Protecció de dades de caràcter personal

Juny de 2020
Protocol: C-12.448

Fundació Institut Guttmann

Informe d'Auditoria de Protecció de Dades de Caràcter Personal

Fundació Unió Carrer de València, 333 · 08009 Barcelona · Tel 93 209 36 99 · Fax 93 200 86 38
Faura-Casas Carrer Còrsega, 299 6ª · 08008 Barcelona · Tel 902 28 28 30 · Fax 93 302 65 96

INDEX

1. OBJECTIUS I CONTINGUT

El mes d'abril de 2016 es va aprovar el Reglament (UE) 2016/679 del Parlament i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (Reglament general de protecció de dades, publicat al DOUE 4.5.2016, referit en endavant com a RGPD o Reglament). Aquesta nova regulació, vehiculada per primer cop a través d'un reglament europeu, comporta canvis significatius en la protecció de dades de caràcter personal, tant des del punt de vista dels drets de les persones com de les obligacions de les persones i entitats que tracten dades de caràcter personal.

El Reglament introdueix els conceptes de privacitat des del disseny i privacitat per defecte. Això implica que el responsable ha d'aplicar, tant en el moment de determinar els mitjans de tractament com en el moment del tractament mateix, les mesures tècniques i organitzatives adequades concebudes per aplicar de manera efectiva els principis de protecció de dades (com, per exemple, la seudonimització), i integrar les garanties necessàries en el tractament per complir els requeriments del Reglament.

Si abans el Reglament de Desenvolupament de la LOPD (RLOPD) determinava amb detall i de forma exhaustiva les mesures de seguretat que havien d'aplicar-se segons el tipus de dades objecte de tractament, amb el RGPD els responsables i encarregats establiran les mesures tècniques i organitzatives apropiades per a garantir un nivell de seguretat adequat en funció dels riscos detectats durant l'anàlisi prèvia.

D'altra banda, cal considerar l'aprovació relativament recent de la nova llei orgànica de protecció de dades, la Llei 3/2018, de 5 de desembre, de Protecció de Dades Personals i garanties dels drets digitals (LOPDGDD), que adapta a l'ordenament jurídic espanyol el RGPD; la nova LOPD conté una disposició derogatòria única per la qual es deroga la LOPD i qualssevol altres disposicions d'igual o inferior rang que contradiguin, s'oposin, o resultin incompatibles amb el que disposa el RGPD.

Per tot plegat, a partir de 24 de maig de 2018:

- Resulta plenament aplicable allò previst al RGPD, i a la Llei Orgànica 3/2018, LOPDiGDD (a partir del 7 de desembre de 2018).
- Correspon al responsable o encarregat del tractament aplicar les mesures tècniques i organitzatives adequades per garantir que només es tracten les dades personals necessàries per a cada finalitat específica del tractament. Per a determinar les mesures tècniques i organitzatives s'atendrà a:
    - El cost de la tècnica
    - Els costos d'aplicació
    - La naturalesa, l'abast, el context i les finalitats del tractament
    - Els riscos pels drets i llibertats
- La falta de determinació per part del responsable o encarregat del tractament de les mesures de seguretat suposa l'incompliment del principi de responsabilitat proactiva.

- A falta de concreció per part del responsable o encarregat del tractament de mesures específiques, s'auditarà atenent a l'esquema de mesures de seguretat previst al RLOPD, sempre que sigui compatible i no contrari al RGPD ni a la LOPDiGDD. Les mesures previstes al RLOPD que ja estiguin implantades poden ser útils, però cal analitzar en cada cas si són suficients o és necessari modificar-les.
- 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. Es tindran en compte les consideracions de l'AEPD en relació a les mesures indispensables que s'ha de complir amb els tractaments d'escàs risc.

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.

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, S.L. 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	Fundació Institut Guttmann
CIF	G08519100
Domicili	Camí de Can Ruti s/n 08916 Badalona

3.1.2. Descripció de l'activitat

La Fundació Institut Guttmann és una entitat privada d'iniciativa social, sense ànim de lucre i aconfessional, impulsada per la societat civil catalana, constituïda l'any 1962. El seu objectiu principal és promoure, impulsar i aconseguir la rehabilitació integral de les persones afectades per una lesió medul·lar, un dany cerebral adquirit o una altra discapacitat d'origen neurològic, desenvolupar la recerca i la docència en aquest àmbit de la neurociència i prestar-los el suport i els serveis més convenients per assolir una reinserció social satisfactòria.

En data de 18 de juny de 2014 s'aprovà la fusió per absorció de la Fundació Privada Institut de Neurorehabilitació Guttmann per la Fundació Institut Guttmann, que es va fer efectiva a partir de 2015. D'aquesta manera, totes les activitats de la Fundació Privada Institut de Neurorehabilitació Guttmann passen a integrar-se dins les activitats que ja duia a terme la Fundació Institut Guttmann, subrogant-se doncs en tots els drets i obligacions de l'entitat fusionada i extingida. Els serveis prestats per l'entitat són els d'hospitalització d'aguts, d'hospital de dia, neurorehabilitació, consultes externes i recerca.

Les instal·lacions actuals de Fundació Institut Guttmann a Badalona són de 2002.

D'altra banda, el projecte Barcelona Health Institut als carrers Meridiana/Garcilaso de Barcelona, suposa l'existència d'unes noves instal·lacions, entre les quals hi ha un gimnàs, sales de tractament, consultes mèdiques (neuroclínica) i els apartaments LIFE domotitzats per a persones amb necessitats especials.

3.2. TREBALLS EFECTUATS

S'han realitzat els treballs de camp de l'auditoria en els diversos departaments i serveis de l'entitat:

- Àrea econòmica-financera
- Delegat de protecció de dades
- Àrea de prevenció de riscos i salut laboral
- Àrea de sistemes informàtics

- Àrea de recursos humans
- Àrea de comunicació i activitats socials
- Àrea d'atenció a l'usuari i admissions
- Àrea d'arxiu
- Àrea de recerca
- Àrea de docència
- Servei d'infraestructures, serveis i medi ambient (ISMA)
- Àrea de màrqueting i GNPT (Guttmann NeuroPersonal Trainer)
- Àrea de treball social
- Infermeria (perfil)
- Fisioteràpia (perfil)
- Neuropsicologia (perfil)
- Medicina (perfil)

Degut a les restriccions i mesures adoptades oficialment per a la prevenció de la Covid-19, els treballs d'auditoria s'han dut a terme a través de videoconferències, sense que hi hagi hagut visites o revisions presencials. No obstant, s'han aportat i recollit informacions i evidències documentals suficients per a l'elaboració d'aquest informe d'auditoria.

