Al contestar por favor cite estos datos:
Radicado No.: **RADS**
Fecha: **FRAD**
Página 1 de 5

Bogotá D.C.,

RESPUESTA EN LINEA

Señores
IQ INTERQUIROFANOS SA 15
Calle 7 N 39-197 piso 2
Tel. 4481845
jeniffer.uribe@iqinterquirofanos.co
MEDELLIN, - ANTIOQUIA.

Asunto: Radicado No 201842401574382– Validez firma electrónica para consentimientos informados

Respetados señores:
Hemos recibido su comunicación en la cual solicita concepto a estr ministerio de si "*es válida la firma electrónica biométrica de los consentimientos informados por parte del paciente y el profesional, con validez jurídica archivado en HC digital?*", al respecto nos permitimos señalar lo siguiente:

La Resolución 1995 de 1999[1], señala:

> *"ARTICULO 5. **GENERALIDADES.***
> *La Historia Clínica debe diligenciarse en forma clara, legible, sin tachones, enmendaduras, intercalaciones, sin dejar espacios en blanco y sin utilizar siglas. Cada anotación debe llevar la fecha y hora en la que se realiza, con el nombre completo y firma del autor de la misma. (Subrayado fuera de texto).*
> *(...)*
> *ARTICULO 12. **OBLIGATORIEDAD DEL ARCHIVO.***
> *Todos los prestadores de servicios de salud, deben tener un archivo único de historias clínicas en las etapas de archivo de gestión, central e histórico, el cual será organizado y prestará los servicios pertinentes guardando los principios generales establecidos en el Acuerdo 07 de 1994, referente al Reglamento General de Archivos, expedido por el Archivo General de la Nación y demás normas que lo modifiquen o adicionen.*
> *"ARTICULO 13. **CUSTODIA DE LA HISTORIA CLÍNICA.***
> *La custodia de la historia clínica estará a cargo del prestador de servicios de salud que la generó en el curso de la atención, cumpliendo los procedimientos de archivo señalados en la presente resolución, sin perjuicio de los señalados en otras normas legales vigentes. El prestador podrá entregar copia de la historia clínica al usuario o a su representante legal cuando este lo solicite, para los efectos previstos en las disposiciones legales vigentes.*
> ***(...)**"*

Esta misma resolución en relación con los medios técnicos de registro y conservación de la historia clínica, en el artículo 18, establece:

> *"Los Prestadores de Servicios de Salud pueden utilizar medios físicos o técnicos como computadoras y medios magneto-ópticos, cuando así lo consideren conveniente, atendiendo lo establecido en la circular 2 de 1997 expedida por el Archivo General de la Nación, o las normas que la modifiquen o adicionen.*

[1] *"Por la cual se establecen normas para el manejo de la Historia Clínica"*

Los programas automatizados que se diseñen y utilicen para el manejo de las Historias Clínicas, así como sus equipos y soportes documentales, deben estar provistos de mecanismos de seguridad, que imposibiliten la incorporación de modificaciones a la Historia Clínica una vez se registren y guarden los datos.
En todo caso debe protegerse la reserva de la historia clínica mediante mecanismos que impidan el acceso de personal no autorizado para conocerla y adoptar las medidas tendientes a evitar la destrucción de los registros en forma accidental o provocada.
Los prestadores de servicios de salud deben permitir la identificación del personal responsable de los datos consignados, mediante códigos, indicadores u otros medios que reemplacen la firma y sello de las historias en medios físicos, de forma que se establezca con exactitud quien realizó los registros, la hora y fecha del registro."

Por su parte, la resolución 2003 de 2014, "Por la cual se definen los procedimientos y condiciones de inscripción de los Prestadores de Servicios de Salud y de habilitación de servicios de salud", en el numeral 3.2.6 para Historia clínica y Registros establece como conceptos de verificación, entre otros los siguientes:

*"**Consentimiento informado**: Es la aceptación libre, voluntaria y consciente de un paciente o usuario, manifestada en el pleno uso de sus facultades después de recibir la información adecuada, para que tenga lugar un acto asistencial. Para efectos del estándar de historia clínica es el documento que se produce luego de la aceptación en las condiciones descritas. En caso que el paciente no cuente con sus facultades plenas, la aceptación del acto médico la hará el familiar, allegado o representante que sea responsable del paciente.*
***Sistema de Información Clínico**: Es todo sistema utilizado para generar, enviar, recibir, archivar o procesar de cualquier forma mensajes de datos y que haya sido creado para la producción, recepción, distribución, consulta, organización, custodia, conservación, recuperación y disposición final de cualquier elemento constitutivo de la Historia Clínica.*
***Firma Electrónica**: Son los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en el mensaje de datos."*

De otro lado, en el estándar de historia clínica y registros, de esta resolución se define:

