**ASSOCIACIÓ CENTRE D'HIGIENE MENTAL NOU BARRIS**

# INFORME D'AUDITORIA DE PROTECCIÓ DE DADES DE CARÀCTER PERSONAL

*Número de Protocol* 9.964

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

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

Per portar a terme l'execució de l'encàrrec, 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 dels treballs: identificació del/s centre/s de l'entitat i, en el seu cas, encarregat/s de tractament, objecte d'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. Dades de l'entitat i treballs efectuats

## 3.1. Dades identificatives.

### 3.1.1. Dades entitat

| | |
|---|---|
| Entitat | ASSOCIACIÓ CENTRE D' HIGIENE MENTAL NOU BARRIS |
| NIF | G-08725665 |
| Domicili | Passeig Valldaura, 214, baixos.<br><br>08042 Barcelona |

### 3.1.2. Descripció de l'activitat

L' ASSOCIACIÓ CENTRE D'HIGIENE MENTAL NOU BARRIS és una entitat sense ànim de lucre, creada l'any 1995.

L'objectiu de la seva creació era desenvolupar i promoure activitats dins de l'àmbit de la salut mental.

L' Entitat per tal d'assolir l'objectiu realitza les següents activitats, entre d'altres:

a) L' Associació i els equips que gestiona es coordinen amb entitats ja siguin culturals, familiars, etc. i professionals relacions amb el fi de l' Associació.
b) L' associació realitza formació de salut mental comunitària a metges de família, MIR Psiquiatria, PIR, psicòlegs en formació, escoles de Treball Social , etc.
c) L' associació te línies obertes d'investigació.
d) L'associació col·labora amb organismes públics relacions en l'àmbit d'actuació de l' Entitat.

## 3.2. Treballs efectuats.

S'han realitzat els treballs de camp de l'auditoria en els diversos serveis i àrees de l' Associació Centre d' Higiene Mental Nou Barris:

En el CSM Nou Barris Sud, els treballs de camp s'han realitzat en les següents àrees:

- Àrea de Sistemes d' Informació.
- Àrea d' Arxiu de Documentació Clínica.
- Àrea d'Admissions.
- Àrea de Recursos Humans i Salut Laboral.
- Àrea d'Administració.
- Àrea de Comunicació.
- Àrea Assistencial.

En el CSM Nou Barris Nord, s'han visitat les següents àrees:

- Àrea Assistencial.
- Àrea d'Admissions.
- Àrea d' Arxiu de Documentació Clínica.

Pel que fa a espais físics, a més de les àrees indicades, s'han revisat els següents: arxius, despatxos, consultes, controls d'infermeria i CPD.

### 3.2.1. Data de realització de l'auditoria

| | |
|---|---|
| **Dies** | 13 i 14 de setembre de 2016 |

### 3.2.2. 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 | Cap d'administració i Gestió dels Centres de Salut Mental Nou Barris Nord i Sud |
| **2** | Sr. Miquel Moya | Responsable d'informàtica |
| **3** | Sra. Meritxell Hernández | Administració CSM Sud |
| **4** | Sra. Gemma Carbó | Administració CSM Sud |
| **5** | Sr. Paloma Lago | Directora dels Centres de Salut Mental Nou Barris Nord i Sud |
| **6** | Dr. Francisco Porras | Cap clínic CSM |
| **7** | Dra. Lliliana Elstein | Cap clínic CSM Nord |
| **8** | Sra. Ana María Fernández | Administració CSM Nord |

Relació de la documentació lliurada a l'auditor:

| Document |
|---|
| Organigrama |

| |
|---|
| Estatuts |
| Cartes de l'Agència Espanyola de Protecció de Dades amb els codis d'inscripció dels fitxers |
| Documents de seguretat |
| Esquema xarxa informàtica |
| Document d'usuaris, permisos i inventari |
| Altes i baixes d'usuaris |
| Relació d'usuaris autoritzats d'accés a les dades |
| Registre contractes |
| Protocol xifrat arxius |
| Annexes documentació informació (pacients, treballadors, etc...) |
| Protocol exercici drets ARCO |
| Contractes |
| Model de clàusula sobre la prestació de serveis sense accés a dades |
| Procediment de gestió i registre d'incidències |
| Taula d'incidències informàtiques |
| Sol·licitud i recollida d'HC per persona diferent a l'interessat |
| Acta Comitè de Direcció i Ordre del dia |
| Certificat de document entregat |
| Sol·licitud primera visita de persona diferent a l'interessat |
| Acta de tancament d'auditoria |
| Quadre d'accions de millora |

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.

# 4. 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. |

# 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, va realitzar la darrera auditoria en matèria de protecció de dades el juliol de 2014, complint amb les previsions legalment establertes en l'article 96 del RDLOPD, segons el que es preveu el criteri de biennalitat en la realització d'auditories.

Des de l'Entitat comentaren que la Comissió de Protecció de Dades va procedir a celebrar una reunió per comentar i difondre les conclusions de l'auditoria anterior, elevant-se al Responsable del Fitxer per tal que adoptés les mesures correctores adequades. L'Entitat aportà acta de tancament d'auditoria celebrada en data de 9 de novembre de 2015. Així mateix s'ha aportat una taula d'accions de millora en la que consta la valoració de les diferents recomanacions de l'informe d'auditoria anterior.

#### Àrees de millora

| | | |
|---|---|---|
| ▲ | No detectada | *És aconsellable que en d'altres ocasions l'acta tancament es celebri en una data més propera a la finalització de l'informe, per exemple dintre dels següents 6 mesos.* |

## 5.2. Aspectes generals.

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

### Situació actual

L'entitat ha fet entrega de les cartes de l'Agència Espanyola de Protecció de Dades (en endavant AEPD) amb els codis dels fitxers.

| FITXER | CODI | FINALITAT | NIVELL | TRACTAMENT |
|---|---|---|---|---|
| Pacients | 2031880119 | Prevenció i assistència sanitària, facturació dels serveis prestats així com també finalitats de docència i investigació. | Alt | Mixt |
| Personal | 2031890468 | Gestió de recursos humans, formació, prevenció de riscos laborals i control presencial dels treballadors. | Alt | Mixt |
| Administració | 2031890467 | Realitzar els processos habituals d'administració i comptabilitat. | Baix | Mixt |