3.2.1. Data de realització de l'auditoria

Data	8 i 9 de Juny de 2020

3.2.2. Persones entrevistades i relació de la documentació entregada a l'auditor

Persones entrevistades per ordre d'intervenció:

NÚMERO	PERSONA ENTREVISTADA	CÀRREC O ÀREA DE TREBALL
1	Sr. Héctor López	Cap econòmic financer
2	Sr. Javier Remacha	Delegat de protecció de dades (DPD)
3	Sra. Sheila Patricio	Responsable del servei de prevenció
4	Sr. Roger Marsal	Cap de serveis informàtics
5	Sra. Elisenda Bassas	Cap de recursos humans
6	Sra. Sandra Palomo	Tècnic de recursos humans
7	Sra. Elisabet González	Cap de comunicació i de responsabilitat social corporativa
8	Dra. Maria Victòria Amargós	Cap del departament d'atenció a l'usuari i admissions
9	Sra. Elena Araujo	Departament d'admissions
10	Dr. Josep Maria Tormos	Director de recerca

11	Dr. Eloy Opisso	Cap de projectes de recerca
12	Sra. Mercè Solans	Coordinadora de docència
13	Sra. Sílvia Calvo	Cap de l'ISMA (Infraestructures, serveis i medi ambient)
14	Sr. David Hurtado	Responsable de màrqueting
15	Sr. Alexis Álvarez	Responsable del departament I+D al Grupo ICA
16	Sra. Àngels Hervàs	Cap de treball social
17	Sr. Emilien Amar	Àrea d'infermeria
18	Sr. Ignasi Soriano	Àrea de fisioteràpia
19	Sr. Joan Saurí	Àrea de neuropsicologia
20	Dr. Raúl Pelayo	Àrea de medicina

Relació de la documentació lliurada a l'auditor:

- Menú documentació auditoria 2020.
- Estatuts de de l'entitat.
- Descripció Hospital de Neurorehabilitació, Guttmann Barcelona Life, Guttmann Brain Health Institute.
- Organigrama.
- Registre d'activitats de tractament IG 2020.
- Sol·licitud inscripció DPD maig 2018.
- Formulari de nomenament de DPD Institut Guttmann maig 2018.
- Carta amb els codis d'inscripció dels fitxers que envia l'AEPD.
- Annex 17 Sistema de seguretat i pla de contingències.docx
- Documents de Seguretat corresponents als diferents fitxers i els seus annexos.
- Annex 21 Esquema de la xarxa.
- Autorització Pacients tractament de dades.
- Autorització gravació sessions formatives.
- Autorització presa d'imatges i veu.
- Autorització presa d'imatges i veu representant legal.
- Contractes LOPD (mostra).
- Models de controls dels registres establerts: 0601 Incidències HCE, 0602 Registre Accessos HCE, Registre Accessos GNPT.
- Informes de revisió mensual dels diferents registres: 0601 Incidències HCE, 0602 Registre Accessos HCE, Registre Accessos GNPT.

- Models per a l'exercici dels drets de les persones: formularis de dret d'accés, rectificació, supressió, oposició, limitació i portabilitat.
- AL-1-RS-PDP-026001-ca Avaluació de Riscos 2020 v2.
- Informe Final Avaluació Impacte Tractament AQuAS.xlsx.
- comunicat a Com DIRECTIU superada auditoria LOPD 2018.pdf
- 2018 Informe Auditoria LOPD FIG.
- Manual d'Acollida Guttmann - Versió juny 2020
- Annex 08 Compromís Professional abril 2019 Ca_LOPD
- Formació LOPD 2020.
- Àrea de docència: Autorització presa d'imatges i veu 2019, Codi Ètic, Compromís de confidencialitat residents, Compromís de confidencialitat alumnes, Full d'incripció_cat formulari, Manual d'acollida MIR.
- Àrea de voluntariat: 03 Annex 08 Compromís de Confidencialitat Voluntariat, Carta voluntariat àmbit de la salut 2019, Contracte compromís 2019, Drets i deures del voluntariat, emergències, Fitxa 19A-Rentat de mans, prevenció de transmissió de gèrmens, Sol·licitud voluntariat 2018, Manual acollida voluntariat v2 2018, Formació voluntariat.
- Mostra de contractes d'encàrrec de tractament i compromís de confidencialitat: 2019_01_17 Carlos Estrela UCAE + CC, 2019_04_03 Augusto F Poveda SODEXO + CC, 2019_05_16 Judith Caleya ASPY + CC, 2019_06_11 Marta Vazquez ASECORP + CC, 2019_09_19 Agustí Piera MASTER + CC, 2019_09_27 Nuria Martin CERBA + CC 2019_10_17 Xavier Manzano LA RIERA PADEL SL, 2020_01_10 Hugo Otero DO WHILE STUDIO.

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 no conformitat 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.
▼	**No conformitat**, 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: Article 24.1 RGPD

Situació actual

D'acord amb l'article 24.1 del RGPD, correspon al responsable del tractament aplicar les mesures tècniques i organitzatives necessàries, a fi de garantir i poder demostrar que el tractament és conforme al mateix RGPD. A més, aquestes mesures es revisaran i s'actualitzaran sempre que sigui necessari. Per aquest motiu, GUTTMANN encarrega la realització d'aquest informe d'auditoria, que serà analitzat pel responsable del tractament i elevat a direcció, per tal que s'adoptin les mesures correctores adients.

L'entitat ja té implementada una política de realització biennal d'auditories sobre protecció de dades. La darrera auditoria sobre protecció de dades que es va realitzar, tal com es pot comprovar en el propi document aportat, és de data 19 de juny de 2018. D'aquest manera, l'entitat aplica correctament la mesura de sotmetre's a una auditoria biennal sobre protecció de dades.

D'acord amb l'acta de 12 de juny de 2018 del Comitè de Direcció de GUTTMANN, que s'ha aportat com a evidència, es va informar al Comitè de Direcció sobre un pronòstic favorable respecte a l'auditoria de protecció de dades, però no sobre el resultat final, ni sobre les mesures correctores adoptades, si fos el cas.

Àrees de millora

●	L'evidència aportada dona compte que es va informar correctament al Comitè de Direcció sobre la realització de l'auditoria i el seu pronòstic favorable, però no sobre el resultat final. Convindria que constés una evidència més clara que l'entitat com a tal, a través del seu Comitè de Direcció, ha estat informada de manera exhaustiva sobre el resultat de l'auditoria i l'ha assumit i, si és el cas, ha adoptat o encarregat les mesures correctores necessàries.

5.2. REGISTRE D'ACTIVITATS DEL TRACTAMENT

Base legal: Article 30 RGPD

Situació actual

L'article 30 del Reglament General de Protecció de Dades (RGPD) estableix l'obligatorietat de realitzar el Registre d'Activitats del Tractament (RAT). Aquesta obligació no afectarà aquelles organitzacions que tinguin menys de 250 treballadors, llevat que el tractament de les dades que facin pugui comportar un risc per als drets i les llibertats dels interessats, no sigui ocasional, o inclogui categories especials de dades o dades personals relatives a condemnes i infraccions penals.

En el cas de l'entitat, els tractaments que du a terme, pel volum i la sensibilitat de les dades tractades, poden implicar un risc per als drets i les llibertats. A més, també cal tenir present que es tracten habitualment dades de salut, que tenen la consideració de dades de categoria especial. Per tant, d'acord amb les previsions del RGPD, l'entitat està obligada a elaborar i mantenir un Registre d'Activitats de Tractament.

A data de l'auditoria, GUTTMANN manifesta que ja ha elaborat un RAT, el qual aporta a aquesta auditoria en format Excel. Segons aquest document GUTTMANN identificaria 18 activitats de tractament diferents amb els noms següents:

- Pacients
- Personal
- Administració
- Reclamacions
- Externs RRPP
- Externs amics
- Vídeos formació
- Externs GBL
- Externs S&L GB
- Externs Docència
- Externs Voluntaris
- Externs TBC
- Videovigilància
- Investigació
- GNPT
- BBHI
- Blanqueig
- Empremtes digitals

Fins a l'entrada en aplicació del RGPD, l'entitat tenia diferents fitxers notificats, que es correspondrien parcialment amb els tractaments de dades identificats al RAT amb el mateix nom. En tot cas, és important assenyalar que l'activitat principal desenvolupada per l'entitat, la que implica un tractament més massiu i sensible de dades, és la corresponent a la prestació d'assistència sòcio-sanitària, especialitzada en aquest cas al tractament de lesions medul·lars, danys cerebrals i discapacitats d'origen neurològic.