"El uso de medios electrónicos para la gestión de las historias clínicas, debe garantizar la confidencialidad y seguridad, así como el carácter permanente de registrar en ella y en otros registros asistenciales, sin que se puedan modificar los datos una vez se guarden los registros."
(...)
"Las historias clínicas y/o registros asistenciales:
*Deben diligenciarse en forma clara, legible, sin tachones, enmendaduras, intercalaciones, sin dejar espacios en blanco y sin utilizar siglas. **Cada anotación debe llevar la fecha y hora en la que se realiza, con el nombre completo y firma del autor de la misma**.* (Resaltado fuera de texto)

Por su parte, el literal c) del artículo 2 de la la Ley 527 de 1999[2], en cuanto a la firma digital se refiere, la define como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje, permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación.

Así mismo, el artículo 28 de la ley 527 precitada, referente a los atributos de la firma digital, consagró:

[2] "Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones". Reglamentada por el Decreto 1747 de 2000, el cual define lo relacionado con las entidades de certificación, los certificados, las firmas digitales y los requisitos que deben cumplir las entidades de certificación cerradas y abiertas.

"Artículo 28. ATRIBUTOS JURIDICOS DE UNA FIRMA DIGITAL. Cuando una firma digital haya sido fijada en un mensaje de datos se presume que el suscriptor de aquella tenía la intención de acreditar ese mensaje de datos y de ser vinculado con el contenido del mismo.

Parágrafo. El uso de una firma digital tendrá la misma fuerza y efectos que el uso de una firma manuscrita, si aquélla incorpora los siguientes atributos:

1. Es única a la persona que la usa.
2. Es susceptible de ser verificada.
3. Está bajo el control exclusivo de la persona que la usa.
4. Está ligada a la información o mensaje, de tal manera que si éstos son cambiados, la firma digital es invalidada.
5. Está conforme a las reglamentaciones adoptadas por el Gobierno Nacional. (Subrayas y negrillas fuera de texto).

Adicionalmente, el Decreto 1074 de 2015[3], en lo concerniente a la firma electrónica define:

*"Artículo 2.2.2.47.1. **Definiciones.** Para los fines del presente capítulo se entenderá por:*
1. Acuerdo sobre el uso del mecanismo de firma electrónica: Acuerdo de voluntades mediante el cual se estipulan las condiciones legales y técnicas a las cuales se ajustarán las partes para realizar comunicaciones, efectuar transacciones, crear documentos electrónicos o cualquier otra actividad mediante el uso del intercambio electrónico de datos.
2. Datos de creación de la firma electrónica: Datos únicos y personalísimos, que el firmante utiliza para firmar.
3. Firma electrónica. Métodos tales como, códigos, contraseñas, datos biométricos, o claves criptográficas privadas, que permite identificar a una persona, en relación con un mensaje de datos, siempre y cuando el mismo sea confiable y apropiado respecto de los fines para los que se utiliza la firma, atendidas todas las circunstancias del caso, así como cualquier acuerdo pertinente.
4. Firmante. Persona que posee los datos de creación de la firma y que actúa en nombre propio o por cuenta de la persona a la que representa.

***Artículo 2.2.2.47.2. Neutralidad tecnológica e igualdad de tratamiento de las tecnologías para la firma electrónica.** Ninguna de las disposiciones del presente capítulo será aplicada de modo que excluya, restrinja o prive de efecto jurídico cualquier método, procedimiento, dispositivo o tecnología para crear una firma electrónica que cumpla los requisitos señalados en el artículo 7° de la Ley 527 de 1999.*

(Decreto 2364 de 2012, art. 2)

***Artículo 2.2.2.47.3. Cumplimiento del requisito de firma.** Cuando se exija la firma de una persona, ese requisito quedará cumplido en relación con un mensaje de datos si se utiliza una firma electrónica que, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo aplicable, sea tan confiable como apropiada para los fines con los cuales se generó o comunicó ese mensaje.*

(Decreto 2364 de 2012, art. 3)

***Artículo 2.2.2.47.4. Confiabilidad de la firma electrónica.** La firma electrónica se considerará confiable para el propósito por el cual el mensaje de datos fue generado o comunicado si:*

1. Los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante.

[3] Por medio del cual se expide el *Decreto Único* Reglamentario del *Sector Comercio*, Industria y Turismo.