### Àrees de millora

| | | |
|---|---|---|
| ● | Àrea de millora | Com ja va quedar constància en l'anterior auditoria degut a l'explotació interna de les dades en qüestió cal inscriure un fitxer de queixes i suggeriments.<br><br>Així mateix, en el cas que hagi rebut alguna donació, caldrà notificar la creació del fitxer de prevenció de blanqueig de capitals, atès que l' Entitat esta subjecte a la Llei 10/2010, de 28 d'abril. |

## 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 (DS) 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:<br>• L'entitat disposa d'un DS per cadascun dels fitxers que té inscrits: fitxer de pacients , fitxer de personal i fitxer d'administració.<br>• L' última versió del DS de pacients és el 20 de juny de 2016, la del DS de personal és el 5 de juliol de 2016, així com l'ultima versió del DS d'administració és el 8 d'agost de 2016. |
| **B.** Àmbit d'aplicació del document amb especificació detallada dels recursos protegits:<br>o Inventari de suports.<br>o Estructura dels fitxers amb dades de caràcter personal i descripció dels sistemes d'informació que els tracten. |
| Comentaris:<br>• En el DS de pacients es troba incorporat un inventari de suport.<br>• En el punt 2 de tots els DS es descriu l'estructura dels fitxers, exposant-se la descripció dels sistemes d'informació que els tracten. |

**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:

- Seria convenient determinar mesures alternatives pel que fa a l' accés de l' arxiu del CSM Sud on es troben les HC actives ja que no es disposa de control d'accés

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

Comentaris:

- L'Entitat disposa de diferents protocols i procediments com per exemple d'altes i baixes d'usuaris, per la gestió d'incidències, etc.
- Així mateix, els DS de l'Entitat disposen de diferents annexes amb formularis i indicacions d'actuacions, com pot ser per l'exercici dels drets ARCO.

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

Comentari:

- Tant en el DS de pacients com en el DS de personal es troba el Manual de Bones Pràctiques.

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

Comentari:

- Consta en el punt 5.8 del DS de pacients, en el punt 5.6.2 del DS de personal i en el punt 5.4.1 del DS d'administració. L' Entitat disposa i té annexat en

els diferents DS un document on especifica el procediment de notificació, gestió i resposta d'incidències.

- Hi ha diferències en els diferents DS pel que fa a la persona que ha de custodiar el registre. Pel que fa a la persona responsable de reflectir les incidències en el registre en el DS és el responsable de seguretat mentre que en el DS de pacients es disposa que ho serà la persona que detecti la incidència.

  Pel que fa a la custòdia d'aquest registre d'incidències, en el DS d'administració i personal s'estableix que la persona responsable de custodiar-lo serà el responsable del fitxer i en el DS de pacients s'indica que ho farà el responsable de seguretat.

- Així mateix, a l' annex *Procediment de gestió i registre d'incidències* de tots els DS hi trobem un model de registre d'incidència.

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

Comentari:

- Es troba regulat en el punt "Procediment, periodicitat i custòdia per a la realització de còpies de seguretat" del DS de Personal i Administració. Manca regular-ho en el DS de Pacients.

- En cap dels DS es fa menció a les còpies de recuperació.

**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 incorporar les mesures necessàries per al transport de suports i documents. S'hi fa una petita menció en el Manual de Bones Pràctiques.

- No es preveu en cap dels DS les mesures de seguretat relatives a la destrucció i reutilització de documents i/o suport

**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. |
| Comentaris:<br><br>• En el DS d'administració trobem el llistat incomplet en el punt *Descripció de les obligacions dels usuaris i tercers amb accés a les dades*. En el DS de pacients es troba un llistat de proveïdors que tenen accés a les dades, però sense els paràmetres que indica la llei. Així mateix ho trobem en el DS de Personal.<br><br>• Hi ha un llistat de proveïdors amb accés a dades sense els paràmetres que indica la llei, tot i això no esta inclòs en el 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 els documents de seguretat oportuns la identificació del fitxer o tractament i el seu responsable i les mesures de seguretat a implementar en relació amb el tractament. |
| Comentari:<br><br>• No queda constància que actuï com a encarregat de tractament de terceres entitats. |
| **Autoritzacions** |
| **K.** Autorització per a l'emmagatzematge de dades de caràcter personal en dispositius portàtils (usuaris/ perfils d'usuaris i període de validesa).<br><br>Tractament de dades de caràcter personal en dispositius portàtils que no permetin el xifratge. |
| Comentari:<br><br>• En el Manual de Bones Pràctiques es regula l'ús dels dispositius d'USB. Durant els treballs de camp s'indica que els ports estan habilitats i que el personal pot utilitzar USB. Cal adaptar el manual de bones pràctiques a la realitat de l' Entitat i, si cal, autoritzar al personal corresponent per la utilització d'aquests dispositius. |
| **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:<br><br>• Manca incloure-ho als tres DS. |
| **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. |
| Comentaris:<br><br>• No es preveu el personal autoritzat per concedir, alterar o anul·lar l'accés sobre els recursos. Es recomana incloure-ho en un protocol. |
| **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:<br><br>• Aquests consten en el punts 5.5 *Control i Limitació d'accés físic*, del DS del fitxer de pacients i personal. |
| **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:<br><br>• En el punt 5.2.1 del DS d' administració i el 5.3.1 de pacients i personal es preveu un llistat de persones autoritzades a l'accés a dades. |
| **P.** Autorització per a les sortides de suports i documents, inclosos els compresos i/ o annexos a un correu electrònic. |
| Comentaris:<br><br>• No es preveu en cap punt les autoritzacions per a les sortides de suports i documents, així com els annexos a un correu electrònic. Cal detallar-ho per exemple en forma de protocol. |

| |
|---|
| **Q.** Personal autoritzat per a la recepció/ enviament de dades de caràcter personal *(nivell mitjà i/ o alt).* |
| Comentari:<br>• Manca detallar en els DS d pacients i personal el personal autoritzat per a la recepció/enviament de dades de caràcter personal. |
| **R.** Personal autoritzat per a la realització del procediment de recuperació de dades. |
| Comentari:<br>• En cap dels DS s'especifica ni el procediment de recuperació de dades ni la persona responsable de dur-la a terme. |
| **S.** Persones en qui el responsable del fitxer ha delegat les autoritzacions que a ell li corresponen. |
| Comentaris:<br>• Veure punt 5.4 del present informe. |
| **Altres mesures** |
| **T.** Procediment d'assignació, distribució i emmagatzematge de contrasenyes que en garanteixi la confidencialitat i la integritat. |
| Comentari:<br>• En cap dels DS es preveu el procediment d'assignació, distribució i emmagatzematge de contrasenyes. |
| **U.** Periodicitat de canvi de les contrasenyes d'accés al sistema i a les aplicacions. |

