ASSOCIACIÓ CENTRE D'HIGIENE MENTAL NOU BARRIS

INFORME D'AUDITORIA DE PROTECCIÓ DE DADES DE CARÀCTER PERSONAL

Número de protocol 8.694

ÍNDEX

1. Objectius i contingut

De conformitat amb el que estableix la normativa vigent sobre protecció de dades[1], tots els responsables de fitxer i/o encarregats de tractament que disposin de fitxers automatitzats i no automatitzats que continguin dades de nivell mitjà i/o alt, hauran de sotmetre, de forma biennal, els seus sistemes d'informació i instal·lacions de tractament de dades a una auditoria.

Com a resultat de l'auditoria s'ha elaborat el present informe que dictamina quines deficiències té el sistema i quines són les propostes de millora.

[1] *Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (publicada en el BOE número 298, de 14 de desembre de 1999).*

Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desenvolupament de la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (publicat en el BOE número 17, de 19 de gener de 2008).

Codi tipus de la Unió Catalana d'Hospitals.

2. Metodologia

Per dur a terme l'auditoria s'ha realitzat una revisió in situ de les instal·lacions de tractament de dades i de sistemes d'informació de l'entitat.

Tant la planificació, com el treball de camp d'auditoria, i l'elaboració del present informe han sigut desenvolupats per un equip de persones constituït per professionals qualificats en el camp de la protecció de dades de *Faura- Casas, Auditors- Consultors, S.L.*, treballant de forma simultània els aspectes tècnics i organitzatius de la seguretat, així com també dels legals.

Per dur a terme l'execució de l'encàrrec d'auditar el Centre, s'han efectuat les següents actuacions:

- ✓ Realització de l'auditoria a través d'entrevistes, qüestionaris, recopilació i supervisió de documents, i anàlisi i revisió de les mesures, controls i procediments de l'entitat.

- ✓ Elaboració del present informe d'auditoria.

El treball d'auditoria s'ha desenvolupat complint els terminis pactats, i s'ha dividit en les fases que s'indiquen a continuació:

- ✓ Planificació de les feines: Identificació dels centres de la Entitat i, en el seu cas, encarregats del tractament, objecte i auditoria.
- ✓ Identificació dels interlocutors
- ✓ Recollida de la informació
- ✓ Estudi i anàlisi de la informació
- ✓ Aclariments
- ✓ Lliurament de l'informe provisional
- ✓ Correccions i aclariments sobre l'informe provisional
- ✓ Lliurament de l'informe definitiu

3. Simbologia

En aquest informe s'hi analitzen tots els punts requerits per la normativa de protecció de dades. En cadascun d'aquests punts s'hi descriu quina és la situació actual, és a dir, la situació en el moment de la realització dels treballs de camp de l'auditoria, i quina és l'àrea de millora o salvetat detectada, que s'il·lustra amb la simbologia següent:

Símbol	Significat
▲	*No detectada*, és a dir, la situació actual de l'Entitat compleix la normativa.
●	*Àrea de millora*, és a dir, l'estat de la situació actual requereix ésser completat perquè no s'ajustaria íntegrament a l'establert a la normativa.
▼	*Salvetat*, és a dir, la situació actual incompleix la normativa i ha de ser modificada de forma prioritària segons les recomanacions efectuades en l'Informe.

4. Dades de l'entitat i treballs efectuats

4.1. Dades identificatives.

4.1.1. Dades de l'entitat

Entitat	ASSOCIACIÓ CENTRE HIGIENE MENTAL NOU BARRIS
NIF	G08725665
Domicili	Passeig Valldaura, 214, baixos 08042 - Barcelona

4.1.2. Descripció de la activitat

L'ASSOCIACIÓ CENTRE D'HIGIENE MENTAL NOU BARRIS és una entitat sense ànim de lucre que es dedica a la prestació de serveis de promoció, prevenció, assistència, rehabilitació i reinserció en salut mental. Així mateix, ofereix cobertura residencial (pisos) i gestiona programes de suport a la llar. També pretén treballar en el camp de la inserció laboral de persones amb problemes de salut mental.

Les activitats primordials que es desenvolupen són les següents:

1. L'associació i els equips que gestiona es coordinen amb entitats (veïnals, culturals, familiars i d'usuaris de salut mental), institucions (sanitàries, socials, educatives, justícia, treball) i professionals que tenen a veure amb el fi de l'associació.

2. L'associació realitza formació de salut mental comunitària a metges de família, MIR de psiquiatria, PIR, psicòlegs en formació (màster, pràcticum en psicologia), escoles de treball social i infermeria en salut mental.

3. L'associació té obertes línies d'investigació sobre salut mental comunitària.

4. L'associació col·labora amb organismes públics relacionats amb el fi de l'associació.

4.2. Treballs efectuats.

S'han realitzat els treballs de camp de l'auditoria en els següents centres i serveis de l'Entitat.

- ✓ Arxiu de Documentació Clínica
- ✓ Sistemes d'Informació
- ✓ Recursos Humans
- ✓ Contractació i facturació
- ✓ Comunicació
- ✓ Admissions
- ✓ Direcció assistencial
- ✓ CSMA Nord
- ✓ CSMA Sud

En relació als espais físics, es van revisar els següents:

- ✓ Arxius de Documentació Clínica
- ✓ Sala de CPD
- ✓ Despatx i arxiu de RRHH
- ✓ Àrea i despatx d'admissions
- ✓ Despatx i arxiu de facturació i comptabilitat
- ✓ Consultes assistencials.

4.2.1 Data de realització de l'auditoria

Dies	26 i 27 de juny de 2014

4.2.2. Persones entrevistades i relació de la documentació lliurada a l'auditor

Persones entrevistades per ordre d'intervenció

NÚMERO	PERSONA ENTREVISTADA	ÀREA DE TREBALL
1	Sra. Pilar Escalante	Responsable de Seguretat de l'Entitat.
2	Dra. Paloma Lago	Directora de l'Entitat.
3	Sr. Miguel Moya	Responsable d'Informàtica.
4	Sra. Meritxell Hernández	Responsable d'admissions i LOPD CSMA Nou Barris Sud.
5	Dra. Liliana Elstein	Cap Clínic CSMA Nord.
6	Sra. Ana Ma. Fernández	Responsable d'admissions i LOPD CSMA Nou Barris Nord.
7	Sr. Juan Carlos Valdearcos	Cap d'infermeria.

Relació de la documentació lliurada a l'auditor:

Document
Estatuts i dades de l'Entitat 2014.
Codis d'inscripció dels fitxers.
Documents de Seguretat.
Xarxa informàtica.
Backup Servidors.
Condicions particulars servidors ISalus.
Instal·lació RACK CSMA Nord.
Inventari 2014.
Assetjament professionals.
Avís a los usuaris.
Circular informàtica.
CSM9b-ADM-01-Recepció Pacient.
CSM9b-ADM-03-Atenció telefònica.
Comunicat Eines informàtiques.
MBP personal i col·laboradors.
Document informatiu personal (cessió al registre de professionals sanitaris)
Procediment intern d'accés a la Història Clínica
Protecció de dades administració_08
Recomanacions 2008, 2011 i 2014.
Relació dels usuaris amb accés a dades.
Renuncia al reconeixement mèdic.
Resolució de casos pràctics.
Responsables de protecció de dades 2014.
Model del full d'informació pacient.
Model del full d'informació i compromís empleats.
Model de fitxa de col·laboradors.

Model full de reclamacions.
Model d'enquesta.
Model de sol·licitud primera visita persona diferent de l'Interessat.
Model de sol·licitud i recollida d'informe de l'interessat i de persona diferent de l'interessat.
Model de sol·licitud canvi de terapeuta.
Contractes d'encarregat de tractament.
Llistat de contractes amb proveïdors amb accés i sense accés a dades.
Compromisos de confidencialitat.
Convenis pràcticum amb UB, UAB, Abat Oliva,
Conveni SCS 2013.
Model de procediment de notificació i gestió d'incidències.
Model de registre d'entrades i sortides.
Mostreig del monitor d'auditoria (registre d'accessos).
Models de drets ARCO.
Eines quan es demana l'accés a la HC.
Model d'entrega d'HC.
Informe auditoria LOPD 2008.
Acta de revisió de 2006.

Recol·lecció de les dades:

- ✓ Relació dels fitxers, estructura i contingut
- ✓ Polítiques de seguretat i procediments (registre d'incidències, còpies de seguretat, identificació i autorització, esborrat de suports, xifrat, etc.)
- ✓ Document/s de Seguretat
- ✓ Auditories anteriors
- ✓ Disseny físic i lògic dels sistemes d'informació
- ✓ Relació d'usuaris, accessos autoritzats i funcions
- ✓ Inventari de suports i registre d'entrada i sortida de suports
- ✓ Registre d'accessos i informes de revisió dels mateixos
- ✓ Etc.