2. Es posible detectar cualquier alteración no autorizada del mensaje de datos, hecha después del momento de la firma.

Parágrafo. *Lo dispuesto anteriormente se entenderá sin perjuicio de la posibilidad de que cualquier persona:*

1. Demuestre de otra manera que la firma electrónica es confiable; o

2. Aduzca pruebas de que una firma electrónica no es confiable.

(Decreto 2364 de 2012, art. 4)

Artículo 2.2.2.47.5. Efectos jurídicos de la firma electrónica. *La firma electrónica tendrá la misma validez y efectos jurídicos que la firma, si aquella cumple con los requisitos establecidos en el artículo 2.2.2.43.3 de este Decreto.*

(Decreto 2364 de 2012, art. 5)

Artículo 2.2.2.47.6. Obligaciones del firmante. *El firmante debe:*

1. Mantener control y custodia sobre los datos de creación de la firma.

2. Actuar con diligencia para evitar la utilización no autorizada de sus datos de creación de la firma.

3. Dar aviso oportuno a cualquier persona que posea, haya recibido o vaya a recibir documentos o mensajes de datos firmados electrónicamente por el firmante, si:

3.1. El firmante sabe que los datos de creación de la firma han quedado en entredicho; o

3.2. Las circunstancias de que tiene conocimiento el firmante dan lugar a un riesgo considerable de que los datos de creación de la firma hayan quedado en entredicho.

Parágrafo. *Se entiende que los datos de creación del firmante han quedado en entredicho cuando estos, entre otras, han sido conocidos ilegalmente por terceros, corren peligro de ser utilizados indebidamente, o el firmante ha perdido el control o custodia sobre los mismos y en general cualquier otra situación que ponga en duda la seguridad de la firma electrónica o que genere reparos sobre la calidad de la misma.*

(Decreto 2364 de 2012, art. 6)

Artículo 2.2.2.47.7. Firma electrónica pactada mediante acuerdo. *Salvo prueba en contrario, se presume que los mecanismos o técnicas de identificación personal o autenticación electrónica según el caso, que acuerden utilizar las partes mediante acuerdo, cumplen los requisitos de firma electrónica.*

Parágrafo. La parte que mediante acuerdo provee los métodos de firma electrónica deberá asegurarse de que sus mecanismos son técnicamente seguros y confiables para el propósito de los mismos. A dicha parte le corresponde probar estos requisitos en caso de que sea necesario.

2.2.2.47.8. Criterios para establecer el grado de seguridad de las firmas electrónicas. Para determinar si los procedimientos, métodos o dispositivos electrónicos que se utilicen como firma electrónica son seguros, y en qué medida lo son, podrán tenerse en cuenta, entre otros, los siguientes factores:

1) El concepto técnico emitido por un perito o un órgano independiente y especializado.

2) La existencia de una auditoría especializada, periódica e independiente sobre los procedimientos, métodos o dispositivos electrónicos que una parte suministra a sus clientes o terceros como mecanismo electrónico de identificación personal."

Expuesto lo anterior se concluye:

Cada anotación de la historia clínica debe tener la fecha y hora en la que se realiza, con el nombre completo y firma del autor de la misma. Para el caso de la firma electrónica y la firma digital (como una especie de la firma electrónica) de las historias generadas en medios electrónicos, además de lo establecido en la resolución 1995 de 1999 y 2003 de 2014 se debe cumplir con lo definido en la Ley 527 de 1999 y las normas que la reglamentan.

Es importante señalar que es el prestador de servicios de salud, el responsable de la generación custodia, conservación y disposición final de la historia clínica de los pacientes que atiende y para ello debe desarrollar los procesos y actividades que se requieran para su manejo y gestión en el medio que defina (papel o electrónico), cumpliendo con las condiciones técnicas establecidas por la normatividad vigente.

A su vez, se hace necesario aclarar que la firma electrónica solo tiene validez cuando el documento conserva su naturaleza de ser electrónico; cuando este se imprime se debería crear los mecanismos para que el destinatario pueda validar la asignación, su autenticidad, la integridad y demás elementos necesarios de la firma electrónica.

Otro mecanismo para asegurar la autenticidad, integridad y demás elementos en un documento electrónico, son los metadatos, los cuales describen el contexto, contenido, y estructura de los documentos, así como su gestión a lo largo del tiempo. En consecuencia, para que un documento electrónico tenga validez se debe contar con lineamientos normalizados que definan la estructura lógica, el contenido, la firma electrónica o digital, los metadatos asociados y el formato del documento electrónico.

Para mayor información sobre la firma electrónica puede acudir a los Ministerios de Tecnologías de información y Comunicaciones y de Comercio Industria y Turismo que son los que regulan la materia.

El anterior concepto tiene los efectos determinados en el artículo 28 de la Ley 1755 de 2015[4].

Cordialmente,

SAMUEL GARCIA DE VARGAS
Director de Prestación de Servicios y Atención Primaria

Elaboró: Sandra G.
Revisó: S. Garcia

SANDRAG:OFICIOS:FIRMA ELECTRONICA CI.docx

[4] "Por medio de la cual se regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo"