos referidos a la seguridad y confidencialidad de los sistemas de receta médica privada electrónica, adicionales a las medidas de seguridad de datos de carácter personal.

• SC01	• Acceso al sistema de receta médica electrónica mediante certificado electrónico cualificado y de acuerdo con las reglas de la política de autenticación electrónica, publicada por el CGCOM.
• SC02	• Acceso al sistema de receta médica electrónica mediante DNI electrónico del paciente, o certificado cualificado que contenga el NIF del paciente y, en su caso, la condición de aseguramiento privado del mismo. • En caso de imposibilidad, acceso a través del DNI del paciente o, en su caso, del padre o tutor.
• SC03	• Integración del equipo de acceso en el sistema de receta electrónica, con autenticación de equipo y comunicaciones cifradas, de acuerdo con las correspondientes políticas de seguridad de comunicaciones electrónicas publicadas por el CGCOM.
• SC04	• Controles de custodia y conservación segura, tanto de los datos del sistema de receta médica privada

	electrónica (base de datos), como de las recetas electrónicas formalizadas documentalmente (firmadas electrónicamente).
• SC05	• Controles de disponibilidad 24x7x365 del sistema de receta médica privada electrónica, en soporte de los servicios de urgencias.

3. Criterios de auditoría

3.1. Controles funcionales y técnicos

3.1.1. [FT01] Posibilidad de prescribir, en cada receta electrónica, uno o varios medicamentos y productos sanitarios

Descripción detallada del control:

En este control se revisa el cumplimiento de esta posibilidad prevista en el artículo 14.1 del RD 1718/2010, en virtud del cual "en la receta médica privada electrónica se podrá prescribir uno o varios medicamentos y productos sanitarios [...]".

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Descripción del funcional de la aplicación referido a la prescripción.
- Modelos-tipo de recetas electrónicas.
- Ejemplos reales de recetas electrónicas con múltiples medicamentos.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: el funcional de la aplicación considera casos de uso y procedimientos para la expedición de recetas electrónicas con múltiples medicamentos o productos sanitarios.
- Revisión documental: el modelo-tipo de receta electrónica dispone de espacio que permita la incorporación de diversos medicamentos o productos sanitarios.
- Revisión documental: existen ejemplos reales de receta electrónica con múltiples medicamentos.

- Revisión técnica: se expide una receta electrónica de prueba al auditor, con múltiples medicamentos o productos sanitarios, y se verifica la documentación resultante.

3.1.2. [FT02] Generación de la relación de medicamentos y productos sanitarios prescritos al paciente

Descripción detallada del control:

En este control se revisa el cumplimiento de la obligación1 contenida en el artículo 8.2 del RD 1718/2010, en virtud de la cual "el sistema de receta médica electrónica generará la relación de medicamentos y productos sanitarios prescritos al paciente y deberá incluir, además de los datos de consignación obligatoria que se especifican en el artículo 3, los siguientes:

a) Código o número de identificación de la prescripción de cada medicamento y producto sanitario, que será asignado por el sistema electrónico con carácter único e irrepetible.
b) Información de la relación activa de medicamentos correspondiente a los tratamientos en curso".

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Descripción del funcional de la aplicación referido a la prescripción.
- Modelos de datos correspondientes a la aplicación de prescripción.
- Ejemplos reales de recetas electrónicas con su correspondiente relación de medicamentos y productos sanitarios.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: el funcional de la aplicación considera casos de uso y procedimientos para la generación de la relación de medicamentos y productos sanitarios prescritos al paciente.
- Revisión documental: existen ejemplos reales de receta electrónica con sus correspondientes relaciones de medicamentos y productos sanitarios.
- Revisión técnica: se expide una receta electrónica de prueba al auditor, con múltiples medicamentos o productos sanitarios, y se verifica la documentación resultante en el sistema.

[1] El artículo 8 del RD 1718/2010 resulta aplicable a la prescripción de la receta médica privada electrónica en virtud de lo establecido por el artículo 14.2 del propio RD 1718/2010.

3.1.3. [FT03] Plan terapéutico en soporte de la prescripción

Descripción detallada del control:

En este control se revisa el cumplimiento de la obligación[2] contenida en el artículo 8.3 del RD 1718/2010, en virtud de la cual "los medicamentos y productos sanitarios serán prescritos según el plan terapéutico establecido [...]".

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Descripción del funcional de la aplicación referido a la prescripción.
- Modelos de datos correspondientes a la aplicación de prescripción.
- Ejemplos reales de planes terapéuticos.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: el funcional de la aplicación considera casos de uso y procedimientos para el establecimiento de planes terapéuticos y sus limitaciones.
- Revisión documental: el modelo de datos permite el establecimiento de controles para implementar las limitaciones establecidas reglamentariamente en relación con el plan terapéutico, en especial en relación con prescripción de medicamentos estupefacientes.
- Revisión documental: existen ejemplos reales de planes terapéuticos con sus correspondientes limitaciones en cuanto a los medicamentos y productos sanitarios prescritos.
- Revisión técnica: se crea un plan terapéutico de prueba al auditor, con múltiples medicamentos o productos sanitarios, y sus correspondientes limitaciones, y se verifica la documentación resultante en el sistema.

3.1.4. [FT04] Control de la periodicidad de la dispensación

Descripción detallada del control:

En este control se revisa el cumplimiento de la obligación[3] contenida en el artículo 8.3 del RD 1718/2010, en virtud de la cual "los medicamentos y productos

[2] El artículo 8 del RD 1718/2010 resulta aplicable a la prescripción de la receta médica privada electrónica en virtud de lo establecido por el artículo 14.2 del propio RD 1718/2010.

[3] El artículo 8 del RD 1718/2010 resulta aplicable a la prescripción de la receta médica privada electrónica en virtud de lo establecido por el artículo 14.2 del propio RD 1718/2010.

sanitarios serán prescritos según el plan terapéutico establecido, en base a intervalos de tratamiento definidos que no podrán ser superiores a un año [...].
No obstante, cada dispensación no podrá superar un mes de duración máxima de tratamiento, salvo que el formato del medicamento o producto sanitario que deba ser dispensado conforme a la prescripción corresponda a un periodo de tratamiento superior según su ficha técnica".

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Descripción del funcional de la aplicación referido a la prescripción.
- Modelos de datos correspondientes a la aplicación de prescripción.
- Ejemplos reales de planes terapéuticos.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: el funcional de la aplicación considera casos de uso y procedimientos para el establecimiento de planes terapéuticos y sus intervalos.
- Revisión documental: el modelo de datos permite el establecimiento de controles para hacer cumplir los intervalos establecidos en el plan terapéutico.
- Revisión documental: existen ejemplos reales de planes terapéuticos con sus correspondientes intervalos en cuanto a los medicamentos y productos sanitarios prescritos.
- Revisión técnica: se crea un plan terapéutico de prueba al auditor, con múltiples medicamentos o productos sanitarios, y sus correspondientes intervalos, y se verifica la documentación resultante en el sistema.