| |
|---|
| Comentari:<br><br>• El punt 5.3.2 *Descripció de les obligacions dels usuaris i tercers amb accés a les dades* del DS de pacients es determina la caducitat de les contrasenyes. Manca detallar-ho en el DS d'administració i de personal. Tampoc es preveu en cap annexa. |
| **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:<br><br>• No consta que es realitzin proves amb dades reals. |
| **W.** Identificació del responsable de seguretat *(nivell mitjà i/ o alt).* |
| Comentari:<br><br>• Aquest consta en el punt *El Responsable de Seguretat*, en el punt 5.2 del DS de pacients i personal. |
| **X.** Els controls periòdics que s'han realitzat per verificar el compliment del que disposa el document *(nivell mitjà i/ o alt)*. |
| Comentari:<br><br>El DS de pacients i personal s' estableix que una de les funcions del responsable de seguretat és coordinador i controlar el compliment de les mesures de seguretat. Així mateix s'indica que haurà de revisar cada mes la informació de control registrada i el funcionament del sistema amb el que elaborarà un informe de les revisions realitzades i els problemes detectats. |

## Àrea de millora

| | | |
|---|---|---|
|  | Àrea de millora | Cal que s'acabin de detallar els punts comentats en el quadre anterior i que l' Entitat adapti els diferents DS a la seva realitat. |

## 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, algunes de les quals consten detallades en el Document de Seguretat.

En el punt *5.2 Responsable de seguretat* del DS de personal i pacients s'estableix com a responsable de seguretat el/la Cap d' Administració i Gestió.

# Àrees de millora

| | | |
|---|---|---|
| ▲ | No detectada | |

## 5.5. Tercers.

## ENCARREGATS DE TRACTAMENT

***Base legal: Article 82 RD 1720/2007.***

### Situació actual

L'entitat disposa d'un llistat, gestionat pel Responsable de Seguretat, on consten identificats els tercers encarregats de tractament, tanmateix aquest és incomplet.

S'ha realitzat un mostreig dels contractes facilitats per l'Entitat, passant a analitzar-ne els següents:

| ET's DETECTATS | SERVEI PRESTAT | CONTRACTE | COMENTARIS |
|---|---|---|---|
| **ASTIM INFORMÀTICA, SR.L.L.** | Servei de manteniment informàtic | ☑ | Es disposa del contracte d'encarregat de tractament d'acord amb les previsions de l'article 12 de la LOPD. Cal especificar el nivell de seguretat de les dades a les quals tindrà accés per tal de determinar les mesures de seguretat que l'encarregat de tractament esta obligat a implantar. |
| **BLÀZQUEZ PLANAS I ASSOACIATS, S.L.** | Assessoria en matèria fiscal i comptable | ☑ | Es disposa del contracte d'encarregat de tractament d'acord amb les previsions de l'article 12 de la LOPD, si bé cal detallar les mesures de seguretat aplicables. |
| **ANTONIO SALVADOR CAÑADAS (ASESORÍA JURÍDICA VERDÚN)** | Assessoria en matèria laboral | ☒ | No s'ha aportat el contracte. |
| **FUNDACIÓ HOSPITAL DE DIA NOU BARRIS** | Col·laboració per l'hospital de Dia. | ☑ | Es disposa del contracte d'encarregat de tractament d'acord amb les previsions de l'article 12 de la LOPD, si bé cal detallar les mesures de seguretat aplicables. |
| **COMTEC QUALITY S.A** | Funcionament de la certificació ISO 9001 | ☑ | No es disposa del contracte d'encarregat de tractament, |

| | | | |
|---|---|---|---|
| | | | amb les previsions establertes en l'article 12 de la LOPD. |

## Salvetat

| | | |
|---|---|---|
| ▼ | Salvetat | S'ha de signar un contracte d'encarregat de tractament amb tots els tercers que per la prestació d'un servei hagin d'accedir a dades de caràcter personal dels fitxers de l'entitat.<br><br>En els contractes d'encarregat de tractament formalitzat, hauran de constar, d'acord amb l'article 12 de la LOPD, el fitxer al que s'accedirà en motiu de la prestació del servei, i les mesures de seguretat a aplicar d'acord amb el nivell de seguretat del fitxer.<br><br>D'altra banda, el llistat en el que es relacionin els proveïdors que presten serveis a l'Entitat, hauran de constar les següents dades: nom del proveïdor, servei que es presta, fitxer al que s'accedeix, data de signatura del contracte, vigència i subcontractació, si s'escau. |

# PRESTACIONS SENSE ACCÉS A DADES

***Base legal: Article 83 RD 1720/2007.***

## Situació actual

Del mostreig efectuat en destaquem els següents tercers sense accés a dades:

| TERCERS SENSE ACCÉS | SERVEI PRESTAT | COMPROMÍS | COMENTARIS |
|---|---|---|---|
| **CLECE, S.A** | Neteja | ☑ | El contracte presentat incorpora una clàusula de compromís de confidencialitat, d'acord amb l'article 83 del RDLOPD. |
| **ISS FACILITY SERVICE, S.A** | Neteja | ☑ | El contracte presentat no incorpora la clàusula de compromís de confidencialitat d'acord amb l'article 83 del RLOPD. En el contracte aportat es regula que el proveïdor podrà incorporar les dades de l' Entitat als seus fitxers, així com cedir les dades dins de l' Espai Econòmic Europeu o fora. |
| **CET APUNTS** | Servei de missatgeria | ☒ | No s'ha aportat. |

## Salvetat

| | | |
|---|---|---|
| ▼ | Salvetat | S'ha de signar un compromís de confidencialitat amb tots els tercers que si bé per la prestació del servei no han d'accedir a dades, sí que accedeixen a les instal·lacions de l'entitat. |