D'acord amb la disposició final onzena de la LOPDGDD, que modifica l'article 6 bis de la Llei 19/2013, de 9 de desembre, de transparència, accés a la informació pública i bon govern, els

subjectes del sector públic citats a l'article 77.1 de la LOPDGDD tenen l'obligació addicional de publicar el seu RAT i fer-lo accessible electrònicament. L'entitat, però, no es troba entre els subjectes obligats de l'article 77.1 de la LOPDGDD.

No detectada

▲	El RAT elaborat per FIDMAG reflecteix i identifica de forma correcta els tractaments realitzats per l'entitat i s'ajusta fonamentalment a les previsions de l'art. 30 RGPD. Tenint en compte els diferents serveis i activitats que realitza l'entitat, constatem que totes elles apareixen reflectides correctament al RAT.

5.3. DEFINICIÓ DE LES MESURES PER PART DEL RESPONSABLE DEL TRACTAMENT

Base legal: Articles 24, 25 i 32 RGPD

Situació actual

El RGPD, a diferència del RLOPD, no preveu mesures específiques per a la seguretat del tractament de les dades personals, sinó que deixa en mans del responsable del tractament la definició i implementació de les mesures més adequades d'acord amb els riscos que plantegi cada tractament de dades. L'article 25 RGPD contempla les obligacions de la protecció de dades des del disseny i per defecte. Sobre les mesures que cal aplicar, s'estableix:

- Es manté un deure d'aplicar les mesures tècniques i organitzatives adients amb la finalitat de garantir que el tractament sigui conforme al RGPD.
- Les mesures adoptades pel responsable del tractament han de ser demostrables.
- Caldrà revisar periòdicament i actualitzar aquestes mesures, quan sigui necessari.
- Cal tenir present sempre el principi de protecció de dades des del disseny i per defecte, que ha de regir tot tractament de dades.

L'entitat disposa de diferents documents de seguretat, que descriuen correctament, de manera integral, la seva política de protecció de dades i les mesures de seguretat que aplica. Aquestes mesures, tal com podem corroborar, es corresponen en bona part amb les que ja preveia l'antic Reglament de 2007 (RLOPD) que desenvolupava la LOPD anterior. Tot i que estem parlant d'una normativa que ja no és la referent, les mesures de seguretat que hi apareixien definides continuen essent un referent rellevant.

El RGPD no impedeix que les mesures de seguretat previstes pel RLOPD continuïn aplicant-se per tal de garantir el compliment de les obligacions del responsable del tractament. D'aquesta manera, l'entitat continua aplicant les mesures de seguretat citades, previstes al RLOPD, a més de voler complir els nous requeriments del RGPD, com ara el nomenament del DPD o l'elaboració d'un RAT, entre d'altres.

D'altra banda, l'AEPD ha definit unes mesures de seguretat mínimes obligatòries que han de complir tots aquells tractaments de dades que suposin un risc escàs. Aquestes mesures de seguretat, de tipus organitzatiu i tècnic, cal garantir-les en tot cas i sobre tots els tractaments. Tal com podem comprovar a través de la documentació aportada a aquesta auditoria, l'entitat assumeix de forma implícita totes aquestes mesures.

Pel que fa al sector sanitari, hem de tenir en compte també com a referents les mesures de seguretat que han determinat com a necessàries les autoritats de control i especialment les que s'han definit a partir dels plans d'inspecció de l'AEPD d'ofici de l'atenció sòcio-sanitària i el decàleg que se'n va elaborar.

MESURES ORGANITZATIVES	
Deure de confidencialitat i secret	Evitar l'accés de persones no autoritzades a les dades personals: evitar pantalles desateses, documents en zones d'accés públic, etc. Quan s'absenti del lloc de treball es procedirà al bloqueig de l'estació o tancament de la sessió.

	Els documents en paper i suports electrònics s'emmagatzemaran en lloc segur (armaris, calaixos o espais d'accés restringit).
	No es llençaran documents o suports electrònics amb dades personals sense garantir-ne la destrucció.
	No es comunicaran dades personals o qualsevol informació personal a tercers.
	Signar amb els treballadors que tinguin accés a dades un acord de confidencialitat i entregar-los un manual per a usuaris amb les obligacions i mesures establertes.
	El deure de secret i confidencialitat es manté fins i tot després de finalitzar la relació laboral del treballador amb l'empresa.
Drets dels titulars de les dades	S'informarà als treballadors, sobretot als que puguin estar de cara al públic, sobre el procediment d'atenció als drets dels interessats, definint de forma clara els mecanismes previstos per a l'exercici d'aquests drets.
	Prèvia presentació del DNI o passaport, les persones interessades podran exercir els seus drets. El responsable del tractament haurà de donar d'atendre les seves peticions.
Violacions de seguretat de les dades	Quan es produeixin violacions de seguretat, es notificaran a l'autoritat de control en el termini de 72 hores d'ença del moment que se'n té coneixement. La notificació es realitzarà a través de la seu electrònica de l'autoritat de control.
	Es podrà gestionar de forma interna un registre d'incidències que es puguin produir amb dades personals.
Documentació paper	S'establiran criteris d'arxiu per a la documentació que contingui dades de caràcter personal, i es custodiarà de forma adequada, quan no es faci servir.
	Categories especials de dades: es restringirà l'accés a aquest tipus de documentació, s'habilitaran mètodes per a la seva destrucció i es durà a terme un registre d'accés a aquests documents.
Delegat de Protecció de Dades	✓ El tractament el realitzi una autoritat o organisme públic ✓ Les activitats consisteixin en operacions que, degut a la seva naturalesa, abast i/o fins, requereixin una observació habitual i sistemàtica d'interessats a gran escala.

	✓ Les activitats principals consisteixin en el tractament a gran escala de categories especials de dades personals i de dades relatives a condemnes i infraccions penals.

MESURES TÈCNIQUES	
Identificació	S'establiran mecanismes d'autenticació personalitzats per accedir als sistemes mitjançant, per exemple, un usuari i contrasenya específics per a cada treballador (identificació inequívoca).
	S'establiran perfils d'usuaris amb diferents nivells d'accés a dades personals segons les funcions del treballador.
	Quan un dispositiu s'utilitzi per al tractament de dades personals i fins d'ús personal, es recomana establir perfils diferents.
	Es recomana disposar de perfils amb drets d'administració per a la instal·lació i configuració del sistema i usuaris sense privilegis.
	Es garantirà, com a mínim, l'existència de contrasenyes per a l'accés a les dades personals emmagatzemades als sistemes. La contrasenya tindrà almenys 8 caràcters (números i lletres) i l'empresa decidirà la complexitat d'aquestes claus. Es canviaran les claus, com a mínim, un cop l'any.
	Cal garantir la confidencialitat de les contrasenyes, evitant que puguin ser exposades a tercers.
	En cas de intents d'accés fallits a un compte d'usuari es bloquejarà aquest compte.
Deure de salvaguarda	Els dispositius i ordinadors utilitzats per a l'emmagatzemament i el tractament de les dades personals hauran de mantenir-se actualitzats.
	En aquests dispositius es disposarà d'un sistema d'antivirus instal·lat i degudament actualitzat.
	Per evitar accessos remots indeguts a les dades personals es prendran les mesures corresponents com l'existència de Firewall.
	Periòdicament (mínim setmanal) es duran a terme processos