5. Anàlisi de les diferents àrees de l'auditoria

I - BLOC GENERAL

5.1. Auditoria.

Base legal: Articles 96 i 110 RD 1720/2007.

Situació actual

L'Associació Centre d'Higiene Mental Nou Barris, en endavant l'Entitat, realitzà la darrera auditoria en matèria de protecció de dades a l'abril de 2008. Tot i que s'indicà que els ha estat impossible efectuar l'auditoria abans, hem de recordar que la normativa preveu, a l'article 96.1 del RD 1720/2007 (RLOPD), la obligació de passar auditories de manera biennal a totes aquelles entitats que tractin dades a partir de nivell mig.

Des de l'Entitat comentaren que les conclusions de l'auditoria anterior van ser analitzades pel Responsable de Seguretat, i que posteriorment van ser elevades al Responsable del Fitxer per tal que adoptés les mesures correctores adequades. Tanmateix no s'ha fet entrega del document en el que es detalla aquesta comunicació ni les decisions preses per tal d'implementar accions de millora vers les salvetats i àrees de millora detectades al 2008.

Salvetat

▼	Salvetat	És necessari que l'Entitat efectuï auditories en matèria de protecció de dades de manera biennal d'acord amb el que estableix la normativa. Cal que l'Entitat procedeixi a elevar les conclusions de la present auditoria al responsable del fitxer a fi de donar solució a les salvetats i àrees de millora detectades.

5.2. Aspectes generals.

Base legal: Articles 79, 80 i 81 RD 1720/2007.

Situació actual

FITXER	CODI	FINALITAT	NIVELL	TRACTAMENT
Fitxer de pacients	2031880119	Registre i seguiment dels serveis assistencials. Facilitar la gestió de la facturació.	Alt	Parcialment Automatitzat
Fitxer de Personal	2031890468	Realització dels processos habituals de recursos humans i pagament de nòmines.	Alt	Parcialment Automatitzat
Fitxer d'Administració	2031890467	Realització dels processos habituals d'administració i gestió de la comptabilitat.	Bàsic	Parcialment Automatitzat

Àrees de millora

▲	No detectada	*Seria recomanable procedir a notificar un fitxer de reclamacions, suggeriments i agraïments, tenint en compte que l'Entitat fa el tractament d'aquest tipus de documentació (a més de tots aquests, fa tractament mitjançant enquestes als usuaris).* *També és necessari que l'Entitat declari un fitxer de recerca, en tant que es pogué comprovar durant els treballs de camp que es desenvolupen projectes d'investigació.* *Així mateix, és necessari que l'Entitat declari un fitxer de prevenció de blanqueig de capitals en tant que es troba subjecta segons la Llei 10/2010 de 28 d'abril, de prevenció de blanqueig de capitals i finançament del terrorisme.*

5.3. Document de seguretat.

Base legal: Articles 88, 95, 105 i 109 RD 1720/2007.

Situació actual

Mesures de seguretat
A. Existeix un document de seguretat per cada fitxer declarat o, per contra, es tracta d'un únic document de seguretat que inclou tots els fitxers declarats per l'entitat amb les especificitats pròpies de cadascun d'ells.
Comentaris: • L'Entitat ha elaborat un document de seguretat (en endavant, DS) per a cadascun dels fitxers declarats davant l'Agència Espanyola de Protecció de Dades (en endavant AEPD), existint també annexes i protocols propis per a cadascun dels fitxers.
B. Àmbit d'aplicació del document amb especificació detallada dels recursos protegits: o Inventari de suports. o Estructura dels fitxers amb dades de caràcter personal i descripció dels sistemes d'informació que els tracten.
Comentaris: • L'Entitat disposa del document *Inventario 2014*, tanmateix aquest no es troba annexat als DDSS. • Tots tres DDSS incorporen l'estructura del fitxer tot detallant el software de gestió per a cadascun d'ells així com el tractament per a les dades en suport paper.
C. Si s'escau, mesures alternatives quan no sigui possible establir sistemes d'obertura mitjançant clau o dispositiu equivalent a les portes dels armaris, arxivadors o

altres elements en què s'emmagatzemin els fitxers no automatitzats amb dades de caràcter personal.

Si s'escau, mesures alternatives quan els armaris, arxivadors o altres elements en què s'emmagatzemin els fitxers no automatitzats amb dades de caràcter personal no es trobin amb àrees en què l'accés estigui protegit amb portes d'accés dotades de sistemes d'obertura mitjançant clau o un altre dispositiu equivalent *(nivell alt)*.

Comentari:

- Cal que es detallin aquestes mesures alternatives de forma més concreta i que es valori en quins casos aquestes poden suposar un major/menor risc per la seguretat de les dades (regular les mesures alternatives pel cas dels arxius d'històries clíniques, on les prestatgeries no disposen de tancament – establir un sistema de control d'accés, per exemple-).

D. Mesures, normes, procediments d'actuació, regles i estàndards encaminats a garantir el nivell de seguretat exigit en el Reglament.

Comentari:

- L'entitat disposa de diversos annexes i protocols que s'adjunten amb el DS.

E. Funcions i obligacions del personal en relació amb el tractament de les dades de caràcter personal incloses en els fitxers.

Comentari:

- Cal que s'incorpori en el circuit de protecció de dades de l'Entitat el Manual de Bones Pràctiques, tot indicant les conseqüències en cas d'incompliment del personal (es pot associar al règim sancionador fixat al Conveni Col·lectiu d'aplicació o a l'Estatut dels Treballadors).

F. Procediment de notificació, gestió i resposta davant les incidències.

Comentaris:

- L'Entitat disposa d'annex a tots els DDSS on es detalla el procediment d'incidències.

G. Procediments de realització de còpies de seguretat i de recuperació de les dades en els fitxers o tractaments automatitzats.

Comentari:

- L'Entitat regula aquest aspecte en els *punts 5.3.3 i 5.2.3* dels DDSS de personal i administració respectivament. També es disposa dels protocols *Planning de Backup de servidores* de l'empresa ASTIM i *Condicions particulars per servidors* de l'empresa ISalus que amplien la informació proporcionada als DDSS. Tanmateix, aquests protocols no es troben annexats als DDSS.

H. Mesures que sigui necessari adoptar per al transport de suports i documents, així com per a la destrucció dels documents i suports o, si s'escau, la reutilització d'aquests últims.

Comentaris:

- Cal que l'Entitat incorpori com annexes als DDSS procediments que estableixin les mesures de seguretat pel transport tant de suports electrònics com de documentació.

- Pel que fa a la destrucció de suports i documentació l'Entitat no disposa de cap document que detalli els procediments de destrucció.

I. La identificació dels fitxers o tractaments que es tractin en concepte d'encarregat de tractament amb referència expressa al contracte o document que reguli les condicions de l'encàrrec, la identificació del responsable i del període de vigència de l'encàrrec, així com també si el tractament es realitza, o no, en els locals del responsable.

Comentari:

- Si bé l'Entitat incorpora mencions sobre aquest aspecte i disposa del document *Llistat proveïdors amb/sense accés a dades de caràcter personal* aquest document no es troba annexat al DS.

J. Quan l'entitat actuï com a encarregat de tractament en els seus propis locals, aliens als del responsable del fitxer, ha de preveure en el document de seguretat oportú la identificació del fitxer o tractament i el seu responsable i les mesures de seguretat a implementar en relació amb el tractament.

Comentari:

- Aquest aspecte no és aplicable ja que l'Entitat no actua com encarregada de tractament de cap altra entitat.

Autoritzacions

K. Autorització per a l'emmagatzematge de dades de caràcter personal en dispositius portàtils (usuaris/perfils d'usuaris i període de validesa). Tractament de dades de caràcter personal en dispositius portàtils que no permetin el xifratge.
Comentari: • Cal que l'Entitat reguli l'ús dels dispositius portàtils al Manual de Bones Pràctiques o protocol annex als DDSS.
L. En relació al tractament de dades de caràcter personal fora dels locals del responsable, cal que hi hagi l'autorització així com també els usuaris/perfils d'usuaris i el període de validesa per a aquest tractament.
Comentari: • Cal que l'Entitat incorpori un document on s'indiqui quins proveïdors disposen d'accés remot (atès que els treballadors no en disposen), així com el període de validesa.
M. Personal autoritzat per concedir, alterar o anul·lar l'accés autoritzat sobre els recursos, de conformitat amb els criteris que estableix el responsable del fitxer.
Comentari: • Cal que l'Entitat elabori i incorpori un protocol en el que s'indiqui el procediment i les persones autoritzades per donar d'alta, modificar i donar de baixa als usuaris del sistema.
N. Personal autoritzat a accedir als llocs on estiguin instal·lats els equips físics que donin suport als sistemes d'informació. Procediment d'accés de persones no autoritzades als espais que contenen dades de caràcter personal.
Comentari: • Aquest aspecte no es troba regulat per part de l'Entitat, cal que s'estableixi als DDSS o document annex quin és el personal autoritzat a l'accés als servidors de l'Entitat.
O. Personal autoritzat a accedir als suports i documents que contenen dades de caràcter personal. Procediment d'accés de persones no autoritzades als espais que contenen dades de caràcter personal.