3.1.5. [FT05] Medidas de control en relación con la prescripción de medicamentos estupefacientes

En este control se revisa el cumplimiento de la obligación contenida en el artículo 14.1 del RD 1718/2010, en virtud de la cual "en la receta médica privada electrónica se podrá prescribir uno o varios medicamentos y productos sanitarios, con las limitaciones establecidas reglamentariamente para la prescripción de medicamentos estupefacientes incluidos en la lista I de la Convención Única de 1961 de estupefacientes", obligación[4] también contenida en el artículo 8.3 del RD 1718/2010, en virtud de la cual "los medicamentos y productos sanitarios serán prescritos según el plan terapéutico establecido [...], con las limitaciones establecidas reglamentariamente para la prescripción de medicamentos

[4] El artículo 8 del RD 1718/2010 resulta aplicable a la prescripción de la receta médica privada electrónica en virtud de lo establecido por el artículo 14.2 del propio RD 1718/2010.

estupefacientes incluidos en la lista I de la Convención Única de 1961 de estupefacientes".

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Descripción del funcional de la aplicación referido a la prescripción.
- Modelos de datos correspondientes a la aplicación de prescripción.
- Ejemplos reales de planes terapéuticos con medicamentos estupefacientes.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: el funcional de la aplicación considera casos de uso y procedimientos para el establecimiento de planes terapéuticos y sus limitaciones referidas a estupefacientes.
- Revisión documental: el modelo de datos permite el establecimiento de controles para implementar las limitaciones establecidas reglamentariamente en relación con el plan terapéutico, en especial en relación con prescripción de medicamentos estupefacientes.
- Revisión documental: existen ejemplos reales de planes terapéuticos con sus correspondientes limitaciones en cuanto a los estupefacientes.
- Revisión técnica: se crea un plan terapéutico de prueba al auditor, con medicamentos estupefacientes, y se verifica la documentación resultante en el sistema.

3.1.6. [FT06] Verificación y registro de información del aseguramiento privado del paciente

Descripción detallada del control:

En este control, que es optativo, se revisa el cumplimiento de la posibilidad de verificar, cuando resulte procedente, el aseguramiento privado del paciente, y registro de dicha información para su posterior uso en el acceso a la historia clínica electrónica. El registro de esta información es voluntario por parte del paciente.

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Descripción del funcional de la aplicación referido a la prescripción.
- Modelos de datos correspondientes a la aplicación de prescripción.
- Ejemplos reales de prescripciones expedidas a asegurados privados.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: el funcional de la aplicación considera casos de uso y procedimientos para la verificación y registro del aseguramiento privado del paciente.
- Revisión documental: existen ejemplos reales de receta electrónica vinculados a un registro de aseguramiento privado.
- Revisión técnica: se crean recetas asociadas a aseguramiento privado y se recuperan a partir de una búsqueda por número de asegurado o similar.

3.1.7. [FT07] Seguimiento de las dispensaciones del tratamiento prescrito

Descripción detallada del control:

En este control se revisa el cumplimiento de la obligación[5] contenida en el artículo 8.4 del RD 1718/2010, en virtud de la cual "el sistema posibilitará al prescriptor el seguimiento de las dispensaciones del tratamiento prescrito y permitirá en el transcurso del tratamiento, informando al paciente, su modificación o anulación, atendiendo a cualquier evento o circunstancia sobrevenida en la situación clínica del paciente, así como a criterios de cumplimiento terapéutico".

Asimismo, se revisa el cumplimiento de la obligación[6] contenida en el artículo 9.5 del RD 1718/2010, en virtud de la cual "cuando el farmacéutico sustituya un medicamento prescrito de conformidad con los criterios legales vigentes, introducirá en el sistema la causa de dicha sustitución, quedando registrado el código del medicamento dispensado. Esta sustitución quedará registrada en el sistema electrónico para posibilitar su consulta por el prescriptor. De la misma forma se actuará en supuestos de sustitución de productos sanitarios".

Finalmente, se revisa el cumplimiento de la obligación[7] contenida en el artículo 9.6 del RD 1718/2010, en virtud de la cual "el sistema electrónico permitirá que

[5] El artículo 8 del RD 1718/2010 resulta aplicable a la prescripción de la receta médica privada electrónica en virtud de lo establecido por el artículo 14.2 del propio RD 1718/2010.

6 El artículo 8.4 del RD 1718/2010, que resulta aplicable a la prescripción de la receta médica privada electrónica en virtud de lo establecido por el artículo 14.2 del propio RD 1718/2010, exige a los prescriptores el seguimiento de las dispensaciones, de acuerdo con lo establecido en el artículo 9 del RD 1718/2010.

[7] El artículo 8.4 del RD 1718/2010, que resulta aplicable a la prescripción de la receta médica privada electrónica en virtud de lo establecido por el artículo 14.2 del propio RD 1718/2010, exige

el farmacéutico bloquee cautelarmente la dispensación de un medicamento prescrito cuando se aprecie la existencia de error manifiesto en la prescripción, inadecuación de ésta a la medicación concomitante, alerta de seguridad reciente o cualquier otro motivo que pueda suponer un riesgo grave y evidente para la salud del paciente. Esta circunstancia se comunicará de forma telemática al prescriptor. El farmacéutico informará sobre dicho bloqueo al paciente.

El prescriptor deberá revisar la prescripción bloqueada cautelarmente procediendo a su anulación o reactivación según considere".

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Descripción del funcional de la aplicación referido a la prescripción.
- Modelos de datos correspondientes a la aplicación de prescripción.
- Descripción del sistema de interconexión con dispensadores.
- Ejemplos reales de informaciones de dispensación recibidas y, en su caso, modificaciones o anulaciones del tratamiento.
- Ejemplos reales de información al paciente.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: el funcional de la aplicación considera casos de uso y procedimientos para la recepción de información para el seguimiento de la dispensación, así como para la realización de modificaciones en el tratamiento, o su anulación, todo ello con información al paciente.
- Revisión documental: existen ejemplos de informaciones de dispensación, así como de sustituciones o bloqueos de dispensaciones, y modificaciones o anulaciones de tratamientos.
- Revisión técnica: se expide una receta electrónica de prueba al auditor, se dispensa y se verifica la recepción de la información.
- Revisión técnica: se modifica un tratamiento.
- Revisión técnica: se anula un tratamiento.

3.1.8. [FT08] Mecanismos de protección y confidencialidad en la dispensación de los tratamientos

a los prescriptores el seguimiento de las dispensaciones, de acuerdo con lo establecido en el artículo 9 del RD 1718/2010.

Descripción detallada del control:

En este control se revisa el cumplimiento de la obligación[8] contenida en el artículo 8.5 del RD 1718/2010, en virtud de la cual "el paciente podrá solicitar en el momento de la prescripción, protección y confidencialidad en la dispensación de algún tratamiento. En estos casos el tratamiento se diferenciará para la dispensación, pudiéndose realizar a través de receta en soporte papel o a través de los procedimientos que se determinen por las Administraciones sanitarias".