## 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 dels fitxers de l'entitat:

| FITXER | LEGITIMACIÓ | COMENTARIS |
|---|---|---|
| **Pacients** | L'Entitat en el CSM Nou Barris Nord i en el CSM Nou Barris Sud entrega el document d'informació i consentiment als pacients que venen derivats al centre per primer cop. | El contingut del document és correcte d'acord amb l'article 5 de la LOPD. Tot i això, s'indica que únicament ha d'informar-se del responsable del fitxer o tractament, per tant no cal informar de qui és la representant o directora. |
| | S'indicà que es remeten SMS recordatoris de primeres visites als pacients, en els que es fa constar: nom del centre, data i hora de la visita així com el professional. | El contingut del SMS és correcte si tenim en compte els criteris que es van establir en a la Quarta Sessió Oberta Anual que va realitzar l' Agència Espanyola de Protecció de Dades. |
| | Els pacients que necessitin una copia de l'informe assistencial el poden sol·licitar omplint el document " Petició d'informe assistencial per l'interessat". | Aquest document és correcte d'acord amb l'article 5 de la LOPD. |
| **Personal** | Al treballador nou se li entrega el document "Full d'informació i confidencialitat de l' empleat" | Aquest document és correcte d'acord amb l'article 5 de la LOPD. Tot i així és important indicar que és erroni identificar a la Directora com a responsable del fitxer, ja que aquest és la pròpia Entitat. |

| | | |
|---|---|---|
| | Als estudiants en pràctiques també se'ls hi entrega un document on s'informa del tractament de dades. | Aquest document no és correcte d'acord amb l'article 5 de la LOPD.<br><br>Cal incorporar la direcció del responsable del fitxer per poder exercir els drets ARCO, així com especificar la finalitat del tractament de dades. Es recomanable modificar el nom del document ja que la fitxa és del col·laborador però el compromís al deure de secret és de voluntaris. |
| | L' Entitat fa entrega als treballadors del document en el qual han d'acceptar o rebutjar l'examen de salut laboral. | Aquest document és correcte d'acord amb l'article 5 de la LOPD. |

## Àrees de millora

| | | |
|---|---|---|
| ● | Àrea de millora | Veure comentaris del quadre anterior. |

## 5.7. Drets ARCO.

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

# Situació actual

El procediment d'exercici del dret d'accés, rectificació i cancel·lació es troba esmentat en el punt 6 *Exercici i tutela dels drets del afectat* de tots els DS. Així mateix, l'Entitat presenta un Protocol de drets ARCO on es troben annexats els formularis d'exercici d'aquests.

Des del departament d'Administració i Admissions comentaren que per exercir qualsevol d'aquests drets, el circuit és el següent:

- S'indica al pacient que es dirigeixi al taulell de recepció del centre ja que és on es troben els formularis. En aquest punt se li fa entrega del formulari corresponent. Aquesta petició queda registrada amb el full d'entrega que se li facilita al titular juntament amb la fotocopia del DNI. Finalment, se l'indica que en 10 dies rebrà resposta tant si la sol·licitud és positiva o negativa.
- En el cas que l'interessat hagi de recollir documentació, en el moment de la recollida ha de firmar un document conforme s'ha realitzat la recollida.
- En el CSM Nou Barris Nord quan un pacient vol exercitar un dret ARCO se'l cita amb la Directora.

Cal indicar que l'Entitat no considera un dret d'accés la petició d'informes, havent-se d'omplir el formulari específic de petició d'informes.

Respecte als drets d'oposició, de rectificació, i cancel·lació, no consta que s'hagi rebut cap sol·licitud al respecte des de la darrera auditoria.

Pel que fa als terminis, durant els treballs de camp s'observa que una sol·licitud de dret d'accés rebuda en el CSM Nou Barris Sud va ser presentada el dia 28 de maig de 2015 i es va donar resposta el 3 de juny de 2015, per tant es compleix el termini legal indicat per la llei.

En el CSM Nou Barris Nord es va presentar una sol·licitud de dret d'accés el 21 d'abril de 2015. No consta quin dia es a donar resposta, donant-hi accés a les dades el dia 4 de juliol.

L' Entitat també recull reclamacions i suggeriments mitjançant els formularis de la Generalitat de Catalunya.

# Àrea de millora

| | | |
|---|---|---|
| ● | Àrea de millora | Cal deixar constància de quin dia es dóna resposta al pacient per tal que l' Entitat pugui disposar d'un correcte control dels terminis de resposta indicats per la llei.<br><br>En el document de "Protocol d'exercici del dret d'accés a la informació, rectificació i cancel·lació", no es fa referència al |

| | | |
|---|---|---|
| | | procediment d'exercici dels drets ARCO.<br><br>Es recomana que s'acabi de completar el Protocol de drets ARCO, procedint a detallar el procediment d'exercici d'aquests drets, tal com s'ha dit anteriorment.<br><br>Cal tenir present que tant si s'exercita un dret d'accés parcial de l'historia clínica (petició d'informe) o bé total, s'hauran de considerar com un dret d'accés, atès els criteris establerts en la Llei Orgànica 15/1999, de 13 de desembre. |

# II - BLOC DE MESURES INFORMÀTIQUES

## 5.8. Accés a xarxes.

***Base legal: Article 85 RD 1720/2007.***

## Situació actual

L'Entitat disposa de dos servidors en els quals s'allotgen les dades SQL Server, l'accés a la xarxa i les del correu electrònic, estant els dos centres connectats mitjançant ADSL. En quan a la seguretat dels equips, aquests tenen instal·lat l'antivirus NOD32 i a més disposen de dos *Firewall,* un a CSM Nou Barris Nord i un altre al CSM Nou Barris Sud. També disposen de dos SAIS, un a cada centre, per tal de donar resposta en cas de fallida d'electricitat.

Pel que fa al sistema de carpetes, l'Entitat presenta un sistema de carpetes en xarxa departamentals. L'accés a les carpetes és limitat segons la categoria professional, limitant-se l'accés al personal de cada departament. També hi trobem carpetes en xarxa personals dels professionals, on tots els professionals poden accedir-hi però no es pot modificar ni esborrar els contingut de la carpeta. Així mateix, no hi ha la percepció de que existeixin carpetes personals locals on es guardi informació al disc dur de l'equip.

Pel que fa al correu electrònic, s'utilitza Microsoft Exchange. Cada treballador té una compte de correu electrònic personalitzat. Tot i així, existeixen algunes comptes genèriques però que únicament serveixen per rebre informació, no per enviar ni contestar.