Comentari: • Tot i que el DS de pacients incorpora la necessitat de determinar un responsable de l'arxiu, l'Entitat no disposa de cap document en el que es detalli el responsable ni quines són les persones autoritzades a accedir a la documentació.
P. Autorització per a les sortides de suports i documents, inclosos els compresos i/ o annexos a un correu electrònic.
Comentari: • Cal que l'Entitat determini aquest aspecte als DDSS o bé que incorpori un protocol en el que es detallin les autoritzacions per a les sortides de suports i documents, així com els arxius adjunts a un correu electrònic.
Q. Personal autoritzat per a la recepció/enviament de dades de caràcter personal *(nivell mitjà i/ o alt)*.
Comentaris: • Cal que l'entitat inclogui en aquest punt sobre quin/s departament/s recau l'autorització, així com les persones autoritzades.
R. Personal autoritzat per a la realització del procediment de recuperació de dades.
Comentari: • Cal que els protocols *Planning de Backup de servidores* i *Condicions particulars per servidors* determinin la persona responsable d'efectuar les còpies de seguretat i les recuperacions de dades.
S. Persones en qui el responsable del fitxer ha delegat les autoritzacions que a ell li corresponen.
Comentar: • Els DDSS, inclouen vàries delegacions essent diferents les persones sobre les que recauen segons la tasca corresponent.
Altres mesures
T. Procediment d'assignació, distribució i emmagatzematge de contrasenyes que en garanteixi la confidencialitat i la integritat.

Comentari:

- Aquest aspecte no consta regulat per part de l'Entitat.

U. Periodicitat de canvi de les contrasenyes d'accés al sistema i a les aplicacions.

Comentari:

- El punt 5.3.2 del DS de pacients (no s'inclou als altres DDSS) menciona que les contrasenyes caducaran als 60 dies. Tanmateix, durant els treballs de camp s'indicà que actualment les contrasenyes caduquen cada 90 dies, de manera que és necessari modificar aquest aspecte del DS. A més, seria convenient incorporar aquesta mesura de seguretat als DDSS de personal i administració.

V. Pel cas que es realitzin proves anteriors a la implantació o modificació dels sistemes d'informació que tractin fitxers amb dades de caràcter personal amb dades reals s'ha d'anotar la seva realització al document de seguretat.

Comentari:

- L'Entitat no desenvolupa proves amb dades reals.

W. Identificació del Responsable de Seguretat *(nivell mitjà i/ o alt).*

Comentari:

- Si bé el DS de pacients al seu punt 5.2.1. determina la figura del Responsable de Seguretat, és necessari establir aquest aspecte al DS de personal, en tant que el fitxer està declarat amb nivell de seguretat alt.

X. Els controls periòdics que s'han realitzat per verificar el compliment del que disposa el document *(nivell mitjà i/ o alt)*.

Comentari:

- Cal que l'Entitat desenvolupi els aspectes incorporats als DDSS i modificar aquells que no s'adaptin a la realitat actual. Així mateix, és necessari procedir a incorporar la revisió i posterior elaboració d'informe vers accessos esdevinguts a les dades.

Àrees de millora

	Àrea de millora	Cal que s'acabin de detallar alguns dels punts comentats en el quadre anterior, així com alguns annexes o protocols. També cal recordar que en tot moment haurà d'estar actualitzat a la realitat de l'entitat.

5.4. Delegació d'autoritzacions.

Base legal: Article 84 RD 1720/2007.

Situació actual

Les autoritzacions que s'atribueixen al responsable del fitxer poden ser delegades en les persones designades en aquest efecte, d'acord amb el que estableix l'article 84 del RD 1720/2007.

En aquest sentit, existeixen algunes delegacions als DDSS com per exemple, els tràmits de legitimació de dades dels pacients a recepció, la legitimació del personal a la responsable d'administració, etc.

Tanmateix, només el *punt 5.2.* del DS de pacients estableix la delegació del Responsable del Fitxer en el Responsable de Seguretat, determinant sobre qui recau aquesta figura (responsable d'administració) i detallant les funcions que aquest té vers el sistema de protecció de dades de l'Entitat. Tot i que aquesta figura està regulada al DS de personal (que és d'aplicació, tenint en compte que el fitxer és de nivell alt) s'ha pogut comprovar que no s'ha designat la persona que desenvoluparà el càrrec.

Àrees de millora

●	Àrea de millora	Cal que l'Entitat determini al DS de personal sobre qui recau la figura del Responsable de Seguretat, doncs aquesta és obligatòria per a tots aquells fitxers a partir de nivell de seguretat mig.

5.5. Tercers.

ENCARREGATS DE TRACTAMENT

Base legal: Article 21 i 82 RD 1720/2007.

Situació actual

Els *punts 5.3.2.* dels DDSS de pacients i personal i 5.2.2. del DS d'administració al seu apartat segon inclouen els proveïdors que tenen accés a les dades del fitxer en qüestió. Així mateix, com s'ha pogut comprovar, l'Entitat disposa d'un llistat amb tots els encarregats de tractament, el qual conté el nom del proveïdor, el servei que presta, els fitxers als quals accedeix per a la prestació del servei, la data del contracte i el període de vigència. Tanmateix, aquest document no es troba annexat al DS.

Es disposa també d'un segon llistat de proveïdors on s'inclouen alguns que no es troben annexats al llistat d'encarregats de tractament.

Un cop revisat el citat llistat d'encarregats de tractament, s'ha realitzat un mostreig, passant a comentar-ne els següents:

ET's DETECTATS	SERVEI PRESTAT	CONTRACTE	COMENTARIS
SERVEIS INFORMÀTICS ISALUS, S.L.	Proveïdor de l'aplicació EKON Salus.	☑	Es disposa de contracte d'acord amb les previsions de l'article 12 de la LOPD però manca preveure el detall de les mesures de seguretat específiques que l'encarregat de tractament adopta respecte les dades de caràcter personal.
ASTIM INFORMÁTICA, S.R.L.L.	Servei de manteniment informàtic.	☒	El contracte facilitat no incorpora cap clàusula relativa al tractament de les dades. Cal que el contracte d'encarregat de tractament inclogui l'autorització per a la subcontractació, donat que ASTIM subcontracta el servei de correu electrònic amb l'empresa ARSYS.
BYTEMASTER SERVICIOS INFORMÁTICOS, S.A.	Instal·lació i manteniment de les infraestructures de telefonia i comunicacions.	☑	El contracte és correcte en els termes establerts per la normativa.

BLÁZQUEZ, PLANAS I ASSOCIATS, S.L	Assessoria en matèria fiscal i comptable.	☑	Es disposa de contracte d'acord amb les previsions de l'article 12 de la LOPD però manca preveure el detall de les mesures de seguretat específiques que l'encarregat de tractament adopta respecte les dades de caràcter personal.
ANTONIO SALVADOR CAÑADAS (ASSESSORIA JURÍDICA VERDÚN)	Assessoria en matèria laboral.	☒	Es tracta d'una clàusula de confidencialitat, no d'un contracte d'encarregat de tractament.
29 ECOLÓGICA, S.L.	Destrucció de documentació.	☑	El contracte és correcte en els termes establerts per la normativa.
FUNDACIÓ HOSPITAL DE DIA NOU BARRIS	Col·laboració per l'hospital de dia. Ús de arxius ubicats a l'hospital de dia per l'emmagatzematge de les HC passives.	☒	No es disposa de contracte d'encarregat de tractament.

Salvetat

▼	Salvetat	Cal tenir signat contracte d'encarregat de tractament amb totes aquelles empreses que accedeixen a dades per a la prestació dels servei objecte de contracte. En el cas d'ASTIM, serà necessari que el contracte incorpori la possibilitat de subcontractació (contracte entre ASTIM i ARSYS). És necessari que els contractes d'encarregat de tractament incorporin les mesures de seguretat a aplicar segons la tipologia de dades a què accedeixen.

PRESTACIONS SENSE ACCÉS A DADES

Base legal: Article 83 RD 1720/2007.

Situació actual

Comentar que dins d'aquest grup es troben tots el proveïdors que, tot i que no han d'accedir a dades de caràcter personal pel tipus de servei que presten, tenen accés a les instal·lacions de l'Entitat.

Després de la revisió dels compromisos facilitats per l'Entitat, s'estableix el següent:

TERCERS SENSE ACCÉS	SERVEI PRESTAT	COMPROMÍS	COMENTARIS
CLECE, S.A.	Serveis de neteja CSMA Nord.	☒	El contracte de serveis no incorpora la clàusula de confidencialitat d'acord amb el que estableix la normativa.
ISS FACILITY SERVICES, S.A.	Serveis de neteja CSMA Sud.	☒	El contracte de serveis no incorpora la clàusula de confidencialitat d'acord amb el que estableix la normativa.
CET APUNTS	Serveis de missatgeria.	☒	La clàusula analitzada és inversa, és a dir, el que s'estableix és una clàusula de confidencialitat de l'Entitat cap a d'apunts, quan hauria de ser al contrari.

S'ha detectat que existeixen alguns acords de confidencialitat que no corresponen, com ara el signat amb l'empresa SEPRA, que desenvolupa el servei de vigilància de la salut (no correspon per considerar que són responsables del fitxer) i amb l'empresa ASTIM, que en ser un encarregat de tractament no s'ha de signar cap clàusula de confidencialitat, ja que aquesta ja es troba inclosa dins del contracte d'encarregat de tractament.

Salvetat

▼	Salvetat	Cal que l'Entitat procedeixi a signar el corresponent acord de confidencialitat amb totes aquelles empreses que prestin serveis sense accedir a dades.

5.6. Legitimació de dades.

Base legal: Articles 5 i 6 LOPD 15/1999.

Situació actual

S'analitza a continuació on s'evidencia la legitimació de les dades *de cada fitxer* de l'entitat:

FITXER	LEGITIMACIÓ	COMENTARIS
Personal	Quan un treballador s'incorpora a l'Entitat, se l'informa sobre el tractament de les dades mitjançant el *Full d'Informació i Confidencialitat de l'empleat*.	El document és correcte en els termes establerts per la normativa, tanmateix, es troba a faltar la determinació de l'adreça de l'Entitat per tal de poder exercir els drets ARCO.
	Pel que fa als estudiants en pràctiques, segons s'indicà durant els treballs de camp, es fa entrega de la *Fitxa de col·laboradors*, on es demanen les dades de l'estudiant i s'annexa el full d'informació i confidencialitat.	Si bé el document incorpora la clàusula d'informació de l'article 5 de la LOPD, manca determinar les dades del responsable del fitxer per tal de poder exercir els drets ARCO.
	En relació a la gestió dels Currículums vitae, l'Entitat comentà que a data d'avui no es guarden els Currículums vitae que arriben directament als centres i que es treballa a partir de convocatòries que ells mateixos publiquen al COMB i COIB.	Tot i que no és necessari informar a aquelles persones que faciliten el seu currículum vitae, sempre que aquests no s'emmagatzemin, es va detectar que tampoc s'informa a aquells que vénen derivats del COMB o COIB i que sí s'inclouen al procés de selecció. En aquest cas, seria convenient que la clàusula anés incorporada a la convocatòria. En el decurs del present informe s'ha facilitat a l'Entitat un model de document per a la legitimació de les dades

		d'aquells candidats que són interessants i dels quals s'emmagatzemarà el seu currículum.
	L'Entitat disposa de dos documents per a la autorització o refús en relació als exàmens de salut laboral. Un és el document elaborat pel propi centre i l'altre és el document facilitat per l'empresa SEPRA, encarregada de PRL i Vigilància de la Salut de l'Entitat. Es confirmà que a data d'avui es fa entrega del document facilitat per l'empresa externa i no l'intern.	Si bé el full informatiu del reconeixement mèdic propi de l'Entitat és correcte, analitzat el document que efectivament s'entrega (de SEPRA) no inclou, la clàusula d'informació i consentiment prevista a l'article 5 de la LOPD.
Pacients	L'Entitat fa entrega del *Full d'Informació i Consentiment* a tots els nous pacients que s'atenen.	El document compleix amb els requeriments establerts per la normativa, tanmateix, s'ha de modificar la determinació del responsable del fitxer, ja que s'indica que és la presidenta de l'Entitat, quan realment el responsable del fitxer és la pròpia entitat, representada per la presidenta.
	Es disposa d'un document *Sol·licitud de primera visita per persones diferents de l'interessat* per aquells casos en que és una tercera persona la que determina la primera visita al centre.	EL document no incorpora la clàusula d'informació seguint les premisses establertes a l'article 5 de la LOPD.
	Quan un pacient sol·licita la còpia d'un informe, es fa entrega del full de *Petició i recollida d'informe assistencial per l'interessat.* Així mateix, es disposa d'un document *Petició i recollida d'informes assistencials per persones diferents de l'interessat,* per aquells casos en que aquests informes o resultats de proves siguin sol·licitats i/o recollits per un tercer.	Cap dels dos documents incorpora la clàusula d'informació d'acord amb les previsions contingudes a l'article 5 de la LOPD.

	L'Entitat dóna la possibilitat de canvi de terapeuta si el pacient ho sol·licita. Per fer aquest canvi es disposa del document *Sol·licitud canvi de terapeuta*.	El document facilitat no incorpora la clàusula d'informació d'acord amb les premisses establertes per l'article 5 de la LOPD.
	L'Entitat disposa del *Full de Reclamacions* i del *Full de suggeriments* per a la gestió d'aquests aspectes de qualitat.	El full de reclamacions incorpora clàusula d'informació de les dades remeses al CatSalut, la qual compleix amb les previsions normatives. El full de suggeriments només indica que el suggeriment pot ser anònim i que en cas de facilitar dades d'identificació, aquestes es sotmetran a la LOPD, sense indicar cap dels aspectes establerts a l'article 5 de la LOPD. L'altra opció és que l'Entitat determini que en tot cas el suggeriment ha de ser anònim. Així no seria necessari incloure la clàusula d'informació.
	Existeix una *Enquesta d'avaluació de la qualitat del servei,* que s'entrega als pacients. Tot i ser en principi anònima, en molts casos els pacients inclouen el seu nom.	El document no incorpora la clàusula d'informació d'acord amb les previsions establertes a l'article 5 de la LOPD. Com s'ha comentat al quadre anterior, es pot indicar de manera expressa que l'enquesta ha de ser anònima.

Àrees de millora

●	Àrea de millora	Veure els comentaris del quadre anterior. *Donat que l'Entitat té accés a la Historia Clínica Compartida de Catalunya (HC3), es recomana que procedeixi a fer una breu menció al full d'informació al pacient sobre la cessió de les dades a l'HC3, així com a la web de l'Entitat quan aquesta es trobi operativa.*

5.7. Drets ARCO.

Base legal: Articles 15-17 LOPD 15/1999.

Situació actual

En el *punt 6* dels DDSS disposen la possibilitat de l'exercici i tutela dels drets dels afectats, i s'indica l'existència dels annexes on es troben els models pel seu exercici. S'han analitzat els models i són correctes, complint amb la normativa de referència, el RD 1720/2007. A més, incorporen indicacions vers el procediment intern a seguir davant d'una sol·licitud de dret ARCO.

Durant els treballs de camp es comprovà que els annexes es troben accessibles a les dues recepcions dels centres, a disposició del personal d'atenció a l'usuari.

Així mateix, l'Entitat disposa de models de resposta a l'exercici dels drets ARCO, on s'estima o es denega l'exercici dels drets, fonamentant la desestimació, si és el cas. Segons indicaren, davant d'una sol·licitud es dóna resposta fent ús d'aquests models i es facilita cita a l'interessat per tal de concretar les seves pretensions.

Com a tònica general, les còpies d'informes no són considerades un dret d'accés tal com preveu l'article 15 de la LOPD. En aquests casos donen resposta dins del termini però no segueixen el procediment establert per a l'exercici dels drets ARCO, existint models paral·lels de sol·licitud de documentació (veure document *Petició i recollida d'informe assistencial per l'interessat)*.

Respecte les sol·licituds de rectificació, cancel·lació i oposició, segons es determinà durant els treballs de camp, no s'han donat casos.

L'Entitat també disposa de models per a l'exercici del dret de queixa d'acord amb les previsions establertes a l'article 19 del Codi Tipus de la Unió Catalana d'Hospitals.

En tots els casos, segons s'indica als protocols i es comprovà durant els treballs de camp, qualsevol sol·licitud de dret ARCO queda degudament registrada en el sí de l'Entitat, anotant-se la sol·licitud a la HC informatitzada.