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Descripción del funcional de la aplicación referido a la prescripción.
- Modelos de datos correspondientes a la aplicación de prescripción.
- Ejemplos reales de prescripciones con protección y confidencialidad en la dispensación.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: el funcional de la aplicación considera casos de uso y procedimientos para la protección y confidencialidad en la dispensación de un medicamento, todo ello con información al paciente.
- Revisión documental: existen ejemplos de informaciones de dispensación, así como de sustituciones o bloqueos de dispensaciones, y modificaciones o anulaciones de tratamientos.
- Revisión técnica: se expide una receta electrónica de prueba al auditor, con protección y confidencialidad, y se verifica el cumplimiento de las medidas en la dispensación.

3.1.9. [FT09] Impresión de la hoja de información al paciente y/o de medicación activa

Descripción detallada del control:

En este control se revisa el cumplimiento de la obligación contenida en el artículo 3.1 del RD 1718/2010, en virtud de la cual "las recetas médicas, públicas o privadas [...] deberán ser complementadas con una hoja de información al paciente, de entrega obligada al mismo, en la que se recogerá la información del tratamiento necesaria para facilitar el uso adecuado de los medicamentos o

[8] El artículo 8 del RD 1718/2010 resulta aplicable a la prescripción de la receta médica privada electrónica en virtud de lo establecido por el artículo 14.2 del propio RD 1718/2010.

productos sanitarios prescritos", así como de la obligación[9] contenida en el artículo 8.6 del RD 1718/2010, en virtud de la cual "al efectuar la prescripción mediante el sistema de receta electrónica, se imprimirá y deberá ser entregado al paciente un documento de información del tratamiento prescrito"; obligaciones que vienen moduladas además por lo establecido en el artículo 14.3 del RD 1718/2010, en virtud del cual "el prescriptor podrá realizar la impresión de la hoja de medicación activa, en función de las características del sistema implantado".

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Descripción del funcional de la aplicación referido a la prescripción.
- Modelos-tipo de documento de información al paciente y, en su caso, de hoja de medicación activa.
- Ejemplos reales de documentos de información al paciente y, en su caso, de hojas de medicación activa.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: el funcional de la aplicación considera casos de uso y procedimientos para la expedición de documentos de información al paciente y, en su caso, de hojas de medicación activa.
- Revisión documental: existen ejemplos reales de documentos de información al paciente y, en su caso, de hojas de medicación activa.
- Revisión técnica: se expide una receta electrónica de prueba al auditor, y se verifica la producción y entrega del documento de información al paciente y, en su caso, de la hoja de medicación activa.

3.1.10. [FT10] Remisión telemática de la hoja de información al paciente y/o de medicación activa

Descripción detallada del control:

En este control se revisa el cumplimiento de la posibilidad[10] contenida en el artículo 8.6 del RD 1718/2010, en virtud de la cual "en el caso de personas que acrediten situación de discapacidad que impida o dificulte el acceso al contenido de los documentos referidos en el apartado anterior, las autoridades sanitarias competentes, en función de las características del sistema de receta electrónica implantado, promoverán la incorporación de las herramientas que permitan a

[9] El artículo 8 del RD 1718/2010 resulta aplicable a la prescripción de la receta médica privada electrónica en virtud de lo establecido por el artículo 14.2 del propio RD 1718/2010.

[10] El artículo 8 del RD 1718/2010 resulta aplicable a la prescripción de la receta médica privada electrónica en virtud de lo establecido por el artículo 14.2 del propio RD 1718/2010.

estos pacientes recibir la información en formato digital accesible, por medio de envío a la dirección de correo electrónico que indiquen u otra vía o canal idóneo a este propósito".

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Descripción del funcional de la aplicación referido a la prescripción.
- Modelos-tipo de documento de información al paciente y, en su caso, de hoja de medicación activa, en formato digital adaptado.
- Ejemplos reales de documentos de información al paciente y, en su caso, de hojas de medicación activa, en formato digital adaptado.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: el funcional de la aplicación considera casos de uso y procedimientos para la expedición de documentos de información al paciente y, en su caso, de hojas de medicación activa, en formato digital adaptado.
- Revisión documental: existen ejemplos reales de documentos de información al paciente y, en su caso, de hojas de medicación activa, en formato digital adaptado.
- Revisión técnica: se expide una receta electrónica de prueba al auditor, y se verifica la producción y entrega del documento de información al paciente y, en su caso, de la hoja de medicación activa, en formato digital adaptado.

3.2. Controles de formalización documental

3.2.1. [FD01] Contenidos mínimos de la receta electrónica

Descripción detallada del control:

En este control se revisan el cumplimiento de las obligaciones de emisión de la receta en soporte electrónico, previstas en los artículos 3.2 y 8.2 del RD 1718/2010, con los datos básicos obligatorios, relativos a paciente, medicamento, prescriptor y fecha de prescripción, así como de la inclusión del código o número de identificación de la prescripción de cada medicamento y producto sanitario, asignado por el sistema electrónico con carácter único e irrepetible; y de la información de la relación activa de medicamentos correspondiente a los tratamientos en curso.

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Descripción del funcional de la aplicación referido a la prescripción.
- Modelos de datos correspondientes a la aplicación de prescripción.
- Modelos-tipo de recetas electrónicas.
- Ejemplos reales de recetas electrónicas.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: el funcional de la aplicación considera casos de uso y procedimientos para la expedición de recetas electrónicas con los datos e informaciones exigidas.
- Revisión documental: el modelo-tipo de receta electrónica incluye los datos e informaciones exigidas.
- Revisión documental: existen ejemplos reales de receta electrónica con los datos e informaciones exigidas.
- Revisión técnica: se expide una receta electrónica de prueba al auditor, con los datos e informaciones exigidas, y se verifica la documentación resultante.

3.2.2. [FD02] Firma electrónica avanzada basada en certificado cualificado de la receta electrónica

Descripción detallada del control:

En este control se revisa el cumplimiento de la obligación prevista en el artículo 3.2.c.6º) del RD 1718/2010, en virtud de la cual "la firma será estampada personalmente una vez cumplimentados los datos de consignación obligatoria y la prescripción objeto de la receta. En las recetas electrónicas se requerirá la firma electrónica, que deberá producirse conforme con los criterios establecidos por la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos", así como artículo 8.1 del RD 1718/2010, que dispone que "el prescriptor [...] firmará electrónicamente la prescripción". La referencia a la Ley 11/2007 debe entenderse realizada hoy, a la Ley 39/2015, de 1 de octubre, de procedimiento administrativo común de las Administraciones Públicas (LPAC), que se encuentra alineada con el Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (Reglamento eIDAS).