Les aplicacions detectades durant el treball de camp utilitzades per l'entitat i en les quals es tracten dades de caràcter personal es detallen a continuació:

| APLICACIÓ | UTILITAT |
|---|---|
| EKON | Gestió assistencial |
| Control de derivacions i ingressos | Gestió de derivacions d'usuaris |
| Outlook | Correu electrònic |
| Microsoft Office | Programes ofimàtics |

## Àrea de millora

| | | |
|---|---|---|
| ▲ | No detecta | |

## 5.9. Connexions remotes.

***Base legal: Article 86 RD 1720/2007.***

## Situació actual

L' Entitat no preveu aquest aspecte en cap dels tres DS.

L'Entitat informà de que els treballadors no poden accedir fora dels locals de l'Entitat al gestor assistencial.

No obstant, el responsable de manteniment de sistemes informàtics sí que accedeix remotament al programa assistencial EKON, sense estar degudament autoritzat en els DS.

## Àrea de millora

| | | |
|---|---|---|
| ● | Àrea de millora | Segons l'article 86 del RDLOPD, quan les dades personals s'emmagatzemin en dispositius portàtils o es tractin fora dels locals del responsable de fitxer o tractament, o de l'encarregat de tractament, és necessari que hi hagi una autorització prèvia del responsable del fitxer o tractament, i en tot cas s'ha de garantir el nivell de seguretat corresponent al tipus de fitxer tractat. Aquesta autorització ha de constar en el DS, per tant, en aquest s'haurà d'establir la relació d'usuaris autoritzats a accedir de manera remota al sistema, a més d'establir les mesures de seguretat aplicades. |

## 5.10. Transmissions per xarxes de telecomunicacions.

***Base legal: Article 104 RD 1720/2007.***

## Situació actual

L' Entitat disposa d'un protocol on s'indica i es detalla la manera d'encriptar documents amb l'eina OpenOffice.

El Manual de Bones Pràctiques fa menció a la transmissió d'informació. Així mateix, s' estableix la prohibició d'utilitzar el fax per l'enviament de documentació amb dades de caràcter personal.

Durant els treballs de camp l'Entitat indica que quan ha de realitzat enviaments de dades de caràcter personal de nivell alt ho fan mitjançant PDF encriptat.

Des del Departament d' Admissions del CSM Nou Barris Sud s'indica que s'envia documentació a l'hospital de dia, a l'Hospital de Subaguts o a residències de manera encriptada amb l' eina Open Office, és a dir es treballa amb l' Open Office però s'exporta a document PDF per tal de ser encriptat. Envien un correu electrònic amb el contingut encriptat i un altre correu electrònic amb la contrasenya del document.

Pel que fa al departament d' Admissions del CSM Nou Barris Sud expliquen durant els treballs de camp que realitzen enviament de documentació a la Clínica la Mercè i als diferents centres del circuit de manera encriptada.

Afirmen que no s'utilitza el fax per l'enviament de documentació amb dades de salut, amb excepció de sol·licitud per part dels Jutjats.

## Àrea de millora

| | | |
|---|---|---|
| ● | Àrea de millora | Està prohibit l'ús del fax per enviar documentació amb dades de caràcter personal de nivell alt. En el cas de que es faci servir, les dades hauran d'estar dissociades, i en el cas de que no es dissocïin i s'enviï documentació per fax, s'haurà de declarar incidència.<br><br>El Dictamen de l'APDCAT (CNS 12/2013) sobre mecanismes de xifratge, , estableix que l'algoritme de xifratge AES (en les seves variants 128 bits i 256 bits), pot considerar-se que compleix amb els requisits de seguretat establerts per l'article 104 del RDLOPD 1720/2007. Altres eines com documents Word o Excel amb contrasenya, no es consideren suficientment segurs. |

## 5.11. Control d'accés.

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

## Situació actual

En els DS es llisten les persones amb el codi d'usuari, el càrrec, el programa i el tipus d'accés que tenen accés a les dades. En els casos que s'accedeixi a les dades de pacients també s'especifica des de quin centre s'accedeix.

L'Entitat disposa d'un protocol on s'explica breument el procediment d'alta i baixa dels usuaris.

El gestor assistencial EKON, presenta un accés limitat per permisos definits segons els perfils i per grup professional, que són els següents:

- Nord
- Sud
- Administració
- Administració Nord
- Administració Sud
- Proc. Administratius
- PSI
- Infermeria
- Gerència
- Equip assistencial
- Col·laboradors.

L'Entitat ha aportat un mostreig dels perfils assignats als treballadors segons el seu perfil professional.

Per donar d'alta un nou treballador, el Departament de Recursos Humans comunica al responsable d'informàtica el perfil del professional perquè aquest li doni d'alta a l' EKON, donant-li l'usuari i contrasenya. Així mateix es comunica a ASTIM que creï una nova compte pel nou treballador, al qual se li facilita, l'usuari i la contrasenya del sistema i el compte de correu electrònic. Quan el treballador entra a treballador al CSM Nou Barris Sud se li comunica de veu, mentre que si entre a treballar al CSM Nou Barris Nord s'informa a Administració del centre i aquests ho comuniquen al treballador.

Pel que fa al sistema de baixa, es segueix el mateix circuit.

## Àrea de millora

| | | |
|---|---|---|
| ▲ | No detectada | |

## 5.12. Identificació i autenticació d'usuaris.

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

### Situació actual

Tot el personal amb accés al sistema i als programes disposa d'usuari i contrasenya, de manera que es garanteix la correcta identificació i autenticació dels usuaris. La identificació de qualsevol usuari per accedir al sistema i als programes és inequívoca i personalitzada.

Pel que fa al programa assistencial EKON el professional disposa d'usuari i contrasenya individual per accedir-hi. Pel que fa la complexitat de la contrasenya aquesta és de 8 dígits, és alfanumèrica amb símbol i caduca cada dos mesos. No s'informa sobre si es poden repetir les dues contrasenyes anteriors. Així mateix, indicaren que tenen instaurat un sistema de bloqueig davant d'un intent d'accés erroni que s'activa després del tercer intent, així com un sistema de bloqueig per inactivitat que s'activa als 10 minuts.

Pel que fa a la complexitat de la contrasenya del sistema té 8 dígits, és alfanumèrica i consta algun símbol i caduca cada dos mesos. En aquest cas no tenen instaurat un sistema de bloqueig per inactivitat ni bloqueig per intent d'accés erroni.

Pel que fa al programa de Derivacions i Ingressos es comenta que no hi ha ni usuaris ni contrasenyes. Es demana més informació sobre aquest programa però no es facilitada.

Es comentà que les primeres contrasenyes adjudicades als usuaris s'obliguen a modificar.