Àrees de millora

▲	No detectada	*D'acord amb l'article 13 de la Llei 21/2000 de 29 de desembre, sobre els drets d'informació concernent la salut i l'autonomia del pacient, i la documentació clínica, el pacient té dret a accedir a la HC i a obtenir una còpia de les dades que hi figuren; procediment que d'acord amb la definició de l'article 15 LOPD s'ha de tractar com un dret d'accés, seguint els criteris establerts en el RLOPD (es tracti d'un accés parcial – còpia d'un informe- o total – còpia de tota la HC-).*

II - BLOC DE MESURES INFORMÀTIQUES

5.8. Accés a xarxes.

Base legal: Article 85 RD 1720/2007.

Situació actual

L'Entitat disposa del document *Xarxa Informàtica Nord-Sud* on es detalla el sistema de xarxa. Tanmateix, aquest document no es troba annexat als DDSS.

A grans trets, indicar que cada centre disposa del seu servidor propi d'arxius i per a la gestió dels usuaris. És important comentar que des del gener d'enguany, l'Entitat ha procedit a externalitzar l'emmagatzematge de dades del programa assistencial EKON Salus, pel que a data de la present auditoria es disposa de Hosting amb l'empresa ISalus vers les dades de l'aplicació assistencial.

Per a la connexió intercentres es disposa de túnel IPsec punt a punt.

Les connexions es gestionen de manera diferent segons el centre. En el CSMA Nord, es fa a través de fibra òptica. Al CSMA Sud la connexió es fa mitjançant radiofreqüència, proporcionada per l'empresa EURONA.

Cada centre disposa del seu Firewall per a l'accés a internet. En el cas del CSMA Sud, es comentà que la UTM té determinat que en cas de fallida de la radiofreqüència, es posi en funcionament la connexió mitjançant ADSL.

Així mateix, indicar que l'Entitat disposa d'un sistema de carpetes de xarxa on existeixen carpetes departamentals, accessibles d'acord amb els permisos del treballador i carpetes personals dels treballadors. En aquest darrer cas, és important comentar que tots els usuaris poden accedir a les carpetes personals d'altres, però la modificació i eliminació de documents és únicament pel propi usuari.

En relació a la seguretat del sistema, a més dels Firewalls ja citats, es va indicar per part de l'Entitat que es disposa d'antivirus Nod32.

El servei de correu electrònic es troba externalitzat amb l'empresa ARSYS Internet S.L.U. Segons s'indicà durant els treballs de camp, el trànsit de correus electrònics és extern, i tota la gestió es troba relacionada mitjançant Microsoft Exchange.

Tots els treballadors de l'Entitat disposen de correu electrònic personal excepte els col·laboradors (estudiants). Així mateix existeixen adreces de correu genèriques; nord, sud, suport i administració.

Les principals aplicacions detectades durant els treballs de camp en les quals es tracten dades de caràcter personal es detallen a continuació:

APLICACIÓ	UTILITAT
EKON Salus	Aplicació de gestió assistencial.
Aplicació d'Ingressos	BBDD Access per a la gestió de pacients ingressats en aguts.
MICROSOFT EXCHANGE	Gestor del correu electrònic.
MICROSOFT OFFICE	Programes ofimàtics i BBDD d'alguns departaments.

Àrees de millora

▲	No detectada	

5.9. Connexions remotes.

Base legal: Article 86 RD 1720/2007.

Situació actual

Aquest aspecte no es troba regulat per l'Entitat al cap dels seus DDSS ni documents annexes.

Durant els treballs de camp, l'Entitat confirmà que únicament tenen accés remot els proveïdors encarregats de tractament que presten serveis informàtics i els treballadors del departament d'informàtica (suport). Així mateix es va informar que l'accés a l'EKON només es pot efectuar des d'unes IP's determinades.

En tot cas, es comentà que els accessos remots s'efectuen des d'una VPN i que per a cada accés VPN és necessari autoritzar l'accés, i aquest requereix dos nivells de validació, el de l'usuari específic (existent de manera prèvia) i la contrasenya existent per a cada accés (es dóna en el moment d'accedir).

Comentar que, els professionals que disposen de correu electrònic, tenen la possibilitat d'accedir al seu compte de correu a través de Webmail, el qual es gestiona mitjançant https.

Es pot afirmar que les mesures de seguretat emprades per al treball fora del lloc on s'ubiquen els fitxers garanteixen el nivell de seguretat corresponent al tipus de fitxer tractat.

Àrees de millora

▲	No detectada	*Cal que l'Entitat reguli el procediment per a l'accés remot i incorpori un llistat on s'identifiqui les persones o empreses que disposen d'aquest tipus d'accés i el seu període de vigència.*

5.10. Transmissions per xarxes de telecomunicacions.

Base legal: Article 104 RD 1720/2007.

Situació actual

El *punt 5.7.* del DS de pacients nomena els mecanismes de seguretat en la transmissió de la informació, on es citen breument els mecanismes per a la transmissió en paper i es remet al document *Manual d'usuari - Encriptació de documents*, per tal de determinar les transmissions per xarxes de telecomunicacions.

Així mateix, quan l'Entitat incorpori el Manual de Bones Pràctiques, inclourà indicacions més extenses al respecte, com ara l'obligatorietat de dissociació per enviar dades mitjançant correu electrònic o fax. A data d'avui, aquestes previsions es troben regulades de manera general al document *Protecció de Dades (recomanacions 2014)*.

Comentar que, tenint en compte que l'Entitat té contractat el servei de correu electrònic amb l'empresa ARSYS i que tots els enviaments viatgen externament, haurem d'aplicar les mateixes mesures de seguretat pel trànsit de correus electrònics entre els treballadors, és a dir, que tots els enviaments que es facin internament entre treballadors i que incorporin dades de nivell alt hauran de fer-se dissociats o utilitzant mecanisme de xifratge segur.

Dit això, s'ha analitzat el *Manual d'Usuari – Encriptació de documents* el qual detalla les mesures de seguretat vers la transmissió de dades per xarxes de telecomunicacions, tot indicant que els enviaments per correu electrònic o fax hauran de ser sempre dissociats. Tanmateix, es considera que incloure el número de HC és correcte, quan, segons el criteri de les Agències de Protecció de Dades (catalana i espanyola) el número de HC és dada identificativa, de manera que és necessari modificar aquest aspecte.

Durant els treballs de camp es pogué comprovar que tot el personal del centre es troba molt conscienciat sobre la prohibició d'enviar correus electrònics o fax amb dades de salut dels pacients. Indicaren que tots els informes s'entreguen al propi pacient en mà o s'envien per missatger a la persona que ho ha de rebre.

A banda d'aquestes mesures per aquells casos d'urgent necessitat, l'Entitat cità que es disposa del WinZip pel xifratge dels correus electrònics. La versió del programa és la 9.0 SR-1,que, d'acord amb les interpretacions de l'APDCAT al seu dictamen CNS 12/2013, no incorpora les mesures de seguretat necessàries pel compliment de la normativa.

Respecte l'ús del fax, s'indicà durant els treballs de camp que el seu ús és molt reduït, limitant-se a casos de sol·licituds urgents. En tot cas, indicaren que si s'ha de fer un enviament mitjançant fax, es fa de manera dissociada. En quant a les sol·licituds de jutjats, si bé es reben per fax, van comentar que l'enviament es fa mitjançant carta certificada a través de l'empresa de missatgeria Unipost.

Àrees de millora

●	Àrea de millora	D'acord amb el dictamen CNS 12/2013 de l'APDCAT, les aplicacions que s'utilitzin per l'encriptació de documents hauran d'incorporar algoritme de xifratge AES-128 o 256, per poder considerar-lo segur. En el cas del Winzip, les versions que incorporen aquest algoritme són la versió 17 i posteriors.

5.11. Control d'accés.

Base legal: Articles 89.1, 91 i RD 1720/2007.

Situació actual

L'Entitat disposa del llistat d'usuaris per a cadascun dels fitxers als *punts 5.3.1* dels DDSS de pacients i personal i *5.2.1.* del DS d'administració. Pel fitxer de pacients, es disposa d'un document *Relació d'usuaris amb accés a dades* el qual incorpora un llistat de tot el personal, el càrrec, el centre on desenvolupa la seva feina, les aplicacions a les que té accés i el tipus d'accés que disposa. Manca, però, nomenar l'existència d'aquest document al DS de pacients.

No existeix cap annex ni document que determini el procediment a seguir per a la creació, modificació i baixa d'usuaris.

Tanmateix, durant els treballs de camp s'indicà per part de l'Entitat que el procediment d'alta d'un nou usuari ve donat per part de direcció o administració (segons sigui personal laboral o personal en pràctiques) que informa de la nova incorporació al responsable d'informàtica. Aquest s'encarrega de gestionar l'alta a les aplicacions i comunica a ASTIM Informàtica l'existència d'un nou usuari, detallant les característiques i accessos que ha de disposar, essent l'empresa ASTIM Informàtica, l'encarregada de donar d'alta el nou usuari al sistema.

S'indicà que el procediment de baixa és el mateix, essent sempre comunicada la baixa per part de direcció general o direcció d'administració al responsable informàtic i encarregant-se aquest de remetre aquesta informació a ASTIM informàtica per tal de desactivar l'usuari, doncs, segons indicaren, no donen de baixa cap usuari del sistema, sinó que el desactiven.

El procediment seguit per a l'alta d'usuaris implica que aquests només puguin accedir a les dades i recursos que necessiten per al desenvolupament de les seves funcions, atès que s'organitzen d'acord amb el departament on treballen i la categoria professional.

Volíem comentar però, que la pràctica que es duu a terme vers les carpetes personals, les quals són accessibles a tots els usuaris, no compleix amb la normativa, ja que en tant que carpetes privades o d'usuari, l'única persona que hauria d'accedir hauria de ser el propi usuari i l'administrador del sistema per possibles incidències.

Els mecanismes que impedeixen que els usuaris accedeixin a més dades de les autoritzades és l'ús de contrasenyes. L'Entitat ha fet entrega d'un mostreig del llistat/relació d'usuaris donats d'alta al sistema *Relació d'usuaris amb accés a dades* el qual determina de manera clara els perfils i tipus d'accés que disposa cada usuari.

Àrees de millora

▲	No detectada	*És necessari que l'Entitat valori la possibilitat que les carpetes siguin únicament d'accés a l'usuari concret, sense que els usuaris puguin veure la informació continguda a les carpetes personals d'altres.* *Cal que l'Entitat elabori un protocol on es plasmi el procediment per a les*

		altes, modificacions i baixes d'usuaris. *Cal annexar al DS de pacients el document Relació d'usuaris amb accés a dades.*

5.12. Identificació i autenticació d'usuaris.

Base legal: Articles 93 i 98 RD 1720/2007.

Situació actual

El *punt 5.3.2.* apartat 2 del DS de pacients determina, entre d'altres aspectes que la mesura de prevenció per evitar que les dades siguin visualitzades per tercers és l'ús de contrasenyes.

Segons s'indicà en el decurs dels treballs de camp, la identificació de qualsevol usuari per accedir al sistema i les aplicacions és inequívoca i personalitzada.

La identificació dels treballadors es duu a terme a través del nom punt i el primer cognom. Les principals aplicacions estan relacionades amb els usuaris del directori actiu.

En relació a les contrasenyes, han de complir amb les següents directrius:

- Han de tenir un mínim de 6 caràcters.
- Han d'incorporar lletres, números i símbols, i es recomana que s'alternin majúscules i minúscules.
- Caduquen de manera automàtica cada 90 dies tant del sistema com de les aplicacions.
- Si bé no existeix bloqueig per intents d'accés reiterats no autoritzats al sistema. Sí que existeix vers l'EKON, que es bloqueja després de 5 intents d'accés erronis.
- Es pogué comprovar que el sistema no es bloqueja de manera automàtica quan es troba en desús.

  Tanmateix, s'insisteix per part del responsable d'informàtica de la necessitat de bloquejar-ho manualment fins que s'instauri el bloqueig automàtic en totes les màquines.
- El sistema disposa de memòria de les darreres 25 contrasenyes utilitzades.

Finalment, respecte el procediment emmagatzematge de *passwords*, afirmaren que mentre estan vigents, s'emmagatzemen de forma inintel·ligible i el departament d'informàtica només pot establir-ne una de nova en cas d'oblit de l'usuari, que aquest haurà de modificar en el primer accés que hi faci. Aquest procediment garanteix la seva confidencialitat i integritat.

Àrees de millora

▲	No detectada	*Cal que l'Entitat incorpori la possibilitat de bloqueig dels equips davant el desús per part de l'usuari.*

5.13. Registre d'accessos.

Base legal: Article 103 RD 1720/2007.

Situació actual

Els *punt 5.8.2.* del DS de pacients i *5.6.1* del DS de personal preveuen l'existència del registre d'accessos, tot indicant que el sistema informàtic que conté les dades de caràcter personal registra qualsevol accés a les dades del fitxer informatitzat, incorporant tots els paràmetres establerts per la normativa.

L'Entitat ha fet entrega d'un mostreig del registre d'accessos de l'EKON en tant que aplicació de gestió assistencial amb dades de nivell alt. Analitzat el citat mostreig, s'ha pogut comprovar que el programa incorpora tots els paràmetres que estableix la normativa.

Tanmateix, d'acord amb el que s'indicà per part de l'Entitat durant els treballs de camp, actualment no revisa mensualment la informació de control registrada i per tant no elaboren el preceptiu informe de revisió mensual del sistema. Només es fa revisió dels accessos quan es donen incidències.

Salvetat

▼	Salvetat	És necessari que el Responsable de Seguretat o persona delegada revisi mensualment i elabori els preceptius informes en els que hi consti una revisió dels accessos esdevinguts i dels problemes detectats.

5.14. Còpies de seguretat.

Base legal: Articles 94, 102 i 112 RD 1720/2007

Situació actual

El procediment de còpies de seguretat el trobem citat al *punt 5.3.3.* del DS de personal i 5.2.3 del DS d'administració, sense que hi hagi cap menció al DS de pacients. Aquesta informació està ampliada amb els protocols *Planning de Backup de servidors* de l'empresa ASTIM Informàtica i *Annex Condicions particulars servidors* de l'empresa ISalus.

A grans trets, d'acord amb el que es manifestà per part de l'Entitat durant els treballs de camp, el procediment de còpies és el següent:

S'efectuen còpies de seguretat diàries i mensuals de manera automàtica.

Les còpies diàries incorporen totes les dades del servidor principal d'arxius i el servidor SQL del CSMA Sud i del servidor CSMA Nord. Aquestes còpies dels dos servidors d'arxius nord i sud són incrementals i s'actualitzen cada 3 hores de dilluns a divendres. La còpia del servidor SQL es duu a terme dos cops al dia.

La còpia mensual és una còpia de seguretat completa i s'efectua el dia 1 de cada mes.

En relació a l'externalització les còpies diàries es compilen i s'envien als servidors de Backup de l'empresa ASTIM Informàtica mitjançant arxiu FTP, quedant allà emmagatzemada per poder restaurar en cas de necessitat.

D'acord amb el que s'indicà durant els treballs de cap, sovint es fan recuperacions de dades per necessitats dels treballadors però no es deixa constància documental d'aquestes restauracions en un informe semestral, d'acord amb el que estableix la normativa.

En relació a les còpies de seguretat de l'EKON, el protocol de ISalus determina que cada dia a les 2 de la matinada es fa la còpia de totes les dades de l'aplicació i que es gestionen mitjançant un espai FTP, procedint a fer una còpia mensual en un disc dur extern (custodiat a les oficines de ISalus).

Cada 6 mesos es fa una restauració completa del sistema, verificant el correcte funcionament de les còpies. S'ha fet entrega de l'informe de verificació. Tanmateix aquest és de data 29/07/2014, corroborant que fins llavors no s'ha dut a terme l'elaboració del preceptiu informe semestral d'aquestes recuperacions.

El procés de còpies garanteix que la informació no és intel·ligible ni manipulada per tercers.

Àrees de millora

▲	No detectada	*Donat que s'ha començat a fer l'informe semestral arrel de la present auditoria, cal que l'Entitat es marqui avisos per fer la sol·licitud a ISalus de rebre els informes semestrals de verificació de còpies i restauracions efectuades.*

5.15. Fitxers temporals suport automatitzat.

Base legal: Article 87 RD 1720/2007.

Situació actual

Els equips tenen el disc dur habilitat per emmagatzemar documentació. A més, analitzant els diferents documents s'ha comprovat que l'Entitat no disposa de cap document on es reguli la obligatorietat de destrucció dels documents que s'elaboren amb caràcter temporal.

Durant els treballs de camp, es detectà que els fitxers temporals que es generen són bàsicament les agendes dels professionals, que imprimeix administració per tal de preparar, si escau la HC del pacient.

Segons s'indicà per part del responsable d'informàtica, l'extracció de l'EKON únicament es pot fer mitjançant impressions de pantalles ja que el personal no disposa d'aquest permís. Únicament el responsable de sistemes d'informació pot desenvolupar llistats de pacients extrets de l'aplicació assistencial, doncs és l'únic que disposa de permisos per fer-ho.

No es detectaren gaires arxius temporals, doncs en general tota la gestió s'efectua directament a l'EKON. Tanmateix, es pogué comprovar que tot el personal està conscienciat vers la necessitat d'eliminar aquest tipus d'arxius un cop finalitzi la necessitat per la qual van ser creats.

Àrees de millora

▲	No detectada	*Es recomana fer recordatoris a tots els treballadors sobre la gestió i destrucció dels fitxers temporals.*

5.16. Registre d'entrades i sortides de suports automatitzats.

Base legal: Article 97 RD 1720/ 2007.