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Descripción del funcional de la aplicación referido a la prescripción.
- Modelos-tipo de recetas electrónicas.
- Ejemplos reales de firmas electrónicas de recetas electrónicas.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: el funcional de la aplicación considera casos de uso y procedimientos para la firma electrónica de los actos del prescriptor.
- Revisión técnica: Empleo de firma electrónica avanzada de la receta electrónica, por ejemplo empleando el carné oficial del Colegio de Médicos correspondiente, u otro sistema basado en certificado cualificado, y de acuerdo con las reglas de la política de firma electrónica, publicada por el CGCOM.
- Revisión técnica: Empleo de formatos de firma electrónica avanzada, como XAdES, CAdES o PAdES.
- Revisión técnica: Cumplimiento por las aplicaciones de firma electrónica avanzada de los requisitos de fiabilidad que se establecen a continuación.
    - Comunicación fiable entre componentes del sistema:
        - La aplicación debe mantener la integridad de:
            - Los datos a firmar, los datos a firmar formateados, la representación de los datos a firmar y el resto de informaciones suministradas por el firmante.
            - Los intercambios de datos durante el flujo del protocolo de comunicación entre la aplicación y el dispositivo, mediante el uso de un canal seguro.
        - La aplicación debe mantener la confidencialidad de los componentes de los datos a firmar, de los datos a firmar formateados y de los datos de autenticación del firmante.
        - La aplicación que opere en un entorno público borrará de forma segura todos los datos relativos a una firma después de haber completado cada proceso de firma.
        - Cuando se utilice un sistema público de creación de firma, éste no deberá retener ni copiar los datos de autenticación del firmante, de los componentes de los datos a firmar ni de los datos a firmar formateadas, a ninguna persona no autorizada por el firmante.

- La aplicación debe garantizar que los datos a firmar presentados al firmante son los mismos que los que éste seleccionó.
- La aplicación debe garantizar que los componentes de los datos a firmar empleados para crear los datos a firmar formateados y la representación de los datos a firmar son los mismos que se presentaron al firmante y que son idénticos a los que éste seleccionó.
- Cualquier dato de autenticación del firmante que sea transferido entre diferentes componentes distribuidos de la aplicación de creación de firma electrónica debe serlo empleando una ruta fiable que ofrezca integridad y confidencialidad.
- Los datos a firmar – con o sin formato - que sean transferidos entre diferentes componentes distribuidos de la aplicación de creación de firma electrónica deben serlo empleando un canal fiable que ofrezca integridad y confidencialidad.
- Todos los procesos y los puertos de entrada y salida del sistema de la aplicación de creación de firma electrónica que no se encuentran en el control de la misma serán cerrados o monitorizados para evitar interferencias.

- Interfaces externas a la aplicación de firma electrónica:
  - La aplicación de firma electrónica debe evitar ser corrompida por código malicioso y, en caso de serlo, debe existir un proceso para sanear los componentes corruptos.
  - La aplicación de firma electrónica debe mantener la integridad de sus componentes funcionales y evitar la posibilidad de su corrupción por intrusos.
  - En relación con los componentes de la aplicación que se pueden descargar de la red, la descarga se realizará desde una fuente fiable, circunstancia que se indicará en la documentación del producto.
- Requisitos generales de los datos a firmar:
  - Los datos a firmar deben incluir, necesariamente, un documento del firmante.
  - La firma debe contener, necesariamente, el certificado del firmante seleccionado, en su caso, relativo a los datos de creación de firma empleados para producir la firma electrónica, de acuerdo con la intención del firmante.

- Los datos a firmar deben contener el tipo de contenido de datos del documento del firmante siempre que esta información no conste en el propio fichero.
- Es necesario verificar la firma electrónica producida, aunque esta verificación no sea completa.

- Requisitos del documento a firmar:
  - El componente de presentación del documento permitirá incluir el tipo de contenido de datos a que corresponde el documento del firmante, de forma explícita, como atributo de la firma.
  - El componente de presentación del documento informará al firmante de los errores sintácticos del documento y le permitirá abortar el proceso de firma.
  - El componente de presentación del documento debe documentar los tipos de contenidos de datos que resulta posible firmar con todas las garantías, así como las consecuencias de firmar documentos con tipos de contenidos falsos.
  - Cuando el firmante solicite la creación de una firma en relación con un tipo de contenido de datos no soportado por el componente de presentación del documento, éste le advertirá de los efectos potencialmente problemáticos de este hecho, y de su responsabilidad.
  - El componente de presentación del documento debe garantizar que el documento presentado al firmante es el mismo que será firmado, así como que es el mismo documento que ha seleccionado el firmante.
  - El componente de presentación del documento no debería permitir firmar documentos con código activo. Si lo permite, entonces debería informar al firmante de la existencia de este código, y habría de existir un visor del documento firmado, con la capacidad de detectar las modificaciones de la presentación del documento firmado.
- Requisitos de los atributos de firma electrónica:
  - La aplicación de firma electrónica permitirá ver los atributos a firmar.
  - La aplicación de firma electrónica debe garantizar que los atributos presentados al firmante son los mismos que serán

firmados, así como que son los mismos atributos que ha seleccionado el firmante.

- La aplicación de firma electrónica debe garantizar la integridad y autenticidad de los atributos de la firma.
- La aplicación de firma electrónica debe informar al firmante de la presencia de texto oculto, macros o código activo en los atributos, y ha de existir un visor de los atributos firmados, con la capacidad de detectar las modificaciones de la presentación de los atributos firmados.
- La aplicación de firma electrónica debe comprobar el periodo de validez del certificado, y su estado de revocación, antes de finalizar el proceso de firma, e impedir el uso en caso de invalidez.
- La aplicación de firma electrónica debe permitir al firmante la inspección de los principales elementos del certificado de firma con el que se firmará.

- Requisitos de resumen y formato de los datos a firmar:
  - La aplicación de firma electrónica impondrá controles para verificar la validez, autenticidad y totalidad de todos los componentes obtenidos para producir el formato correcto de firma escogido por el signatario.
  - La aplicación de firma electrónica empleará los algoritmos de resumen adecuados para la producción de la representación de los datos a firmar.
  - La aplicación de firma electrónica empleará los formados de entrada de firma electrónica adecuados para la producción de la firma de los datos a firmar.
  - La aplicación de firma electrónica debe garantizar la correcta producción de la representación de los datos a firmar.
- Interacción segura entre aplicación y firmante:
  - La aplicación de firma electrónica, antes de iniciar el proceso de firma, solicitará al firmante que realice una acción, no trivial, y difícil de producir por accidente, para invocar la firma.
  - La aplicación de firma establecerá un límite al periodo de inactividad de la aplicación, en que ésta no se relaciona con el firmante o se encuentra en tiempo de procesamiento. Transcurrido este límite temporal, se exigirá una nueva autenticación al usuario.