És important indicar que no es guarda una relació de les contrasenyes de manera inintel·ligible.

### Salvetat

| | | |
|---|---|---|
| ▼ | Salvetat | Cal tenir una relació de les contrasenyes de forma inintel·ligible. |

## 5.13. Registre d'accessos.

***Base legal: Article 103 RD 1720/2007.***

## Situació actual

El punt 5.8.2 del DS de pacients indica que es guardarà de cada accés la identificació de l'usuari que accedeix, la data, l'hora en que s'accedeix, el fitxer accedit i el tipus d'accés i si l'accés és autoritzat o no.

Des del Departament de Sistemes d'Informació s'informà de que l' EKON encara no té implementar el mecanisme per les auditories d'accessos, per tant el responsable d'informàtica no té cap mitjà per tenir coneixements sobre els registre d'accessos, ja que l'actual registre d'accessos estan en unes dades inintel·ligibles.

En conseqüència, s'indicà que no realitzen revisions mensuals de la informació de control registrada.

## Salvetat

| | | |
|---|---|---|
| ▼ | Salvetat | Tal com disposa l'article 103 LOPD el responsable de seguretat haurà de revisar almenys una vegada al mes l' informació de control registrada mitjançant el registre d'accessos i haurà d'elaborar un informe de les revisions realitzades i els problemes detectats.<br><br>A més, de cada intent d'accés s'ha de guardar com a mínim: la identificació de l'usuari, la data i hora en què es va realitzar, el fitxer al que s'ha accedit, el tipus d'accés i si ha estat autoritzat o denegat. Quan l'accés hagi estat autoritzat s'hauran de guardar la informació que permeti identificar el registre accedit. |

## 5.14. Còpies de seguretat.

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

## Situació actual

El punt 5.3.3 del DS de Pacients Informatitzats, el punt 5.3.5 del DS d'Històries Clíniques descriuen el procediment de realització de les còpies de seguretat, encara que res es disposa pel que fa a la recuperació de les dades.

Pel que fa a la còpia de seguretat de Windows es fa una còpia de sencera setmanalment. Aleshores es fan còpies incrementals diàries dels ordinadors que es consideren sensibles pel tipus d'informació que contenen. Així mateix també es fa còpia seguint aquest procediment del de la unitat H ( servidor CSM Nou Barris Sud) i de la unitat N ( servidor del CSM Nou Barris Nord). Cada dia es fa còpia al servidor i s'envia a ASTIM.

Pel que fa a la gestor assistencial, es fa copia sencera cada dia. Es rep cada dia per la nit al servidor del CSM Nou Barris Sud.

Durant els treballs de camp s'informa que no es fa una verificació semestres de les còpies de seguretat.

Pel que fa a les recuperacions de dades, s'indicà que aquestes es realitzen dos o tres cops a l'any, sense quedar constància.

## Salvetat

| | | |
|---|---|---|
| ▼ | Salvetat | Per tal de donar compliment a l'article 94 RLOPD el responsable del fitxer s'ha d'encarregar de verificar cada sis mesos la correcta definició, funcionament i aplicació dels procediments de realització de còpies de seguretat i recuperació de dades. |

## 5.15. Fitxers temporals suport automatitzat.

***Base legal: Article 87 RD 1720/2007.***

## Situació actual

En el DS i, específicament, en el Manual de Bones Pràctiques no es deixa constància de que en el cas que es tingui necessitat de crear fitxers temporals s'han d'esborrar una vegada aquests hagin deixat de ser necessaris per a la finalitat per la qual es van crear.

Durant els treballs de camp no es detectà que els diferents professionals treballessin amb documents dels que no es fes còpia d'aquests a les carpetes en xarxa del servidor ni tampoc que arxius temporals quedessin guardats fora dels llocs que ofereixen seguretat.

## Àrea de millora

| | | |
|---|---|---|
| ● | Àrea de millora | Cal fer constar en el Manual de Bones Pràctiques i fer recordatoris de que els fitxers temporals que s'han creat exclusivament per la realització de treballs temporals o auxiliars han de complir el nivell de seguretat que els correspongui. A més , aquests s'hauran d'esborrar o eliminar una vegada deixin de ser necessaris per la tasca concreta. |

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

***Base legal: Article 97 RD 1720/ 2007.***

## Situació actual

El punt 5.8.1 del DS de pacients únicament es considera l'entrada i la sortida de suports en format físic, com són les històries clíniques. Tot i així hi ha annexat un model de registre per les entrades i sortides de suports físics i automatitzats, però aquest no s'utilitza.

Durant els treballs de camp, encara que es comprovà que els treballadors podien portar USB no es va constatar l'entrada i sortida d'USB amb dades de nivell mitjà o alt.

## 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 disposa de vuit ordinadors portàtils que no surten del centre.

Pel que fa als USB el Manual de Bones Pràctiques estableix que els ports estan inhabilitats, però els treballs de camp s'informa que es permeten USB, que els ports estan habilitats i que els professionals poden portar USB personals, com s'ha comentat anteriorment. Tot indicant que no es te la certesa de que els treballadors els utilitzin per guardar documents amb dades de caràcter personal de nivell mig o alt.

S'indica que tots els equips es troben inventariats, així com etiquetats. S'aportà mostreig per l'Entitat de l'inventari dels equips informàtics.

D'altra banda, es comentà des de l'Entitat que tenen fax.

Pel que fa a la destrucció documental l' encarregada és l'empresa externa ECOLOGICAL. L' Entitat disposa de dos tipus de recipients: un pel confidencial i l'altre pel no confidencial. Quan els contenidors del paper confidencial estan plens ho comuniquen a l'empresa i ho passen a recollir per procedir a la seva destrucció, emeten després un certificat.

Pel que fa a destructores el CSM Nou Barris Sud disposa d'una destructora a la sala d'arxiu, mentre que en el CSM Nou Barris Nord la destructora es troba a la sala d'administració.

En el CSM Nou Barris Nord s'indica que hi ha contenidors oberts on els professionals poden tirar documentació amb el nom i cognoms i telèfon del pacient.

Pel que fa a la reparació dels equips, en un primer moment, si es tracta de problemes de configuració, s'intenta fer en el centre de l' Entitat. En el cas que no es pugui reparar l'equip, l'empresa externa ASTIM recull l'equip i s'ho emporta a les seves instal·lacions.

