



AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS



**SISTEMA DE
INFORMACIÓN**
del Sistema
Nacional
de Salud

"El Sistema de Información del Sistema Nacional de Salud en el siglo XXI"

18/octubre/2017

Ministerio de Sanidad, Servicios Sociales e Igualdad
Salón de Actos Ernest Lluch

PLAN AUDITORÍA DE HOSPITALES, PRINCIPIOS Y DECÁLOGO PARA PROFESIONALES SANITARIOS

Cristina Gómez Piqueras



1. LEGISLACIÓN APLICABLE
2. ANTECEDENTES
3. DESARROLLO DEL PLAN SECTORIAL 2016- 2017
4. CONCLUSIONES GENERALES
5. CONCLUSIONES TRATAMIENTOS DE DATOS CON FINALIDADES ASISTENCIALES
 - MEDIDAS DE SEGURIDAD TRATAMIENTOS AUTOMATIZADOS
 - MEDIDAS DE SEGURIDAD DOCUMENTOS EN PAPEL
6. CONCLUSIONES TRATAMIENTOS DE DATOS CON FINES DE INVESTIGACIÓN
7. DECÁLOGO PROFESIONALES SANITARIOS



Año 1995, Plan Sectorial de Oficio Sector Sanitario.

Deficiencias más notorias:

Incumplimiento del deber de información artículo 5.

No existían procedimientos para atender derechos ARCO

Poca implicación de los órganos directivos de los centros

No estaba establecido el nivel de seguridad de los datos.

No estaban definidos ni documentados los procedimientos en materia de cesión de datos médicos entre centros.

No existía control de salida de datos de los centros.

No estaban definidas correctamente las medidas de seguridad.



Año 2010, Seguimiento mediante cuestionario a Hospitales del Catálogo Nacional, públicos y privados.

Conclusiones :

Notable mejoría respecto de las conclusiones obtenidas en 1995.

Aún así persistían carencias en:

inclusión de cláusulas informativas en recogida de datos.

Carteles informativos sobre protección de datos.

Procedimientos atención derechos ARCO.

Revisiones del documento de seguridad.

Registros de acceso a los datos. En particular en los accesos a las historias clínicas.



PLAN SECTORIAL 2016-2017

Dirigido a Hospitales de titularidad pública con gestión directa o indirecta

Distribuidos por diferentes Comunidades Autónomas

Centrado en las carencias detectadas en las actuaciones del 2010

Tratamientos de datos inspeccionados:

Finalidad Asistencial

Investigación médica



CONCLUSIONES GENERALES

Tendencia a la mejora en el sector en relación al cumplimiento de la normativa de Protección de Datos.

Se debe mejorar:

1. CALIDAD Y CONFIDENCIALIDAD DE LOS DATOS.
2. INFORMACIÓN OFRECIDA A LOS PACIENTES.
3. OBTENCIÓN DE CONSENTIMIENTOS.
4. MEDIDAS DE SEGURIDAD Y CONTROLES DE ACCESO.



FINALIDAD DE ESTE INFORME

- 1.- TERCERA ETAPA EN LA EVALUACIÓN PERMANENTE DEL SECTOR SANITARIO.
- 2.- ELEMENTO DE REFLEXIÓN PARA LA MEJORA EN EL TRATAMIENTO DE LOS DATOS EN EL SECTOR SANITARIO.
- 3.- HERRAMIENTA BÁSICA PARA LA PLENA ADAPTACIÓN AL RGPD (MAYO DE 2018).
- 4.- LA AGPD AL SERVICIO DEL SECTOR SANITARIO.



CONCLUSIONES PARA TRATAMIENTOS CON FINES ASISTENCIALES (1)

1. CALIDAD DE DATOS : casos de suplantación de identidad en identificación de pacientes.
2. DEBER DE INFORMACIÓN: grandes diferencias entre los centros auditados.
3. DEBER DE SECRETO: compromiso de confidencialidad para el personal con acceso a la información médica.
4. PRESTACIONES DE SERVICIOS: Revisar los contratos con entidades externas que acceden a datos personales



CONCLUSIONES PARA TRATAMIENTOS CON FINES ASISTENCIALES (2)

5. OPOSICION A FACILITAR DATOS : establecer procedimiento para recabar consentimiento si el paciente desea que sea facilitada su presencia y ubicación en el Hospital.

MEDIDAS DE SEGURIDAD TRATAMIENTOS AUTOMATIZADOS

6.REGISTRO DE INCIDENCIAS: no siempre está correctamente implementado. Se deben comprobar los procesos de recuperación de datos.

7.CONTROL DE ACCESO: los facultativos pueden acceder sin restricciones a datos de pacientes no asignados. Establecer alertas de confidencialidad, y limitar acceso a datos no necesarios.



CONCLUSIONES PARA TRATAMIENTOS CON FINES ASISTENCIALES (3)

8. AUTENTICACIÓN DE USUARIOS, deficiencias en algunos Hospitales:

carencia de política de cambio de contraseñas

reiteración ilimitada de intentos de acceso

distribución de contraseñas sin confidencialidad.