- La aplicación de firma electrónica debe implantar las siguientes funciones en relación con el control del proceso de firma electrónica:
  - Posibilidad de seleccionar el documento y los atributos de firma, en especial el certificado de firma deseado.
  - Posibilidad de completar el proceso de invocación de firma para iniciar la interacción entre la aplicación y el dispositivo – seguro – de creación de firma.
  - Posibilidad de autenticar al firmante mediante datos de autenticación basadas en información secreta o biometría.
  - Posibilidad de modificar los datos de autenticación del firmante, de acuerdo con la política de seguridad de la aplicación.
- La interfaz de la aplicación de firma electrónica debe ser lo más simple y directa posible, para evitar que el firmante se pierda y genere situaciones inseguras.
- La interfaz de la aplicación de firma electrónica debe borrar de la pantalla los datos personales del firmante, tras las operaciones completadas, así como dentro de un plazo de inactividad razonable, en caso de operaciones interrumpidas.

o Identificación y autenticación del firmante:

- La aplicación de firma electrónica, cuando sea responsable de la autenticación del firmante, deberá proveer una función para realizar este proceso de forma segura.
- Cuando los datos de autenticación del firmante se encuentren almacenados en la aplicación de firma electrónica, estos datos se deberán preservar de forma confidencial y borrarse cuando ya no sean necesarios.
- La aplicación de firma electrónica, de forma coordinada con el dispositivo seguro de firma electrónica, deberá permitir varios intentos de autenticación, mediante un contador y una función de bloqueo, en caso de superación de los intentos permitidos. La aplicación no deberá dar información sobre el tipo de error cometido por la persona que se autentica.
- La aplicación de firma electrónica debe funcionar de forma coordinada con el dispositivo de firma electrónica, en todo aquello que se encuentre referido a la política de seguridad

de los datos de autenticación (especialmente longitudes de claves y semántica de la contraseña), y no debe impedir la aplicación de la política de cambio de contraseña del dispositivo de firma electrónica.

- La aplicación de firma que gestione la autenticación del firmante debe implantar una ruta fiable desde el teclado del ordenador o del lector de tarjeta, hasta el dispositivo de firma electrónica.
- La aplicación de firma debe implantar una función de cambio de los datos de autenticación de firma, excepto cuando su política de seguridad lo prohíba y esta prohibición no suponga una interferencia con la política de cambio de contraseña del dispositivo de firma electrónica.
- La aplicación de firma electrónica no mostrará los datos de autenticación de firma, sino uno o más símbolos para indicar el tecleado de los datos. Estos símbolos no revelarán ni permitirán adivinar los datos de autenticación.
- La aplicación de firma electrónica requerirá la introducción dos veces de unos nuevos datos de autenticación, y comprobará que las dos son idénticos antes de entregarlos al dispositivo de firma para el cambio.

3.3. Controles específicos de seguridad y confidencialidad

3.3.1. [SC01] Acceso del médico al sistema de receta electrónica

Descripción detallada del control:

En este control se revisa el cumplimiento de la obligación[11] establecida en el artículo 8.1 del RD 1718/2010, en virtud de la cual "el prescriptor ha de acreditar su identidad". Asimismo, se revisa el cumplimiento de la obligación establecida en el artículo 14.2 del RD 1718/2010, en virtud de la cual "el acceso al sistema de receta médica privada electrónica se efectuará [...] a través del [...], además del certificado electrónico del prescriptor".

Asimismo, de acuerdo con lo establecido en el artículo 18.1 del RD 1718/2010, "el prescriptor se responsabilizará [...] del acceso [...] para la prescripción electrónica. Las instituciones en las que los prescriptores presten sus servicios pondrán los medios necesarios para que puedan cumplirse estas obligaciones".

[11] El artículo 8 del RD 1718/2010 resulta aplicable a la prescripción de la receta médica privada electrónica en virtud de lo establecido por el artículo 14.2 del propio RD 1718/2010.

Este control se complementa con, y apoya en, el control [IN03], sobre verificación interoperable de certificados electrónicos cualificados.

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Descripción del funcional de la aplicación referido a la prescripción.
- Diseño técnico del sistema de autenticación de la aplicación de prescripción.
- Modelos de datos de autenticación intercambiables correspondientes a la aplicación de prescripción.
- Ejemplos reales de autenticación.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: el funcional de la aplicación considera casos de uso y procedimientos para la autenticación del prescriptor.
- Revisión técnica: Se verifica el funcionamiento correcto del sistema de autenticación, mediante un juego de pruebas de certificados, vigentes y revocados, – por ejemplo, correspondientes al carné oficial del Colegio de Médicos correspondiente –, y de acuerdo con las reglas de la política de autenticación electrónica, publicada por el CGCOM.

3.3.2. [SC02] Acceso del paciente al sistema de receta electrónica

Descripción detallada del control:

En este control se revisa el cumplimiento de la obligación establecida en el artículo 14.2 del RD 1718/2010, en virtud de la cual "el acceso al sistema de receta médica privada electrónica se efectuará a través del certificado del DNI electrónico del paciente y en caso de imposibilidad se accederá a través del Documento Nacional de Identidad o en su caso del padre o tutor".

Para el caso de sistema de receta electrónica apoyada en un aseguramiento privado, a efectos del servicio opcional de almacenamiento de la prescripción en la historia clínica del paciente, se podría utilizar, de forma complementaria, cualquier sistema de firma electrónica reconocida que contenga el NIF del paciente y, en su caso, la condición de aseguramiento privado del mismo.

Este control se complementa con el control [IN03], sobre verificación interoperable de certificados electrónicos cualificados, en el caso del DNI electrónico y otros certificados.

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Descripción del funcional de la aplicación referido a la prescripción.
- Diseño técnico del sistema de autenticación de paciente, con DNI electrónico o, de forma complementaria, otro sistema de firma electrónica avanzada basada en certificado cualificado, de la aplicación de prescripción.
- Diseño técnico de autenticación mediante DNI no electrónico.
- Modelos de datos de autenticación intercambiables correspondientes a la aplicación de prescripción.
- Ejemplos reales de autenticación.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: el funcional de la aplicación considera casos de uso y procedimientos para la autenticación del paciente con DNI electrónico o, de forma complementaria, otro sistema de firma electrónica avanzada basada en certificado electrónico cualificado; y para la autenticación basada en DNI no electrónico.
- Revisión documental: Existen procedimientos solventes para la identificación del padre o tutor, en el caso de acceso a la receta electrónica de menores de edad o mayores de edad sujetos a tutela.
- Revisión técnica: Se verifica el funcionamiento correcto del sistema de autenticación, mediante el DNI electrónico del auditor, y de acuerdo con las reglas de la política de autenticación electrónica, publicada por el CGCOM.
- Revisión técnica: Se verifica el procedimiento de verificación de la identidad del paciente, con el DNI no electrónico del auditor.

3.3.3. [SC03] Seguridad del equipo de acceso en el sistema de receta electrónica

Descripción detallada del control:

En este control se revisa el cumplimiento de la obligación[12] prevista en el artículo 8.1 del RD 1718/2010, en virtud de la cual "el prescriptor accederá al sistema de receta médica electrónica a través de un equipo integrado en el Sistema de receta electrónica que deberá estar autentificado, garantizándose las comunicaciones

[12] El artículo 8 del RD 1718/2010 resulta aplicable a la prescripción de la receta médica privada electrónica en virtud de lo establecido por el artículo 14.2 del propio RD 1718/2010.

cifradas", de acuerdo con las correspondientes políticas de seguridad de comunicaciones electrónicas publicadas por el CGCOM.