	de còpia de seguretat de les dades personals en un suport diferent al que s'utilitza per al treball diari. Es disposarà d'una còpia de seguretat en un lloc diferent d'on s'emmagatzemen les dades.
	Categories especials de dades: es durà a terme un registre d'accessos d'aquest tipus de dades.
Gestió de suports i dispositius	Es disposarà d'un inventari actualitzat dels diferents suports/dispositius que continguin dades personals.
	Categories especials de dades: quan calgui realitzar l'extracció de dades personals fora del recinte on se'n fa el tractament, ja sigui per mitjans físics o electrònics, s'haurà de valorar la possibilitat d'utilitzar un mètode d'encriptació.
	S'establiran mecanismes de restricció d'accés a la sala on es trobin els servidors (CPD).
	Com a norma general, els fitxers que continguin dades personal s'emmagatzemaran en un servidor de fitxers i no en els dispositius dels usuaris de forma local.

El compliment d'aquestes mesures mínimes serà avaluat en diferents punts d'aquest informe.

Els tractaments que realitza GUTTMANN a data de l'auditoria són, en gran part, els mateixos que realitzava anteriorment a l'entrada en aplicació del RGPD el 25 maig de 2018, de manera que les mesures de seguretat ja van ser definides i implementades sota l'anterior règim legal, tenint en compte les característiques i els riscos d'aquests mateixos tractaments. No obstant, és important tenir en compte també que s'han estat desenvolupant nous serveis, com ara els corresponents al Barcelona Guttmann Life i l'Sports & Life Guttmann Club.

Els diferents documents de seguretat de seguretat i els seus annexos, el RAT i especialment el document "*Annex 17 Sistema de seguretat i pla de contingències*" contenen una descripció detallada de com es tracten les dades en les diferents activitats de tractament que du a terme GUTTMANN i les mesures de seguretat que s'hi apliquen. És en aquest document on podem observar de forma exhaustiva les mesures de seguretat que ha definit i aplica a dia d'avui. Comprovem que tots els documents estan actualitzats.

El document "Annex 21 Esquema de la xarxa" presenta un esquema general de la xarxa informàtica de l'entitat i de mesures de seguretat previstes a nivell general.

El document Excel "*AL-1-RS-PDP-026001-ca Avaluació de Riscos 2020 v2*" constitueix un exercici rellevant d'anàlisi de riscos realitzat pel DPD de l'entitat, realitzat exhaustivament sobre tots els tractaments identificats al RAT. En aquest RAT s'han analitzat profusament diferents riscos i s'han establert propostes per minimitzar-los de forma correcta. Com a aspecte millorable,

tanmateix, val a dir que no hi consta una valoració sobre si aquests tractaments requeririen o no una avaluació d'impacte de manera obligatòria, d'acord amb l'article 35.1 RGPD.

També tenim en compte el document "Informe Final Avaluació Impacte Tractament AQuAS", que és un informe d'avaluació d'impacte centrat en analitzar la comunicació de dades realitzada a Institut Guttmann de dades de pacients per part de l'Agència de Qualitat i Avaluació Sanitàries de Catalunya (AQuAS).

Finalment, cal fer notar l'obligació que tenen les entitats del sector públic o vinculades al servei públic d'aplicar les mesures de seguretat de l'Esquema Nacional de Seguretat (ENS), d'acord amb la disposició addicional primera de la LOPDGDD. Malgrat l'entitat presta un servei vinculat al sector públic, no es troba dins els supòsits d'entitats obligades; amb tot, és recomanable tenir en compte els paràmetres i requeriments definits l'ENS a l'hora d'establir mesures de seguretat aplicables.

Àrees de millora

●	Els documents de seguretat aportats a aquesta auditoria i el "*Annex 17 Sistema de seguretat i pla de contingències*" demostren i evidencien que s'han tingut en compte els riscos que impliquen les activitats de tractament de dades i que s'han implementat mesures de seguretat en relació a aquests riscos. Aquestes mesures, tal com estan definides i plantejades, responen en bona mesura a les que ja preveia l'antic RLOPD i resulten adequades. En tot cas, caldrà que aquestes mesures sempre es puguin revisar i actualitzar, tenint en compte les necessitats dels nous tractaments que puguin sorgir i els principis de privacitat per disseny i per defecte. Constatem l'evidència documental de la realització d'anàlisis de riscos en relació a les diferents activitats de tractament, tal com es pot comprovar amb el document ""*AL-1-RS-PDP-026001-ca Avaluació de Riscos 2020 v2*". Aquest document és correcte, perquè preveu les circumstàncies i característiques dels diferents tractaments i les mesures de seguretat que els corresponen. No obstant, caldria que inclogués també una previsió o valoració sobre la necessitat de realitzar o no una avaluació d'impacte (AIPD) en relació a cadascun dels tractaments. Cal tenir en compte que la introducció de noves tecnologies (com ara els controls per empremta digital o l'adopció d'aplicacions de missatgeria instantània) poden implicar riscos rellevants per als drets de les persones i més encara si es tracten dades de caràcter sensible o de categoria especial, com són les dades relatives a la salut personal, o dades que permeten la identificació unívoca, com l'empremta digital. Sobre l'obligatorietat de realitzar o no una AIPD, caldrà tenir en compte l'art. 35 RGPD i els criteris de la llista de tractaments especificats per l'AEPD. Hem d'entendre tot això també vinculat a l'obligació que té l'entitat de gestionar el risc en general i el principi de responsabilitat proactiva. En el cas de l'entitat, seria particularment necessari revisar la necessitat de realitzar una avaluació d'impacte sobre els controls per empremta digital.

	Les autoritats de control han publicat guies sobre criteris i metodologia a emprar en l'elaboració d'avaluacions d'impacte, tant l'Autoritat Catalana de Protecció de Dades (APDCAT) com l'Agència Espanyola de Protecció de Dades (AEPD). També recentment l'AEPD ha publicat una eina online sobre la matèria que s'anomena GESTIONA. Degut a la complexitat d'aquests informes, el més habitual és encarregar-ne l'elaboració a empreses o entitats especialitzades, sota la supervisió del DPD de l'entitat. D'altra banda, cal tenir en compte que no seria correcte que sigui el DPD qui elabori directament els informes d'avaluació d'impacte, ja que això plantejaria problemes de compatibilitat amb les seves altres funcions d'assessorament i supervisió.

5.4. DELEGAT DE PROTECCIÓ DE DADES

Base legal: Article 37 RGPD

Segons la informació i evidències proporcionades, l'entitat va procedir a nomenar internament el Sr. Javier Remacha Fuentes com a delegat de protecció de dades (DPD). Aquest nomenament es va comunicar a l'APDCAT el dia 01/05/2018. L'autoritat de control va comunicar la recepció de la comunicació en data 11/05/2020, assignant-li el codi 0199/698/2018. S'aporten i es comproven la comunicació i la resposta de l'autoritat de control.

La figura del DPD ja consta a tots els documents de seguretat, juntament amb una descripció exhaustiva de les seves funcions. En general, s'ha fet difusió suficient de la figura del DPD. Tal com es pot comprovar, els textos legals que fa servir l'entitat per a informar sobre el tractament de les dades, de conformitat amb l'art. 13 RGPD, ja informen també sobre l'existència de la DPD i la forma de comunicar-s'hi. També apareix en la informació legal que es proporciona a tot el personal a través del manual d'acollida. Aquesta informació es proporciona a totes les noves incorporacions al personal i és consultable a través de la intranet corporativa.