Situació actual

Comentar que és el DS de pacients al *punt 5.8.1*. l'únic que preveu l'existència d'aquest registre respecte les entrades i sortides, i únicament ho preveu per a les entrades i sortides de HC en format paper. Tot i això, es disposa de l'annex 6 que incorpora el model per dur a terme el registre d'entrades i sortides tant en format paper com en suport informàtic. S'ha revisat el model i aquest compleix amb la normativa incorporant tots els paràmetres que estableix el RD 1720/2007.

Durant els treballs de camp no es detectaren sortides de suports informàtics atès que l'Entitat no proporciona dispositius d'emmagatzematge als treballadors, i els dispositius personals es troben prohibits. A més, l'únic supòsit en que es podria donar moviments seria amb les còpies de seguretat, que, tenint en compte que la transmissió és telemàtica als servidors de ASTIM, no existeix trasllat en suports físics automatitzats.

Àrees de millora

▲	No detectada	

III- BLOC DE MESURES FÍSIQUES O DOCUMENTALS

5.17. Dispositius portàtils, inventari, etiquetatge, xifrat i destrucció de suports i documents.

Base legal: Articles 86, 92, 101 i 112 RD 1720/ 2007.

Situació actual

L'Entitat no estableix cap directriu vers l'ús dels USB si bé comentaren que el seu ús es troba totalment prohibit, no s'ha determinat aquest aspecte als DDSS ni s'ha elaborat cap protocol en el qual es reguli l'ús dels dispositius d'emmagatzematge externs.

En relació als ordinadors portàtils comentaren que únicament en disposen d'un i que en cap cas incorporen dades de caràcter personal, doncs només es fa servir per fer presentacions als propis centres de l'Entitat.

Només direcció general, direcció d'administració i personal de suport disposen de smartphones. L'Entitat no fa ús de tauletes o altres dispositius electrònics.

Es constatà durant els treballs de camp que tots els equips estan degudament etiquetats i inventariats per l'empresa ASTIM i que es disposa d'un inventari de suports que dóna informació sobre tots aquests dispositius (centre, ubicació, identificació del suport, data d'adquisició).

Pel que fa a la reparació dels equips, segons informà l'Entitat durant els treballs de camp, normalment és l'empresa ASTIM Serveis Informàtics els que efectuen les reparacions in situ. Quan és necessari traslladar l'equip, ASTIM s'encarrega de fer el formateig per tal que els dispositiu no incorpori dades.

Respecte la destrucció dels dispositius prèviament a donar de baixa el dispositiu es formateja el disc dur. En general, l'equip no es destrueix, es guarda en el magatzem per tal de poder recuperar una peça si és necessari.

La destrucció del paper, en general, es fa a través de destructores, distribuïdes pels diferents departaments. Tanmateix, quan hi ha un gran volum de paper per destruir, es desa en contenidors oberts i es truca a l'empresa ECOLÒGICA, que s'encarrega de fer la destrucció emetent certificat (durant els treballs de camp es pogué revisar un dels certificats). Tanmateix, no existeix un protocol específic que reguli el procediment de destrucció de documentació.

Àrees de millora

●	Àrea de millora	Cal que l'Entitat reguli l'ús dels USB a un protocol o al futur Manual de Bones pràctiques de manera detallada. Així mateix, convé elaborar un protocol per a la regulació del sistema de destrucció de suports i documentació. Els contenidors utilitzats pel desament de paper pendent de destrucció i transport de documentació amb dades de caràcter personal han de disposar d'un mecanisme que n'obstaculitzi l'obertura per evitar accessos indeguts.

5.18. Control d'accés.

Base legal: Articles 99, 107, 108 i 111 RD 1720/ 2007.

Situació actual

Trobem que l'Entitat ha regulat al punt d'estructura del fitxer i al punt 5.5 dels DDSS de pacients i personal, la descripció de les mesures de seguretat que garanteixen el control d'accés a les àrees físiques de la documentació i la sala de servidors. Així mateix, aquesta informació es troba ampliada al DS de pacients on es regula de forma més concreta els criteris de seguretat vers les HC (concretament al *punt 5.4* del DS).

Respecte l'accés als arxiu d'històries clíniques actives s'indica que està restringit mitjançant portes que disposen de tancament amb clau, dins de les recepcions dels centres. Tanmateix, segons es comprovà durant els treballs de camp, les prestatgeries no disposen de mecanisme de tancament. Durant el dia, que hi ha personal del departament, l'accés es lliure al personal assistencial de l'Entitat, però els treballadors del departament s'encarreguen de controlar qui accedeix. Fora de l'horari d'arxiu, l'accés es troba restringit i controlat. S'indica al DS de pacients que en aquests casos, l'accés haurà de ser anotat a un registre.

Per la seva banda, per a l'arxiu de documentació clínica passiva, trobem varis arxius; en primer lloc, al CSMA Sud disposen d'una sala únicament destinada a l'arxiu que disposa de clau. Al CSMA Nord, degut al volum de HC passives, s'ha procedit a comptar amb un espai destinat a l'arxiu al centre de la Fundació Hospital de Dia de Nou Barris. Tot i que no es revisà la sala durant els treballs de camp, segons es comentà, si bé disposa de mecanisme de tancament, les prestatgeries es troben obertes. A més, es comparteix arxiu amb la Fundació Nou Barris, sense que hi hagi cap mecanisme que n'obstaculitzi l'accés a les HC de l'Entitat.

Les reclamacions, suggeriments i agraïments, es troben custodiats als despatxos d'administració, els quals incorporen tancament mitjançant clau. Així mateix, els armaris on s'emmagatzema la informació també es troben tancats amb clau.

Respecte els expedients de personal, es troben tots al despatx de la directora d'administració, el qual disposa de mecanisme de tancament i en armaris que també disposen de tancament mitjançant clau.

Vers el fitxer d'administració, que incorpora dades de nivell bàsic, comentar que el seus arxius de documentació física es troben emmagatzemats al despatx de la Directora administrativa o despatxos d'administració, essent sales que disposen de totes les mesures de seguretat, no accessibles a persones no autoritzades.

En relació amb el CPD, hem de dir que en el cas del CSMA Sud es troba al mateix arxiu de documentació clínica dins d'un rack que disposa de clau. Al CSMA Nord, el servidor està ubicat al despatx d'administració, dins d'un rack que també disposa de tancament mitjançant clau.

Salvetat

▼	Salvetat	És necessari que els armaris o arxivadors que incorporin dades de nivell alt estiguin dotats de sistemes d'obertura mitjançant una clau o un altre dispositiu equivalent. Caldria procedir a regular en un protocol el procediment per a l'accés als arxius de documentació clínica. És necessari que l'Entitat disposi d'una sala únicament destinada a la custòdia del CPD, sense que hi pugui accedir personal no relacionat amb el manteniment de la màquina.

5.19. Registre d'accessos.

Base legal: Article 113 RD 1720/2007.

Situació actual

Si bé el DS de l'Entitat estableix l'existència del registre d'accessos vers el fitxers informatitzats, no s'ha trobat cap menció respecte l'accés a la documentació física, únicament es determina que qualsevol accés a l'arxiu de HC quedarà anotat en un registre creat a l'efecte, però no s'estableix cap previsió respecte els paràmetres que haurà de contenir el registre.

Tanmateix, com ja s'ha comentat, l'arxiu físic es troba custodiat pel personal d'administració, que controla tant la preparació de les HC per les visites, com qualsevol petició d'HC.

Àrees de millora

●	Àrea de millora	Tenint en compte que a la sala de custòdia de documentació hi tenen accés múltiples usuaris, és necessari portar un control que permeti identificar els accessos esdevinguts.

5.20. Criteris d'arxiu.

Base legal: Articles 106 RD 1720/2007.

Situació actual

Els DDSS, al punt d'estructura dels fitxers determinen l'existència d'arxius en format paper per a la documentació de cada fitxer. Tanmateix, no es detalla quins són els criteris d'arxiu que s'utilitzen.

Fitxer de Pacients: Existeixen dos arxius actius, un per a cada centre. Tots dos arxius es troben dins les recepcions dels centres, en una sala annexa. L'ordre de tots dos arxius és mitjançant número d'HC seqüencial.

Respecte l'arxiu passiu, al CSMA Sud existeix un petit arxiu per aquelles HC de pacients que fa més d'un any que es van visitar i dels que han estat èxitus. Està endreçat per número de HC seqüencial.

Al CSMA Nord no es disposa d'arxiu definitiu, trobant-se les HC passives al mateix arxiu actiu però separades de les actives.