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Modelo de seguridad de la aplicación de prescripción.
- Mecanismos de autenticación de equipo.
- Mecanismos de cifrado de comunicaciones.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: Existe un modelo de seguridad robusto y fiable de conexión entre el equipo del prescriptor y la aplicación de prescripción, con mecanismos fuertes de autenticación y cifrado de comunicaciones.
- Revisión técnica: Se verifican los registros de actividad y autenticación de la aplicación de prescripción para comprobar los procedimientos de autenticación del equipo.
- Revisión técnica: Se revisan el establecimiento efectivo de un canal cifrado o, alternativamente, un sistema de mensajería cifrada entre una aplicación local del equipo del prescriptor y la aplicación de prescripción o sistema de receta electrónica.

3.3.4. [SC04] Controles de custodia y conservación segura

Descripción detallada del control:
En este control se revisa el cumplimiento de la obligación establecida en el artículo 18.1 del RD 1718/2010, en virtud de la cual "el prescriptor se responsabilizará [...] del acceso y utilización de datos para la prescripción electrónica. Las instituciones en las que los prescriptores presten sus servicios pondrán los medios necesarios para que puedan cumplirse estas obligaciones".

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Modelo de seguridad de la aplicación de prescripción.
- Descripción de los procedimientos de custodia y conservación de recetas electrónicas, y datos del sistema. En particular, política de evidencia electrónica y preservación digital de las recetas electrónicas.
- Descripción de procedimientos de borrado seguro de datos y recetas, transcurrido el plazo legal de conservación, así como de transferencia a la historia clínica del paciente.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión mixta: Existen procedimientos y mecanismos de custodia y conservación segura de los datos del sistema de receta médica privada electrónica (base de datos),
- Revisión mixta: Existen procedimientos documentados y mecanismos de custodia y conservación segura, así como de mantenimiento evidencial y preservación digital, de las recetas electrónicas formalizadas documentalmente (firmadas electrónicamente).

3.3.5. [SC05] Controles de disponibilidad 24x7x365 del sistema de receta médica privada electrónica

Descripción detallada del control:

En este control, opcional, se revisa la existencia de controles de disponibilidad 24x7x365 del sistema de receta médica privada electrónica, en soporte de los servicios de urgencias.

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Modelo de seguridad de la aplicación de prescripción.
- Plan de continuidad del negocio.
- Plan de recuperación ante el desastre.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: Existen planes y procedimientos formalmente documentados que soportan la operativa 24x7x365, de la aplicación de prescripción.
- Revisión documental: Existen registros fiables de la prueba ordinaria de los planes de continuidad y recuperación.

3.4. Controles de interoperabilidad

3.4.1. [IN01] Normas de interconexión de sistemas de receta médica electrónica privada

Descripción detallada del control:

En este control se revisa el cumplimiento de las normas de interconexión de sistemas de receta médica electrónica privada entre los diferentes agentes funcionales (prescriptor, dispensador, etc.)

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Descripción del funcional de la aplicación referido a la prescripción.
- Diseño técnico de comunicaciones de la aplicación de prescripción.
- Modelos de datos intercambiables correspondientes a la aplicación de prescripción.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: Las comunicaciones necesarias para la interconexión e intercambio de datos entre las aplicaciones de prescripción y dispensación, así como a terceros requeridos, están correctamente documentadas.
- Revisión técnica: Se verifica el funcionamiento correcto de los canales establecidos, mediante un juego de pruebas de conexión.

3.4.2. [IN02] Consumo de servicios de autenticación delegada

Descripción detallada del control:

En este control, opcional, se revisa el cumplimiento de la obligación[13] establecida en el artículo 8.1 del RD 1718/2010, en virtud de la cual "el prescriptor ha de acreditar su identidad", mediante el consumo de servicios de autenticación delegada, como STIRK o CEF eID.

Este control es complementario, y apoya, al control [SC01], referido al control de acceso por parte del prescriptor. Este control aplica cuando el proceso de autenticación se delega a un sistema externo.

[13] El artículo 8 del RD 1718/2010 resulta aplicable a la prescripción de la receta médica privada electrónica en virtud de lo establecido por el artículo 14.2 del propio RD 1718/2010.

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Descripción del funcional de la aplicación referido a la prescripción.
- Diseño técnico del sistema de autenticación de la aplicación de prescripción.
- Modelos de datos de autenticación intercambiables correspondientes a la aplicación de prescripción.
- Ejemplos reales de autenticación delegada.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: el funcional de la aplicación considera casos de uso y procedimientos para la autenticación delegada.
- Revisión documental: Las comunicaciones necesarias para la interconexión e intercambio de datos entre las aplicaciones de prescripción y de autenticación delegada, están correctamente documentadas.
- Revisión técnica: Se verifica el funcionamiento correcto del sistema de autenticación delegada, mediante un juego de pruebas de certificados, vigentes y revocados.

3.4.3. [IN03] Verificación interoperable de certificados electrónicos

Descripción detallada del control:

En este control se revisa el cumplimiento de la obligación[14] establecida en el artículo 8.1 del RD 1718/2010, en virtud de la cual "el prescriptor [...]firmará electrónicamente la prescripción", y en el artículo 14.2 del RD 1718/2010, en virtud de la cual "el acceso al sistema de receta médica privada electrónica se efectuará a través del certificado del DNI electrónico del paciente y en caso de imposibilidad se accederá a través del Documento Nacional de Identidad o en su caso del padre o tutor, además del certificado electrónico del prescriptor", lo cual exige la verificación interoperable de certificados de médico colegiado y de pacientes, incluyendo DNI electrónico y otros certificados electrónicos cualificados de firma avanzada.

La verificación se puede realizar en local, mediante un sistema apropiado de verificación de certificados, o bien en remoto, empleando una plataforma específica de servicio de verificación de certificados.

[14] El artículo 8 del RD 1718/2010 resulta aplicable a la prescripción de la receta médica privada electrónica en virtud de lo establecido por el artículo 14.2 del propio RD 1718/2010.

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Descripción del funcional de la aplicación referido a la prescripción.
- Diseño técnico del sistema de verificación de certificados electrónicos de la aplicación de prescripción.
- Modelos de datos de verificación de certificados electrónicos correspondientes a la aplicación de prescripción.
- Ejemplos reales de verificación de certificados electrónicos.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: el funcional de la aplicación considera casos de uso y procedimientos para la autenticación delegada.
- Revisión documental: Las comunicaciones necesarias para la interconexión e intercambio de datos entre las aplicaciones de prescripción y SINCERT, están correctamente documentadas.
- Revisión técnica: Cumplimiento por las aplicaciones de verificación de firma electrónica reconocida de los requisitos de fiabilidad que se establecen a continuación.
    - Proporcionar servicios de confianza a las aplicaciones usuarias o consumidoras de los servicios de certificación y firma para la receta electrónica.
    - Proporcionar, en un único punto de llamada, como por ejemplo DSS, todos los elementos de confianza y de interoperabilidad organizativa, semántica y técnica necesarios para integrar los distintos certificados reconocidos y firmas del sistema de receta electrónica.
    - Permitir el empleo de formatos, estándares y políticas de firma electrónica y de certificados para las firmas electrónicas entre las aplicaciones usuarias, y de otros elementos de interoperabilidad relacionados con los certificados, tales como el análisis de los campos y extracción univoca de la información pertinente. En particular, se tendrán en cuenta los estándares europeos de las Organizaciones Europeas de Estandarización en el campo de las Tecnologías de Información y Comunicación aplicadas a la firma electrónica.
    - Incorporar las listas de confianza de los certificados interoperables entre las distintas Administraciones públicas nacionales y europeas

según el esquema operativo de gestión correspondiente de la lista de confianza, a efectos de operaciones transfronterizas.