L'existència del DPD no consta a l'organigrama de l'entitat, tal com es pot comprovar amb el document d'organigrama aportat i al manual d'acollida.

El DPD té altres responsabilitats a l'entitat. En particular, és responsable de l'Oficina Tècnica de Suport a la Gestió. Entre d'altres, desenvolupa tasques de protecció de dades, prevenció de riscos laborals, comunicacions i relacions públiques i de sistema de gestió. Com que no té altres funcions que impliquin la presa de decisions sobre el tractament de les dades que realitza l'entitat, el càrrec de DPD resulta compatible i sense conflicte d'interès. D'altra banda, el DPD té coneixements jurídics i demostrada formació i experiència en matèria de protecció de dades. En particular, consta que ha assistit a la formació específica impartida per la Unió Catalana d'Hospitals en aplicació del seu Codi Tipus.

D'acord amb les informacions i evidències proporcionades, no hi ha un document específic de pla d'actuació del DPD. No obstant, al Document de Seguretat ja es defineixen un seguit d'accions i tasques que s'atribueixen a la DPD i que constitueixen una definició sobre la seva actuació; el DPD envia mensualment a direcció un informe sobre revisió d'accessos i cada 6 mesos envia un informe sobre incidències detectades. També es preveuen plans de formació sobre protecció de dades coordinats pel DPD. En particular, es té en compte el document "*5 Formació LOPD 2020_BDN*", que és una presentació sobre protecció de dades que es proporciona a tot el personal per defecte.

No detectada

▲	Malgrat no haver-hi una obligació expressa, com a mesura de difusió del seu nomenament recomanem que s'incorpori la figura de la DPD a l'organigrama de l'entitat, per tal de demostrar que l'entitat en fa difusió pública. D'altra banda, atesa l'excepcionalitat viscuda arran de la declaració de l'estat d'alarma motivada per la crisi sanitària de la Covid-19, és possible que hi hagi hagut circumstàncies innovadores o excepcionals pel que fa al tractament de les dades. Seria recomanable que el DPD documentés per escrit canvis i/o incidències que s'hagin pogut produir eventualment durant aquest període.

5.5. ENCARREGATS DEL TRACTAMENT I PROVEÏDORS SENSE ACCÉS A DADES

ENCARREGATS DEL TRACTAMENT

Base legal: Article 28 RGPD i disposició transitòria cinquena LOPDGDD

Els diferents documents de seguretat de GUTTMANN ja contenen instruccions i previsions sobre com l'entitat ha de procedir correctament en la seva relació amb encarregats del tractament de les dades, d'acord amb la normativa vigent. En concret, s'hi estableix la necessitat de tenir contractes signats amb els encarregats del tractament i fer-los acceptar les mesures de seguretat definides pel responsable. A aquest efecte, s'hi preveu que als contractes mercantils s'hi afegeixi una clàusula, i que en alguns casos, s'incorpori una ampliació de contracte a contractes ja signats.

El document Excel "*Llistat actualitzat gener 2020*" aportat a aquesta auditoria conté una relació exhaustiva i actualitzada de proveïdors de servei. Mitjançant aquest document, el DPD pot controlar aspectes relatius a aquests proveïdors: si són o no encarregats, la data del contracte, la seva vigència i si tenen o no la consideració d'encarregat. Comprovem també que l'entitat disposa d'un model de contracte d'encàrrec de tractament de dades degudament actualitzat i ajustat al RGPD.

No consta que hi hagi implementat un protocol sobre selecció de proveïdors, per tal de poder garantir per part del responsable del tractament que es contracta amb qui reuneix els requisits i s'ajusta als requeriments de la normativa. De nou, amb la crisi del coronavirus s'ha vist que sovint moltes incidències provenen de proveïdors que no sempre són capaços de garantir la seguretat en el tractament de les dades.

D'altra banda, un cop revisada una mostra aportada de contractes d'encàrrec de tractament de dades personals, fem els següents comentaris al respecte:

ET DETECTATS	SERVEI PRESTAT	CON-TRAC-TE	COMENTARIS
Do While Studio, S.L.	Realització del disseny de la interfície de la Nova Història Clínica	✓	El contracte és ajustat a la normativa vigent aplicable.
La Riera Pàdel, S.L.	Gestió d'activitats a Sport&Life Guttmann Club.	✓	El contracte és ajustat a la normativa vigent aplicable.
Cerba Internacional	Processar mostres biològiques de pacients i personal adscrit i incorporar-ne resultats.	✓	El contracte és ajustat a la normativa vigent aplicable.
Máster S.A., de Ingeniería y	Gestió documental relativa al projecte de	✓	El contracte és ajustat a la

Arquitectura	construcció de nou edifici de Guttmann Barcelona.		normativa vigent aplicable.
Asesores Corporativos, S.A.	Assessorament legal en medi ambient, prevenció de riscos laborals i seguretat industrial.	✓	El contracte és ajustat a la normativa vigent aplicable.
Sodexo Iberia, S.A.	Serveis de cafeteria i cuina. Disseny i control de dietes de pacients.	✓	El contracte és ajustat a la normativa vigent aplicable.
Leader Network Marketing, S.L. (UCAE)	Servei de gestió administrativa i documental per a la coordinació d'activitats.	✓	El contracte és ajustat a la normativa vigent aplicable.
Professors de l'àrea de docència.	Serveis de docència	×	Els professors de l'àrea de docència són encarregats del tractament de les dades dels alumnes.

Segons disposa la Disposició transitòria cinquena de la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i Garantia dels Drets Digitals, els contractes anteriors al 25 de maig de 2018, redactats d'acord amb l'antiga LOPD i que no hagin estat actualitzats o adaptats al RGPD, es mantindran vigents fins al final i, si són per termini indefinit, fins al 25 de maig de 2022. Durant aquesta vigència, qualsevol de les parts signants podrà requerir l'altra per tal de signar un nou contracte que sigui conforme al RGPD. Tot i que és possible deixar passar els terminis, el més recomanable és procedir ja a actualitzar tots els contractes d'encàrrec de tractament de dades de conformitat amb el RGPD.

A partir del 25 de maig de 2018 tots els nous contractes amb Encarregats de Tractament han de respectar el contingut que preveu l'article 28 del RGPD.

Àrees de millora

●	Com a element de millora, cal tenir en compte els professionals autònoms que tenen una vinculació mercantil amb l'entitat, com ara els professors de l'àrea de docència. Si aquests proveïdors de serveis autònoms tenen accés a dades de GUTTMANN, com és el cas d'aquests professors, haurien de signar contractes d'encàrrec de tractament de dades. Fins ara, a aquests professors se'ls ha aplicat un procediment d'acollida molt semblant al que s'aplica al personal laboral, de manera que se'ls ha fet signar un compromís de confidencialitat i se'ls ha proporcionat unes instruccions sobre

	seguretat, que han d'assumir. Això és correcte, i aporta un nivell adequat de seguretat, però el que és adequat jurídicament és considerar-los encarregats de tractament i fer-los signar un contracte com a tal. Finalment, caldria implementar un protocol sobre selecció de proveïdors, per tal de poder garantir que els encarregats del tractament contractats aplicaran condicions de seguretat d'acord amb la normativa i les instruccions del responsable del tractament. De nou, amb la crisi de la Covid-19 s'ha pogut comprovar que sovint moltes incidències provenen de proveïdors que no sempre són capaços de garantir la seguretat en el tractament de les dades.