Així mateix, com ja s'ha comentat, existeix un arxiu general a l'edifici de la Fundació Hospital de dia Nou Barris, i l'ordre que es segueix és el mateix que per a la resta d'arxius de documentació clínica, per número de HC seqüencial.

Fitxer de Personal: Únicament existeix un arxiu per a tots els treballadors de l'Entitat, tant actius com passius, ubicat al despatx de la directora d'administració al CSMA Sud, es distribueixen en A-Z. Es diferencien entre actiu i passiu i l'ordre de l'arxiu és mitjançant data d'antiguitat del treballador.

Fitxer d'Administració: L'arxiu relatiu al fitxer d'administració es troba emmagatzemat al despatx de la directora d'administració i està endreçat per data de factura. Per aquelles factures anteriors als darrers dos exercicis econòmics, es traslladen a l'arxiu de la Fundació Hospital de dia Nou Barris, amb el mateix criteri d'arxiu, per data de factura.

Àrees de millora

▲	No detectada	*Cal que l'Entitat actualitzi la informació del DS de pacients, tot incorporant l'existència de l'arxiu passiu a la Fundació Hospital de Dia Nou Barris.*

5.21. Entrades i sortides de documents.

Base legal: Articles 97 i 114 RD 1720/2007.

Situació actual

Comentar que el DS de pacients és l'únic que incorpora aquest aspecte al *punt 5.8.1.,* on es preveu l'existència d'aquest registre respecte les entrades i sortides d'històries clíniques.

Indicà l'Entitat que totes les sortides d'informes o altra documentació clínica es facilita directament al pacient de manera que la sortida de documentació amb dades de nivell alt és mínima.

El supòsit en el que surt documentació amb dades de salut dels pacients la trobem quan hi ha sol·licitud d'històries clíniques per part dels jutjats. Com ja s'ha dit, en aquests casos, l'enviament es fa mitjançant Unipost per correu certificat. S'inclou un document fora de l'expedient on el jutjat segella l'entrada. Així, es disposa d'un registre indirecte de la sortida de documentació clínica.

Tanmateix, en el decurs dels treballs de camp es van detectar alguns moviments de documentació que no es registren, tal com es detalla a continuació:

- No es registra l'entrada dels resultats dels exàmens de salut laboral que envia l'empresa SEPRA. Així mateix, no es registra la sortida d'aquesta documentació quan s'entrega al treballador.

- Tot i que el trasllat de les HC a l'arxiu passiu existent a la Fundació Hospital de dia Nou Barris s'efectua per part del personal del centre, és necessari que es registri la sortida de dita documentació mèdica.

Àrea de millora

●	Àrea de millora	Cal que l'Entitat incorpori i faci ús d'un registre d'entrades i sortides de per a tots aquells casos en que hi hagi moviment de documentació amb dades de nivell alt. El registre ha de permetre conèixer, directa o indirectament dels següents camps: - Tipus de document, data i hora d'enviament. - Emissor i receptor - Núm. de documents inclosos a l'enviament / recepció - Persona responsable del lliurament / recepció

5.22. Fitxers temporals.

Base legal: Articles 87 i 112 RD 1720/2007.

Situació actual

Com ja s'ha comentat anteriorment al *punt 5.15* d'aquest Informe, a data de la present auditoria l'Entitat no disposa de cap protocol que estableixi l'obligatorietat d'eliminar els documents creats de forma paral·lela o temporal.

En qualsevol cas, com a document habitual que es genera i que té caràcter temporal es va detectar les agendes dels facultatius. Segons va indicar el personal d'administració, s'imprimeixen per tal de preparar les HC dels pacients que seran visitats cada dia. Tanmateix, d'acord amb el que van indicar, al final del dia, un cop verificat que ha tornat totes les HC, es procedeix a eliminar aquests documents mitjançant les destructores.

Àrees de millora

▲	No detectada	*Cal que l'Entitat incorpori als DDSS o document annex les directrius vers la creació de documents temporals i la obligació tant de custodia mentre són necessaris com de destrucció un cop acabi la finalitat per la qual van ser creats.*

IV- BLOC DE MESURES ORGANITZATIVES

5.23. Registre d'incidències.

Base legal: Articles 90 i 100 RD 1720/2007.

Situació actual

Els *punts 5.8.3.* del DS de pacients, 5.6.2 del DS de personal i 5.4.1 del DS d'administració determina la definició d'incidència, el contingut que ha d'incorporar la notificació i l'existència d'un registre d'incidències custodiat pel responsable de seguretat. Així mateix, s'incorpora com *annex 7 Procediment de gestió i registre d'incidències* que facilita el model de notificació amb detall del procediment de notificació, gestió i resposta de les incidències.

S'ha detectat que hi ha diferències importants en les regulacions que fan els DDSS vers aquesta qüestió, com exemple, en relació a la custòdia del registre; mentre el DS de pacients determina que està en poder del Responsable de Seguretat, el DS de personal esmenta que ho custòdia el responsable del fitxer, representat per la directora del centre.

Durant els treballs de camp es comentà que el procediment de gestió d'incidències que es segueix en l'actualitat dista molt de l'establert a l'annex 7.

En cas d'incidència, el treballador envia un correu electrònic a suport indicant la incidència i aquest decideix la gestió que es farà. Segons indicaren, normalment la resolució d'incidències informàtiques les efectua l'empresa ASTIM informàtica.

S'ha facilitat per part de l'Entitat un mostreig de notificacions d'incidències esdevingudes d'ençà la darrera auditoria, el que ha permès confirmar la informació facilitada durant els treballs de camp, verificant que, efectivament, el personal de l'associació envia correu electrònic a suport per tal de notificar la incidència.

En relació al registre d'incidències es comentà per part de l'Entitat que no existeix un registre d'acord amb l'annex 7, sinó que els correus electrònics que es reben s'emmagatzemen en una bústia específica (suport) i que és el que realment es fa servir com a registre de les incidències esdevingudes, s'ha pogut comprovar que existeix una bústia específica per a la comunicació i gestió d'incidències.

Àrees de millora

▲	No detectada	*Cal que el procediment de notificació d'incidències plasmat a l'annex 7 s'adapti realment al procediment que l'Entitat duu a terme en la gestió de les incidències esdevingudes.*

5.24. Difusió de funcions i obligacions.

Base legal: Article 89.2 RD 1720/2007.

Situació actual

Si bé existeixen circulars disperses on es nomenen algunes obligacions vers la protecció de dades (circular informàtica i recomanacions 2014), l'Entitat està en procés d'elaboració del Manual de Bones Pràctiques. En cap dels documents citats l'Entitat incorpora les conseqüències pels treballadors en cas d'incompliment de les funcions i obligacions encomanades.

Finalment en relació a la formació en matèria de protecció de dades, indicar que, si bé habitualment s'intenta acudir a les sessions del Codi Tipus, a nivell intern no s'ha efectuat, d'ençà la darrera auditoria, cap sessió formativa en matèria de Protecció de dades.

Àrees de millora

●	Àrea de millora	El Manual de Bones Pràctiques haurà d'incorporar a més de les obligacions dels treballadors en relació a les dades titularitat de l'Entitat, les conseqüències pel personal en cas d'incompliment de les funcions i obligacions establertes. És necessari que l'Entitat efectuï, de manera periòdica, formació als treballadors en matèria de protecció de dades.

6. CONCLUSIONS

Inspeccionats tots els punts determinats pel Reglament de desenvolupament de la Llei orgànica 15/1999, de protecció de dades de caràcter personal, havent- se dut a terme les actuacions a les diferents dependències de l'entitat, realitzades les entrevistes amb els corresponents responsables d'àrea, havent-se valorat la documentació aportada, avaluats els sistemes de tractament de la informació, l'equip auditor detecta que les àrees de millora i salvetats, de conformitat amb l'establert al RDLOPD, són:

ÀREES DE MILLORA
I- BLOC GENERAL
5.3. Document de seguretat.
5.4. Delegació d'autoritzacions
5.6. Legitimació de dades.
II- BLOC DE MESURES INFORMÀTIQUES
5.10. Transmissions per xarxes de telecomunicacions.
III- BLOC DE MESURES FÍSIQUES O DOCUMENTALS
5.17. Dispositius portàtils, inventari, etiquetatge, xifrat i destrucció de suports i documents.
5.19. Registre d'accessos.
5.21. Registre d'entrades i sortides de documentació.
IV- BLOC DE MESURES ORGANITZATIVES
5.24. Difusió de funcions i obligacions.

SALVETATS
I- BLOC GENERAL
5.1. Auditoria.
5.5. Tercers.
II- BLOC DE MESURES INFORMÀTIQUES

5.13 Registre d'accessos.
III- BLOC DE MESURES FÍSIQUES O DOCUMENTALS
5.18. Control d'accés.

Barcelona, 15 de juliol de 2014.

Pere Ruiz Espinós

- Soci -