- Revisión técnica: Se verifica el funcionamiento correcto del sistema de verificación de certificados, mediante un juego de pruebas de certificados, vigentes y revocados.

3.4.4. [IN04] Modelos de datos para el acceso al sistema de receta médica privada del prescriptor

Descripción detallada del control:

En este control se revisa la existencia de modelos de datos comunes para el acceso al sistema de receta médica privada del prescriptor por las aplicaciones de dispensación, al objeto del cumplimiento de la obligación prevista en el artículo 2.3 del RD 1718/2010, en virtud del cual "la receta médica garantizará que el tratamiento prescrito pueda ser dispensado al paciente en cualquier oficina de farmacia del territorio nacional", así como en el artículo 14.1 del RD 1718/2010, en virtud del cual "los tratamientos prescritos al paciente en receta médica privada electrónica podrán ser dispensados en cualquier oficina de farmacia del territorio nacional".

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Modelos de datos de receta intercambiables correspondientes a la aplicación de prescripción.
- Ejemplos reales de recetas de acuerdo con los modelos de datos establecidos.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: Los modelos de datos están correctamente documentados e implementados en los esquemas de base de datos.
- Revisión técnica: Se verifica la consistencia de las implementaciones del modelo de datos en las diferentes aplicaciones, mediante contraste de recetas reales.

3.4.5. [IN05] Empleo del esquema de intercambio de recetas médicas privadas electrónicas

Descripción detallada del control:

En este control se revisa la existencia de instrumentos de intercambio de recetas entre al sistema de receta médica privada del prescriptor por las aplicaciones de dispensación, típicamente en XML, al objeto del cumplimiento de la obligación prevista en el artículo 2.3 del RD 1718/2010, en virtud del cual "la receta médica garantizará que el tratamiento prescrito pueda ser dispensado al paciente en cualquier oficina de farmacia del territorio nacional", así como en el artículo 14.1 del RD 1718/2010, en virtud del cual "los tratamientos prescritos al paciente en receta médica privada electrónica podrán ser dispensados en cualquier oficina de farmacia del territorio nacional".

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Modelos de instrumentos (vocabularios XSD) para el intercambio de informaciones de receta electrónica entre las aplicaciones de prescripción y dispensación.
- Ejemplos reales de instrumentos de XML correspondientes a recetas intercambiadas.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: Los vocabularios XSD están correctamente documentados e implementados en los procedimientos de intercambio.
- Revisión técnica: Se verifica la consistencia entre recetas reales en XML y el correspondiente vocabulario.

3.4.6. [IN06] Modelo de integración de las recetas en la historia clínica del paciente

Descripción detallada del control:

En este control, opcional, se revisa la posibilidad de que, a petición del paciente, las recetas electrónicas prescritas se integren en su sistema de historia clínica electrónica.

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Modelos de instrumentos (vocabularios XSD) para el intercambio de informaciones de receta electrónica entre las aplicaciones de prescripción e historia clínica de terceros.
- Ejemplos reales de instrumentos de XML correspondientes a recetas intercambiadas.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: Los vocabularios XSD están correctamente documentados e implementados en los procedimientos de intercambio.
- Revisión técnica: Se verifica la consistencia entre recetas reales en XML y el correspondiente vocabulario.

3.5. Controles de protección de datos de carácter personal

3.5.1. [PD01] Cláusula de información de protección de datos personales

Descripción detallada del control:

En este control se revisa el cumplimiento de la obligación establecida en el artículo 3.2, último párrafo, del RD 1718/2010, en virtud de la cual "En [...] la hoja de información al paciente para el caso de receta electrónica se incluirá una cláusula que informe al paciente en los términos establecidos en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal".

El anexo del RD 1718/2010 establece el siguiente modelo de cláusula:
"El paciente autoriza el acceso por el farmacéutico a los tratamientos incluidos en esta relación.
El paciente conservará este documento de información durante el período de validez del tratamiento.
En cumplimiento del art. 5 de la Ley Orgánica 15/99, se informa de que estos datos serán incorporados al fichero "..." para la gestión y control de la prestación farmacéutica, cuyo órgano responsable es "..." Puede ejercer sus derechos de acceso, rectificación, cancelación y oposición ante "..." o en el telf. ...".

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Modelos-tipo de documento de información al paciente y, en su caso, de hoja de medicación activa.
- Ejemplos reales de documentos de información al paciente y, en su caso, de hojas de medicación activa.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: existen ejemplos reales de documentos de información al paciente y, en su caso, de hojas de medicación activa.
- Revisión técnica: se expide una receta electrónica de prueba al auditor, y se verifica la producción y entrega del documento de información al

paciente y, en su caso, de la hoja de medicación activa, con la cláusula LOPD.

3.5.2. [PD02] Medidas de seguridad de nivel alto

Descripción detallada del control:

En este control se revisa el cumplimiento de las obligaciones establecidas por el artículo 11 del RD 1718/2010, en virtud del cual "el sistema de receta médica electrónica garantizará la seguridad en el acceso y transmisión de la información, así como la protección de la confidencialidad de los datos, de conformidad con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Se implantarán las medidas de seguridad de nivel alto, previstas en la referida normativa de protección de datos de carácter personal".

Asimismo, el artículo 19.1 del RD 1718/2010 establece que "en los trámites a que sean sometidas las recetas médicas y órdenes de dispensación hospitalaria, y especialmente en su tratamiento informático, así como en su proceso electrónico, deberá quedar garantizada, conforme previene la normativa específica de aplicación, la confidencialidad de la asistencia médica y farmacéutica, la intimidad personal y familiar de los ciudadanos y la protección de sus datos de carácter personal. A tal efecto, se implantarán en el tratamiento de los datos las medidas de seguridad previstas en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal y en su normativa de desarrollo".

Finalmente, la disposición adicional séptima del RD 1718/2010 indica que "en las actuaciones previstas en este real decreto que tengan relación con el tratamiento, cesión y custodia de datos de carácter personal se estará a lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, y en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal".

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Inscripción del fichero correspondiente en la Agencia Española de Protección de Datos.
- Documento de seguridad de datos personales del sistema de receta electrónica.
- Diagrama de entidad-relación de la base de datos de soporte al sistema de receta electrónica.
- Identificación de flujos de entrada y salida de datos personales.
- Planes y procedimientos de tratamiento y seguridad relativos a los datos de carácter personal.