En referència a la seva destrucció, s'indicà que l' encarregat és també l'empresa ASTIM. Aquests tercer procedeix a recollir l'equip al centre. En el centre d'aquest tercer es formata els disc dur i es retorna l'equip a l' Entitat.

### Salvetat

| | | |
|---|---|---|
| ▼ | Salvetat | Cal que els contenidors on es tira documentació amb dades de caràcter personal estiguin tancats. |

## 5.18. Control d'accés.

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

# Situació actual

Pel que fa l'accés al servidor de l'Entitat, aquest es troba en una sala destinada també per arxiu i per emmagatzemar material d'oficina. Aquesta sala es manté oberta durant el dia ja que la majoria de treballadors té accés a la mateixa. Aquesta sala es troba dins del departament d'admissions i per accedir-hi també hi ha una porta que també resta oberta durant la jornada laboral. No obstant, en el punt *Control i limitació del accés físic* del DS de pacients s'indica que únicament tindrà aquest a la sala de servidors el personal informàtic, mentre que en el DS de personal s'indica que tindran accés a la sala del servidor el personal d' administració i assistencial.

Pel que fa a l'arxiu d'històries clíniques aquesta es troba en la mateixa sala on es troben els servidors i el material d'oficina. Com ja s'ha comentat, aquesta disposa de dispositiu de tancament en clau però només s'utilitza al finalitzar la jornada laboral atès que durant el dia el personal d'administració controla l'accés a la sala.

Les fulles de reclamacions i suggeriments que presenten els pacients i usuaris es guarden en un armari del departament d'admissions tancat en clau.

Pel que fa a l'arxiu passiu aquest es troba en una altra sala que resta tancada amb clau. La clau es troba a administració en un armari tancat en clau.

Pel que fa a l'arxiu d'històries clíniques actives del CSM Nou Barris Nord, per accedir-hi és necessari un codi.

Pel que fa a la documentació dels pacients que es troben en actual tractament, des de el CSM Nou Barris Sud ens comenten que gairebé casi no s'utilitza ja que tota la informació es troba informatitzada. Al CSM Nou Barris Nord, s'indica que alguns professionals sí que treballen amb les històries clíniques dels pacients, estan en els despatxos les histories clíniques necessàries per aquell dia, i estan el despatx degudament tancat en clau quan el professional deixa el despatx.

Pel que fa la documentació de Departament de Recursos humans, aquesta es troba emmagatzemada en el despatx de la Cap d' Administració en un armari tancat. El despatx també queda tancat en clau si no es troba la Cap. En aquest despatx, i també en armaris tancats en clau s'emmagatzema la documentació d'Administració.

Pel que fa al passiu d'Administració aquest es troba en un armari del departament d'admissions, el qual disposa de tancament en clau.

# Àrees de millora

| | | |
|---|---|---|
| ● | Àrea de millora | De conformitat amb l'article 111 del RDLOPD, els armaris, arxivadors o altres elements en què s'emmagatzemin els fitxers no automatitzats amb dades de caràcter personal, han d'estar en àrees en què l'accés estigui protegit amb portes d'accés dotades de |

| | | |
|---|---|---|
| | | sistemes d'obertura mitjançant una clau o dispositiu equivalent. Aquestes àrees s'han de mantenir tancades quan no sigui necessari l'accés als documents inclosos en els fitxers. És a dir, cal que a l'arxiu d'històries clíniques no entri personal que no esta autoritzat, així com evitar que estigui obert durant tot el dia.<br><br>Cal que a la sala de servidors no s'utilitzi per guardar material d'oficina, per evitar que entrin professionals no relacionats amb el manteniment dels servidors.<br><br>Quan, ateses les característiques dels locals, no es possible complir amb aquestes premisses, s'hauran d'establir mesures alternatives, les quals hauran de constar en el DS. |

## 5.19. Registre d'accessos.

***Base legal: Article 113 RD 1720/2007.***

## Situació actual

El DS de pacients únicament considera el registre dels accessos informatitzats, no disposant-se cap consideració pel que fa al registre d'accessos físics.

En el Manual de Bones Pràctiques s'estableix que l'Entitat realitzarà una revisió mensual dels accessos físics esdevinguts en les històries clíniques, tanmateix durant els treballs de camp es comprovà que ni en el CSM Nou Barris Sud ni Nord no es duu a terme cap registre d'accessos a l'arxiu actiu d'històries clíniques, ni tampoc al passiu.

Quan un professional del CSM Nou Barris Sud necessita una història clínica accedeix a l'arxiu i l'agafa, no quedant constància de quan un professional agafa una història clínica i quan la torna a l' arxiu. Pel que fa al CSM Nou Barris Nord quan un professional necessita una història clínica pel dia següent el personal d'administració li deixa en una safata dins del mateix arxiu. Al final del dia cada professional la torna a deixar en una safata perquè administració l'arxivi. En aquest procés tampoc queda constància de les històries clíniques que s'extreuen i que es retornen a l'arxiu. Així mateix, s'indica que hi ha professionals que ells mateixos agafen les històries clíniques i les retornen.

## Salvetat

| | | |
|---|---|---|
| ▼ | Salvetat | Per donar compliment a l'article 103 del RLOPD l'accés a la documentació que contingui dades de nivell alt s'ha de limitar exclusivament al personal autoritzat. Així mateix, s'han d'establir mecanismes que permetin identificar els accessos realitzats en el cas de documents que puguin ser utilitzats per múltiples usuaris. |

## 5.20. Criteris d'arxiu.

***Base legal: Articles 106 RD 1720/2007.***

# Situació actual

Els criteris d'arxiu garanteixen la correcta conservació de la documentació, la localització i consulta de la informació i possibiliten l'exercici dels drets d'oposició al tractament, accés, rectificació i cancel·lació..

Fitxer de pacients: Hi ha dos arxius actius d' HC: un a CSM Nou Barris Sud i un altre a CSM Nou Barris Nord. L'arxiu actiu d'HC de CSM Nou Barris Sud es troba emmagatzemats en una sala adjunta a la sala d'admissions, sent el criteri d'arxiu el número d'història clínica. El criteri per considerar-se com passiu és que el pacient sigui un èxitus o bé hagi estat traslladat. Pel que fa a l'arxiu d'aquest, es troba en una sala del mateix centre, seguint-se el mateix criteri d'arxiu indicat, custodiant-se la documentació de manera indefinida.