PRESTACIONS SENSE ACCÉS A DADES

Base legal: Article 24 RGPD

Situació actual

L'entitat és conscient que determinats serveis prestats per altres persones o entitats impliquen no haver de tenir cap accés a dades personals, però podrien suposar un accés involuntari o accidental a les dades. Per prevenir aquesta situació de risc i un possible accés indegut, correspon aplicar un compromís de confidencialitat.

Amb el document Excel "*Llistat actualitzat gener 2020*" comprovem que es manté una relació actualitzada de proveïdors que tenen accés a dades, qualificats com a encarregats de tractament de dades, que es diferencien dels que no tenen accés a dades. En funció del tipus de proveïdor i de si té o no accés a dades, se li fa signar un model de contracte d'encàrrec de tractament o se li fa signar un compromís de confidencialitat que reflecteixi la realitat de la situació i preservi la confidencialitat i la seguretat de les dades, de conformitat amb el RGPD.

Tot i que no s'han aportat exemples específics de clàusules o compromisos de confidencialitat signats, comprovem que efectivament tots els proveïdors sense accés a dades ja s'identifiquen al document i que ja hi ha també un procediment previst per a fer-los signar un model de compromís de confidencialitat.

No detectada

▲	

5.6. LICITUD DEL TRACTAMENT, BASE JURÍDICA, INFORMACIÓ I CONSENTIMENT

Base legal: Articles 5, 6, 7, 8, 9, 10, 11, 12, 13 i 14 RGPD

Situació actual

En punt anterior en què es feia referència específica al RAT ja hem indicat les activitats de tractament previstes per l'entitat. Analitzem ara de manera general la legitimitat de les diferents activitats de tractament de dades que du a terme l'entitat i que es fan constar al RAT, que són les següents:

- **Pacients**

La base jurídica del tractament consisteix en la prestació de serveis d'assistència sanitària i social, conforme a l'article 9.2 lletra h) del Reglament General de Protecció de dades.

Tant per la documentació com pels treballs de camp i la informació proporcionada, comprovem que la informació legal sobre el tractament es proporciona correctament, de conformitat amb l'art. 13 RGPD. D'acord amb el document de seguretat corresponent, a cada pacient (o representant legal) se li lliura el document "*Annex 09 Autorització Pacient per al tractament de dades 2020 v2 ca*", que s'arxivarà a la història clínica degudament signat. Aquest document conté ja de forma completa tota la informació sobre el tractament de les dades i un seguit d'autoritzacions expresses que el pacient pot acceptar o no lliurement. El responsable del tractament determina que aquesta tasca correspon al servei d'admissions.

Els usos que GUTTMANN pretén realitzar de les dades amb el consentiment del pacient són pertinents i proporcionats, ja que responen a interessos del servei, de l'entitat i del propi pacient. En concret, es demana autorització per informar sobre el número de l'habitació a les visites, per emetre recordatoris de visita per mitjans electrònics, per rebre informació sobre novetats de l'entitat, per participar en enquestes de satisfacció, per tractar les dades de salut sense identificar la persona amb finalitats de recerca. Tots aquests usos són legítims, i la forma legítima de poder-los fer és a través del consentiment exprés del pacient, tal com ha previst correctament l'entitat.

- **Personal**

La base jurídica del tractament consisteix en la preparació i execució d'un contracte de treball, de conformitat amb l'article 6.1.b) RGPD. La finalitat del tractament és la gestió i manteniment de la relació laboral.

L'entitat s'encarrega directament de l'elaboració de les nòmines i la gestió laboral mitjançant el programa INTEGRHO. Tots els membres del personal tenen una targeta personal que serveix per identificar el professional, però també per dur a terme el control d'accessos a determinats espais, el control de fitxatges i el control horari.

En general, quan una persona entra a treballar a GUTTMANN i es recullen les seves dades, s'aplica un procés d'acollida que implica proporcionar i fer signar, entre d'altres, els següents documents relatius a protecció de dades:

- Informació sobre protecció de dades i compromís de confidencialitat.
- Bones pràctiques dins els manuals d'acollida.
- Formació LOPD 2020.

Tant el document d'informació i compromís com el document de bones pràctiques han estat aportats per l'entitat a aquesta auditoria i, després de revisar-los, corroborem que en general són adequats i actualitzats pel que fa al compliment de l'obligació d'informar sobre el tractament de les dades, d'acord amb l'art. 13 del RGPD.

Pel que fa als processos de selecció, es poden vehicular a través de la web (on ja hi ha un avís legal sobre el tractament de les dades) o mitjançant anuncis al portal Linkedin, tot i que en molts casos són antics estudiants de màster i postgrau o personal en pràctiques els que acaben convertint-se en treballadors de l'entitat. Ja no es reben habitualment currículums per correu electrònic, com passava abans. En tot cas, per al cas que es rebés un email amb un currículum, es conserva encara un model de resposta que incorpora la informació de l'art. 13 RGPD.

Pel que fa a l'ús de la dada de la imatge del treballador, la base jurídica prevista és la prestació del consentiment de l'interessat, i seria només per a finalitats de comunicació. El model documental "*Autorització presa d'imatges i veu 2020 ca*" presenta una informació correcta sobre el tractament de la dada de la imatge del personal, d'acord amb l'art. 13 del RGPD, i permet a la persona interessada prestar el seu consentiment per al tractament.

Pel que fa a la vigilància de la salut, és un servei que li presta a l'entitat l'empresa Aspy Prevención, per a la qual cosa es fa servir una aplicació pròpia d'aquesta empresa. La revisió mèdica és voluntària generalment, i es dona l'opció a negar-s'hi. En alguns casos, tanmateix, com per exemple en el del personal que treballa amb rajos X, la revisió és obligatòria.

A partir de la crisi generada per la Covid-19 i d'acord amb l'autoritat sanitària, s'ha establert un procediment pel qual l'empresa de prevenció pot aportar també una informació sobre la sensibilitat d'un pacient al virus, a banda de la clàssica informació sobre l'aptitud. D'altra banda, la necessitat d'augmentar el teletreball ha portat a la necessitat d'elaborar un acord específic com a annex del contracte de treball, el qual, un cop analitzat, resulta adequat a la finalitat de gestionar aquesta situació sobrevinguda sense implicar un tractament addicional de dades.

Des de GUTTMANN també s'han organitzat proves serològiques amb els treballadors, que s'han dut a terme a l'hospital Can Ruti, però en cap cas l'entitat no té accés als resultats; només la pròpia persona pot accedir als resultats a través del portal "La meva salut". L'entitat no té dades sobre la immunitat que puguin haver desenvolupat determinades persones de forma individual.

No consta que l'entitat faci un ús del telèfon o del correu electrònic personal de les persones treballadores o qualsevol altra dada que se situï més enllà de la relació laboral, llevat que calgui realitzar alguna comunicació puntual i esporàdica. En aquest sentit, no es detecten tractaments que puguin tenir la condició de desproporcionats o innecessaris des del punt de vista de la gestió de la relació laboral.

- **Administració**

Aquest tractament respon al desenvolupament de relacions comercials amb persones jurídiques i, per tant, a l'establiment de mesures contractuals. Aquesta seria la base jurídica del tractament.