- Procedimientos de ejercicio de los derechos de acceso, rectificación, cancelación y oposición.
- Registros de actividad generados en ejecución de los procedimientos de seguridad y de ejercicio de derechos.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: Documento de seguridad LOPD.
    - Existe un documento de seguridad elaborado por el responsable del fichero o tratamiento, que recoge las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente, que es de obligado cumplimiento para el personal con acceso a los sistemas de información.
    - El documento de seguridad podrá ser único y comprensivo de todos los ficheros o tratamientos, o bien individualizado para cada fichero o tratamiento. También podrán elaborarse distintos documentos de seguridad agrupando ficheros o tratamientos según el sistema de tratamiento utilizado para su organización, o bien atendiendo a criterios organizativos del responsable. En todo caso, tendrá el carácter de documento interno de la organización.
    - El documento contiene, como mínimo, los siguientes aspectos:
        - Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.
        - Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este Reglamento.
        - Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.
        - Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
        - Procedimiento de notificación, gestión y respuesta ante las incidencias.
        - Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.
        - Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción

de los documentos y soportes, o en su caso, la reutilización de estos últimos.
        - La identificación del responsable o responsables de seguridad.
        - Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.
    - Cuando exista un tratamiento de datos por cuenta de terceros, el documento de seguridad contiene la identificación de los ficheros o tratamientos que se traten en concepto de encargado con referencia expresa al contrato o documento que regule las condiciones del encargo, así como de la identificación del responsable y del período de vigencia del encargo.
    - El documento de seguridad se mantiene actualizado en el momento de la revisión y existe un procedimiento para su revisión que se aplica siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, como consecuencia de los controles periódicos realizados. En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.
    - El contenido del documento de seguridad se adecua, en el momento de la revisión, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.
- Revisión documental: Responsable de seguridad LOPD.
    - En el documento de seguridad se designa uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el mismo. Esta designación puede ser única, para todos los ficheros o tratamientos de datos de carácter personal, o diferenciada según los sistemas de tratamiento utilizados, circunstancia que consta claramente en el documento de seguridad.
- Revisión documental: Funciones y obligaciones del personal.
    - Las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información están claramente definidas y documentadas en el documento de seguridad.

  - También se definen las funciones de control o autorizaciones delegadas por el responsable del fichero o tratamiento.
  - El responsable del fichero o tratamiento adopta las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones, así como las consecuencias en que pudiera incurrir en caso de incumplimiento.
- Revisión mixta. Identificación y autenticación.
  - El responsable del fichero o tratamiento adopta las medidas que garanticen la correcta identificación y autenticación de los usuarios.
  - El responsable del fichero o tratamiento establece un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.
  - Cuando el mecanismo de autenticación se base en la existencia de contraseñas existe un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad (los controles SC01 y SC02 no permiten el empleo de contraseñas para el acceso de médicos y pacientes, de forma que esta posibilidad queda limitada a otros accesos).
  - El documento de seguridad establece la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenan de forma ininteligible.
  - El responsable del fichero o tratamiento establece un mecanismo que limita la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.
- Revisión técnica: Control de acceso.
  - Los usuarios tienen acceso únicamente a aquellos recursos que precisan para el desarrollo de sus funciones.
  - El responsable del fichero se encarga de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.
  - El responsable del fichero establece mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.
  - Exclusivamente el personal autorizado para ello en el documento de seguridad concede, altera o anula el acceso autorizado sobre

los recursos, conforme a los criterios establecidos por el responsable del fichero.
    - En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos, está sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.
- Revisión mixta: Control de acceso físico.
    - Exclusivamente el personal autorizado en el documento de seguridad tiene acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información.
- Revisión mixta: Registro de accesos LOPD.
    - De cada intento de acceso se guardan, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.
    - En el caso de que el acceso haya sido autorizado, se guarda la información que permita identificar el registro accedido.
    - Los mecanismos que permiten el registro de accesos están bajo el control directo del responsable de seguridad competente y no permiten la desactivación ni la manipulación de los mismos.
    - Existen procedimientos que garantizan que el período mínimo de conservación de los datos registrados es de dos años.
    - El responsable de seguridad se encarga de revisar al menos una vez al mes la información de control registrada y elabora un informe de las revisiones realizadas y los problemas detectados.
- Revisión técnica: Acceso a datos a través de redes de comunicaciones.
    - Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones, sean o no públicas, garantizan un nivel de seguridad equivalente al correspondiente a los accesos en modo local.
- Revisión mixta: Registro de incidencias LOPD.
    - Existe un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.

  - En el registro de incidencias se consignan, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.
  - El procedimiento garantiza que es necesaria la autorización del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.
- Revisión mixta: Gestión y distribución de soportes y documentos (sólo aplicable a los movimientos de datos de receta en soporte magnético, óptico o análogo).
  - Los soportes y documentos que contienen datos de carácter personal permiten identificar el tipo de información que contienen, se encuentran inventariados y sólo son accesibles por el personal autorizado para ello en el documento de seguridad.
  - Se exceptúan estas obligaciones cuando las características físicas del soporte imposibilitan su cumplimiento, quedando constancia motivada de ello en el documento de seguridad.
  - La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento es autorizada por el responsable del fichero o se encuentra debidamente autorizada en el documento de seguridad.
  - En el traslado de la documentación se adoptan las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.
  - Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal, se procede a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.
  - La identificación de los soportes que contienen datos de carácter personal que la organización considerase especialmente sensibles se realiza utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

  - Existe un sistema de registro de entrada de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.
  - Se dispone de un sistema de registro de salida de soportes que permite, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el destinatario, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.
  - La identificación de los soportes se realiza utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.
  - La distribución de los soportes que contengan datos de carácter personal se realiza cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte.
  - Se cifran los datos que contienen los dispositivos portátiles cuando éstos se encuentran fuera de las instalaciones que están bajo el control del responsable del fichero.
  - Se evita el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado. En caso de que sea estrictamente necesario se hará constar motivadamente en el documento de seguridad y se adoptarán medidas que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos.
- Revisión técnica: Ficheros temporales.
  - Se garantiza que aquellos ficheros temporales o copias de documentos que se hubiesen creado exclusivamente para la realización de trabajos temporales o auxiliares cumplen el nivel de seguridad alto.
  - Todo fichero temporal o copia de trabajo así creado es borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su creación.

- Revisión mixta: Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento.
    - Cuando los datos personales se almacenan en dispositivos portátiles o se traten fuera de los locales del responsable de fichero o tratamiento, o del encargado del tratamiento, existe una autorización previa del responsable del fichero o tratamiento, y en todo caso se garantiza el nivel de seguridad correspondiente al tipo de fichero tratado.
    - La autorización a la que se refiere el párrafo anterior consta en el documento de seguridad y se establece para un usuario o para un perfil de usuarios y determinando un período de validez para las mismas.
- Revisión técnica: Telecomunicaciones.
    - La transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realiza cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.
- Revisión mixta: Copias de respaldo y recuperación.
    - Se establecen procedimientos de actuación para la realización como mínimo semanal de copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.
    - Asimismo, se establecen procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.
    - El responsable del fichero verifica cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.
    - Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizan con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote su realización en el documento de seguridad.
    - Si está previsto realizar pruebas con datos reales, previamente se ha realizado una copia de seguridad.

- Se conserva una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan, que cumple en todo caso las medidas de seguridad exigidas, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.