Pel que fa a l'arxiu actiu de CSM Nou Barris Nord es troba també en una sala adjunta a admissions, sent el criteri d'arxiu el número d'història clínica. En aquest cas es considera passiu quan transcorre un any des de l'última visita. L' arxiu passiu es troba a l' Hospital de Dia, on segueix el mateix criteri d'arxiu.

Fitxer de RRHH: Pel que fa els expedients dels treballadors, aquests es troben al despatx de la Cap d'Administració, sent aquesta la responsable de l'arxiu, seguint un criteri d'arxiu per ordre alfabètic. L'arxiu actiu són els expedients dels treballadors actius. En quan al passiu, format per expedients dels treballadors dels últims 5 anys,

Fitxer d' administració: Pel que fa a la documentació d'administració de l'any en curs i l'anterior, aquesta es troba al despatx de la Cap d' Administració, ordenat seguint un criteri temporal. El passiu, és a dir, la documentació dels anys anteriors es troba en un armari de la sala d'admissions, ordenat per anys.

# Àrees de millora

| | | |
|---|---|---|
| ▲ | No detectada | |

## 5.21. Entrades i sortides de documents.

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

# Situació actual

L'Entitat únicament regula el registre d'entrada i sortida d'històries clíniques.

Cal recordar que l'arxiu passiu d'històries clíniques del CSM Nou Barris Nord es troba situat en l' Hospital de Dia, no existint cap registre de les històries que surten del CSM cap a l'arxiu passiu. únicament existeix un llistat d'històries clíniques i quan aquestes són traslladades a l'arxiu passiu s'eliminen de la llista, no considerant-se que es compleixin així els paràmetres indicats per la llei.

Durant els treballs de camp el departament de Recursos Humans indica que l'examen de salut laboral ho realitza una empresa externa anomenada SEPRA . Aquesta envia els resultats dels exàmens a l' Entitat, no existint un registre d'entrada d'aquests documents.

En el departament d'admissions del CSM Nou Barris Nord s'informa que poden rebre derivacions o informes d'altres centres, dels quals no existeix registre d'entrada.

# Salvetat

| | | |
|---|---|---|
| ▼ | Salvetat | S'ha d'establir un sistema de registre d'entrada i sortida de suports que permeti directa o indirectament, conèixer el tipus de documentació o suport, la data i hora, l' emissor, el número de documents, el tipus d'informació, la forma d'enviament i la persona responsable de la recepció o entrega degudament autoritzada. |

## 5.22. Fitxers temporals.

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

## Situació actual

El Manual de Bones Pràctiques té en compte que s'ha de garantir que el paper inservible sigui destruït.

Es detectà durant els treballs de camp que és possible la generació de fitxers temporals, en el context de l'activitat mèdica diària de l'Entitat, encara que es té plena consciència de que, un cop finalitzada la tasca per la qual s'ha generat el document, aquest ha de ser destruït mitjançant la destructora de la que disposen a cada centre.

## Àrees de millora

| | | |
|---|---|---|
| ▲ | No detectada | |

# IV- BLOC DE MESURES ORGANITZATIVES

## 5.23. Registre d'incidències.

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

### Situació actual

En tots els DS es regula el registre d'incidències. Tal com s'ha comentat en el punt 5.3 f d'aquest informe existeixen diferències entre els DS pel que fa a la persona responsable de reflectir les incidències en el registre i la persona responsable de custodiar-lo.

L' Entitat disposa de l' annex *Procediment de gestió i registre d'incidències* on es disposa la notificació, gestió, resposta i registre de les incidències. Així mateix s'adjunta un model de comunicació d'incidència i un model de registre d'incidències, encara que cal indicar que l' Entitat no utilitza aquests models.

Durant els treballs de camp s'indica que quan un professional detecta una incidència aquest envia un correu electrònic al departament d'administració i aquest informa al departament que correspongui.

L' Entitat ha aportat mostreig del registre d'incidències relacionades amb protecció de dades però únicament les informàtiques..

### Àrea de millora

| | | |
|---|---|---|
| ● | Àrea de millora | Cal que l' Entitat adapti un procediment únic pel que fa a la notificació, gestió i registre d'incidències i ho reflecteixi en el DS o en l' annex corresponent. |

## 5.24. Difusió de funcions i obligacions.

***Base legal: Article 89.2 RD 1720/2007.***

# Situació actual

L'Entitat entrega al treballador el Manual de Bones Pràctiques en el que consten les funcions i les obligacions del personal. No obstant, no hi ha l'obligació de signar-lo. Segons s'indicà, aquest Manual no és entregat als estudiants en pràctiques.

Pel que fa a la formació, es comentà que les persones que formen la Comissió de Protecció de Dades intenten assistir a les formacions del Codi Tipus, de la mateixa manera que s'intenta que a cada sessió hi vagi persones diferents.

# Salvetat

| | | |
|---|---|---|
| ▼ | Salvetat | Segons l'article 89.2 del RDLOPD, el responsable del fitxer ha d'adoptar les mesures necessàries perquè el personal conegui d'una forma comprensible les normes de seguretat que afectin l'exercici de les seves funcions, així com les conseqüències en que pugui incórrer en cas d'incompliment.. Per això, és important que s'entregui i que es faci signar el Manual de Bones Pràctiques, tant als empleats com als estudiants en pràctiques. |

# 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** |
| 5.2. Aspectes generals |
| 5.3 Document de seguretat |
| 5.6. Legitimació de dades |
| 5.7. Drets ARCO |
| **II- BLOC DE MESURES INFORMÀTIQUES** |
| 5.9. Connexions remotes |
| 5.10 Transmissions per xarxes de telecomunicacions |
| 5.15 Fitxers temporals suport automatitzat |
| **III- BLOC DE MESURES FÍSIQUES O DOCUMENTALS** |
| 5.18. Control d'accés |
| **III – BLOC DE MESURES ORGANITZATIVES** |
| 5.23 Registre d'incidències |

| **SALVETATS** |
|---|
| **I- BLOC GENERAL** |
| 5.5 Tercers |
| **II- BLOC DE MESURES INFORMÀTIQUES** |
| 5.12 Identificació i autenticació d'usuaris |
| 5.13. Registre d'accessos |
| 5.14 Còpies de seguretat |
| **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 Entrades i sortides de documents |
| **IV-BLOC DE MESURES ORGANITZATIVES** |
| 5.24 Difusió de funcions i obligacions |

Barcelona, 19 de setembre de 2016.

Pere Ruiz Espinós

- Soci-