Tot i que, en general, l'entitat no recull ni manté dades personals de clients o proveïdors que siguin persones físiques, no es pot descartar la possibilitat que, en l'establiment de relacions comercials, hi hagi tractaments de dades personals de persones físiques, bé sigui en representació de persones jurídiques o bé en el seu propi nom. Tal com preveu el document de seguretat, aquest tractament no disposa de moment d'un document o instrument específic de legitimació, ja que el tractament es fonamenta en unes relacions que no impliquen tractament de dades, però manté les mateixes mesures de seguretat i garanties que estan previstes per a d'altres tractaments (delegat de protecció de dades, registres, etc.).

- **Reclamacions**

Aquest tractament respon a la necessitat legal de tenir un procediment de reclamacions i/o suggeriments, de conformitat amb la Llei 15/1990, d'ordenació sanitària de Catalunya, i amb la Instrucció 03/2004. Per tant, la base legítima del tractament és el compliment d'una obligació legal.

Aquest procediment el pot iniciar l'usuari dels serveis emplenant un formulari. En aquests formularis ja s'inclou una nota a peu de pàgina que informa adequadament sobre el tractament de les dades, tal com preveu l'art. 13 RGPD.

És el personal de l'àrea d'atenció a l'usuari que s'encarrega de proporcionar aquests formularis i fer-ne seguiment.

- **Externs**

En un únic document de seguretat, GUTTMANN té prevista la regulació de la seva relació amb aquells col·lectius de persones físiques amb qui manté algun tipus de vinculació comercial o de prestació de serveis diferent de les previstes en d'altres tractaments. Per tant, s'inclourien en aquest apartat els següents col·lectius, tal com estableix el document de seguretat "*Document de Seguretat Fitxer Externs 2019*". A aquests tractaments hi afegiríem el de vídeos en la formació, ja que preveu la captació de la dada de la imatge i la veu de persones vinculades a la formació (alumnes i professors, que tenen la condició de col·laboradors externs).

- Voluntaris
- Treballadors en benefici de la Comunitat
- Amics de l'Institut Guttmann
- Empreses i col·laboradors externs
- Alumnes
- Videos formació

Aquests col·lectius coincidirien amb les activitats de tractament identificades al RAT com a "Externs Voluntaris", "Externs TBC", "Externs Amics", "Externs docència" i "Video formació".

La base jurídica del tractament seria generalment, en tots aquests casos, l'existència d'una vinculació contractual, de conformitat amb l'article 6.1.b) RGPD i la finalitat del tractament seria la gestió dels serveis corresponents, tant si aquests col·lectius actuen com a receptors o prestadors. En el cas dels vídeos, però, la base jurídica és el consentiment de la persona interessada, que ha de signar un document de consentiment exprés.

D'acord amb la documentació aportada relativa a la gestió concreta de cada col·lectiu i dels serveis corresponents, es comprova específicament que en cada cas hi ha un contracte o matrícula específica (també en el cas dels voluntaris), un procediment d'acollida, unes instruccions sobre seguretat, una informació sobre protecció de dades (inclosa al contracte) i un compromís de confidencialitat que la persona ha de signar.

Es detecta que en el cas del procediment d'acollida dels MIR, la informació sobre protecció de dades és conforme a l'antiga legislació sobre protecció de dades, i caldria actualitzar-la.

En el cas dels col·laboradors externs, que inclouen els professors, es recullen les seves dades mitjançant un formulari que ja inclou la informació de l'art. 13 RGPD. No obstant, no hi ha un contracte d'encàrrec de tractament de dades signat amb aquests professors.

En el cas dels "*Amics de l'Institut Guttmann*", són persones que lliurement decideixen fer donacions puntuals o periòdiques a l'entitat i, a canvi, reben alguna prestació. Aquestes persones proporcionen a través de la web de GUTTMANN, on hi ha un formulari de recollida de dades i un avís legal. Es comprova que la informació que proporciona aquest avís legal de la web s'ajusta a l'antiga legislació; per tant, no és correcte i caldria actualitzar-lo.

La gestió dels treballadors en benefici de la comunitat i el tractament de les seves dades es fonamenta en la col·laboració que l'entitat manté amb el Departament de Justícia, de qui depenen les dades en darrera instància.

No es detecten tractaments que puguin tenir la condició de desproporcionats o innecessaris des del punt de vista de la gestió dels serveis i de la finalitat del tractament.

- **Externs RRPP:**

El RAT identifica un tractament dit "Externs", que no apareix desenvolupat al document de seguretat titulat "Externs". Es tracta de les dades, coincidents en molts casos amb altres categories d'interessats relatius a GUTTMANN, que es tracten amb la finalitat de facilitar la comunicació de l'entitat. La base jurídica és el consentiment de la persona interessada.

En el cas de la revista "*Sobre Ruedas*", que té 12.000 subscriptors, s'envia als pacients que ho han autoritzat expressament i per escrit durant la seva primera visita.

La revista "*Fulls*" s'envia als treballadors de GUTTMANN per defecte, ja que s'entén aquí que pot aplicar-s'hi una base jurídica d'interès legítim. Això és correcte, si es preveu la possibilitat que un treballador exerceixi el seu dret d'oposició i s'atén correctament.

Pel que fa a la comunicació d'esdeveniments que organitza l'entitat, les convocatòries es llancen generalment a través de xarxes socials, com ara Twitter i Linkedin. En general, però, també es crea una web específica per a cada esdeveniment a través d'una empresa subcontractada. Els participants poden inscriure's a través d'un formulari de la web, on ja consta un avís legal amb informació de l'art. 13 RGPD. En aquest cas, el formulari també preveu que es presti el consentiment per al tractament de les dades.

D'acord amb les informacions proporcionades, en alguns casos s'han comprat dades de caràcter personal per realitzar-hi enviaments, però en aquest cas no hi ha hagut mai cap comunicació de dades a GUTTMANN. És a dir, l'entitat no hi ha tingut cap accés, sinó que s'ha limitat a generar el contingut perquè fos l'empresa gestora de bases de dades la que fes l'enviament.

En qualsevol cas, sempre que s'ha volgut fer una activitat de difusió per xarxes que impliqui fer servir dades d'una persona, se li ha demanat el consentiment exprés, de forma prèvia i per escrit.

- **Externs GBL i Externs S&L GC:**

Aquestes dues activitats de tractament corresponen a dades obtingudes i tractades en la prestació dels serveis Guttmann Barcelona Life i Sport&Life Guttmann Club. Aquests dos tractaments no estan desenvolupats al document de seguretat corresponent als Externs, ni se n'ha analitzat informació o documentació específica en aquesta auditoria. No obstant, consisteixen en una extensió de la prestació assistencial sòcio-sanitària que realitza l'entitat. La base jurídica seria, per tant, la prestació sòcio-sanitària, juntament amb el compliment del contracte que va vinculat a la prestació d'aquests serveis.

En el cas de Guttmann Barcelona Life, consisteix en un equipament social format per apartaments domotitzats i adaptats. A través d'un procediment de selecció, persones amb discapacitat física o mobilitat reduïda poden optar a beneficiar-se dels serveis que implica aquest equipament, entre ells una residència adaptada. En tot cas, l'usuari del servei ha de signar un contracte de servei residencial com a requisit imprescindible.

En el cas de Sports&Life Guttmann Club, és un servei adreçat no només a antics pacients de l'hospital i a persones del seu entorn, sinó també a qualsevol persona amb una discapacitat d'origen neurològic. Es pretén fomentar la pràctica de l'esport i la realització d'activitats socials i culturals entre persones dels col·lectius esmentats.