9. COPIA DE SEGURIDAD: Se deben conservar en ubicación diferente junto a los procedimientos de recuperación.

10. AUDITORÍA DE SEGURIDAD: Realizarla sobre todos los tratamientos.

11. REGISTRO DE ACCESOS: Habilitarlos y realizar auditorias periódicas.

12. EVITAR ISLAS DE INFORMACIÓN.



CONCLUSIONES PARA TRATAMIENTOS CON FINES ASISTENCIALES (4)

MEDIDAS DE SEGURIDAD DOCUMENTOS EN PAPEL

13. TRASLADO DE DOCUMENTACIÓN MÉDICA: implantar procedimiento para evitar acceso indebido a la Historia Clínica en traslados de pacientes.

14. GESTIÓN Y CUSTODIA DE DOCUMENTOS EN PAPEL:
establecer mecanismos de comprobación de la integridad

numeración de páginas,

índice de contenidos, etc.



INVESTIGACION (1)

INVESTIGACION CLÍNICA → DOS TIPOS :

ENSAYOS CLÍNICOS

Implican tratamientos de datos de salud de los sujetos voluntarios objeto del estudio (sanos o enfermos)

OTROS : ESTUDIOS RETROSPECTIVOS, TESIS, PROYECTOS FIN DE GRADO, ETC

pueden implicar accesos a Historias Clínicas de pacientes de Hospitales.



INVESTIGACION (2)

ENSAYOS CLÍNICOS . Consideraciones previas.

-RD 1090/2015, de 4 de diciembre, por el que se regulan los Ensayos Clínicos con Medicamentos ...

-CODIGO TIPO FARMAINDUSTRIA

Figuras : IP – MONITOR – PROMOTOR

CEIm

Elementos : CRD → DISOCIACION DE LOS DATOS

PROTOCOLO, CI, HIP, SEGURO



INVESTIGACION (3)

CONCLUSIONES ENSAYOS CLÍNICOS

1. Se debe facilitar información completa y clara del art.5 LOPD.
2. Tabla que permite revertir la disociación.

Esta tabla, como cualquier otro fichero, debe ser incluida dentro de la Política de Seguridad del Hospital.

3. Contratos de Ensayos Clínicos.
4. Es necesario implementar un protocolo de custodia de los datos personales de los ensayos, una vez finalizados.



INVESTIGACION (4)

CONCLUSIONES ESTUDIOS RETROSPECTIVOS, TESIS, PROYECTOS FIN DE GRADO, etc.

1. Se debe informar y solicitar el consentimiento de los pacientes.

Cuando no es posible, se debe asegurar el anonimato de los pacientes separando los datos identificativos de los clínicos.

2. Se debe controlar el acceso a las Historias Clínicas para evitar que se consulten sin justificación.



DECÁLOGO PARA PROFESIONALES SANITARIOS

- 1. TRATA LOS DATOS DE LOS PACIENTES COMO QUERRÍAS QUE TRATASEN LOS TUYOS.
- 2. ACCEDE A LOS DATOS PERSONALES SOLO SI ES NECESARIO PARA LA REALIZACIÓN DE TU TRABAJO.
- 3. TUS ACCESOS A LA DOCUMENTACIÓN CLÍNICA QUEDAN REGISTRADOS; SE SABE CUANDO Y A QUÉ HAS ACCEDIDO; LOS ACCESOS SON AUDITADOS POSTERIORMENTE.
- 4. NO INFORMES A TERCEROS SOBRE LA SALUD DE TUS PACIENTES, SALVO QUE HAYAN CONSENTIDO O TENGAS UNA JUSTIFICACIÓN



- 5. CUANDO SALGAS DEL DESPACHO CIERRA LA SESIÓN QUE TIENES ABIERTA EN TU ORDENADOR. NO FACILITES A NADIE TU CLAVE Y CONTRASEÑA.

- 6. NO ENVÍES INFORMACIÓN CON DATOS DE SALUD POR CORREO ELECTRÓNICO O POR CUALQUIER RED PÚBLICA; SI TIENES QUE HACERLO, NO OLVIDES CIFRAR LOS DATOS.

- 7. NO TIRES DOCUMENTOS CON DATOS PERSONALES A LA PAPELERA; DESTRÚYELOS TÚ MISMO O SIGUE EL PROCEDIMIENTO IMPLANTADO EN TU CENTRO.



- 8. CUANDO TERMINE DE PASAR CONSULTA, CIERRA CON LLAVE LOS ARMARIOS O ARCHIVADORES DE DOCUMENTACIÓN CLÍNICA.

- 9. NO DEJES LAS HISTORIAS CLÍNICAS SOBRE LAS MESAS SIN SUPERVISIÓN.

- 10. NO CREES FICHEROS CON DATOS PERSONALES DE PACIENTES, CONSULTA SIEMPRE ANTES CON EL DEPARTAMENTO DE INFORMATICA.



SISTEMA DE
INFORMACIÓN
del Sistema
Nacional
de Salud

AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS



MUCHAS GRACIAS