A falta de documentació específica per analitzar, constatem la necessitat de revisar que en els procediments de recollida de dades d'aquests serveis es proporciona la informació sobre el tractament de les dades de conformitat amb l'art. 13 RGPD, bé sigui al contracte, bé sigui a través de qualsevol altre document.

- **Videovigilància:**

A través d'aquesta activitat de tractament es capta la imatge i/o la veu de persones que es troben a les instal·lacions de GUTTMANN, amb la finalitat de preservar la seguretat i controlar els accessos. Per tant, la base legal d'aquest tractament seria el compliment d'una missió en interès públic, d'acord amb l'article 6.1.e) del RGPD.

D'acord amb el document de seguretat específic sobre aquest tractament, el compliment del deure d'informació es fa a través d'un cartell informatiu col·locat a totes les portes d'entrada del recinte de l'hospital, tant si són entrades generals, de treballadors o d'entrada de mercaderies, en un lloc ben visible segons el model legalment establert. D'altra banda, segons aquest mateix document, l'entitat disposa d'impresos disponibles que contenen la informació completa sobre el tractament, de conformitat amb l'art. 13 RGPD. Està previst que hi hagi procediments d'exercicis de drets, limitats al fet que les dades recollides es conserven només durant quinze dies.

El tractament descrit és correcte i no planteja problemes de legitimitat o licitud.

- **Investigació.**

La recerca és una activitat fonamental de GUTTMANN i constitueix generalment un tractament de dades sensibles o de categoria especial. D'acord amb les informacions proporcionades, l'entitat du a terme diferents activitats de recerca que poden distingir-se entre estudis retrospectius, estudis prospectius i Cohorts. Els estudis retrospectius es duen a terme sempre amb dades seudonimitzades o directament anonimitzades. En el cas dels estudis prospectius i el projecte Cohort, el tractament es fonamenta jurídicament en l'obtenció del consentiment de l'interessat, que pot revocar en qualsevol moment. Els consentiments utilitzats són avaluats sempre per un Comitè d'Ètica i inclouen una informació exhaustiva sobre el tractament de les dades.

En general, tota la recerca que du a terme l'entitat es fa aplicant mesures de seudonimització. En concret, s'aplica un sistema de codificació sobre l'aplicació que gestiona la història clínica, de manera que se li assigna un número i s'aconsegueix la dissociació efectiva de les dades.

En general, la seudonimització que aplica GUTTMANN està plantejada de manera correcta, perquè només l'investigador principal té la clau per reidentificar, en cas necessari. La resta d'investigadors tracten les dades sense poder identificar en cap cas les persones. No obstant, d'acord amb les informacions proporcionades, no hi ha un compromís de no reidentificació que se'ls faci signar. És important en aquest punt tenir en compte els requisits legals de la seudonimització, segons el model descrit a la disposició addicional dissetena, lletra d), de la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades i garantia dels drets digitals, que són:

- Separació tècnica i funcional entre l'equip investigador i els que fan la seudonimització.
- Compromís de confidencialitat i de no fer cap activitat de reidentificació signat per l'equip investigador.
- Aplicació de mesures per evitar la reidentificació.

Finalment, cal tenir en compte les particularitats dels projectes Cohort, que impliquen sotmetre els participants a proves de ressonància magnètica i preveuen intensificar-ne la monitorització, recollint dades dels seus mòbils, controlant l'exercici diari que fan, la seva mobilitat, etc. Malgrat aquesta previsió, no consta que s'hagi fet una valoració sobre la necessitat de realitzar o no una avaluació d'impacte sobre aquest tractament. Cal tenir en compte que és obligatòria la realització d'avaluacions d'impacte en relació a tractaments de dades que impliquin un alt nivell de risc per als drets i llibertats de les persones, sobretot si es preveuen elements de monitorització o la introducció de noves tecnologies en el tractament, entre d'altres, de conformitat amb l'art. 35 RGPD i els criteris de la llista de tractaments especificats per l'AEPD. Hem d'entendre tot això també vinculat a l'obligació que té l'entitat de gestionar el risc en general i el principi de responsabilitat proactiva.

En el cas particular de l'entitat, seria recomanable revisar la necessitat de realitzar una avaluació d'impacte sobre l'activitat de recerca en general que du a terme i probablement també en relació a algun projecte específic que pugui implicar un risc més elevat.

Les autoritats de control han publicat guies sobre criteris i metodologia a emprar en l'elaboració d'avaluacions d'impacte, tant l'Autoritat Catalana de Protecció de Dades (APDCAT) com l'Agència Espanyola de Protecció de Dades (AEPD). També l'AEPD ha publicat una eina online sobre la matèria que s'anomena GESTIONA. Degut a la complexitat d'aquests informes, el més habitual és encarregar-ne l'elaboració a empreses o entitats especialitzades, sota la supervisió del DPD de l'entitat. No seria correcte que fos el DPD qui elaborés directament els informes d'avaluació d'impacte, ja que plantejaria problemes de compatibilitat amb les seves altres funcions d'assessorament i supervisió.

- **GNPT**

Brain Health Solutions és una empresa *startup* participada per GUTTMANN i Grupo ICA per a la comercialització i manteniment d'una plataforma informàtica dins el sector sòcio-sanitari. El nom d'aquesta plataforma és GNPT i està destinada a tractar dades de pacients.

D'acord amb les informacions proporcionades, se signen contractes d'encàrrec de tractament de dades amb els clients, que han estat revisats per la Unió Catalana d'Hospitals. Quan la plataforma es ven a altres centres de salut, l'encarregat del tractament és Brain Health Solutions i el centre de salut actua com a responsable del tractament. En aquest cas, la base jurídica del tractament seria l'existència del contracte de prestació de serveis. Quan el servei es presta als pacients de GUTTMANN, l'entitat actua com a responsable del tractament i Brain Health Solutions com a encarregada. La base jurídica seria, en aquest cas, la mateixa prestació assistencial. D'altra banda, en tots els casos, Grupo Ica actua com a encarregada del tractament.

Constatem que s'ha fet una anàlisi de riscos específica respecte a aquest tractament, la qual s'ha materialitzat en un document i s'ha aportat a aquesta auditoria. D'aquesta manera, s'han tingut en compte riscos i aspectes de licitud, i s'han pogut minimitzar de forma positiva.

D'acord amb les informacions proporcionades, la plataforma disposa d'una intel·ligència artificial i ofereix propostes terapèutiques en relació als pacients. No obstant, tal com matisen els responsables de comercialitzar la plataforma, sempre hi ha un professional humà que pren les decisions. Descartem, per tant, l'existència d'una situació de risc, com podria ser una presa de decisions automatitzada.

Els servidors de la plataforma es troben a Madrid. No consta que hi hagi transferències internacionals contràries al dret.

No es detecten usos de dades que no siguin ajustats a la finalitat o que no estiguin justificats.

- **BBHI - Barcelona Brain Health Initiative**

Aquest tractament no deixa de ser un projecte de recerca que presenta algunes especificitats. Els participants es registren i proporcionen les seves dades a través de la web del projecte, a l'adreça https://bbhi.cat/participa, on han d'emplenar un formulari i llegir necessàriament un primer avís legal sobre el tractament de les dades, que és conforme a l'art. 13 RGPD.

El document de seguretat no indica quina és la base jurídica definida pel responsable del tractament en aquest cas, però resulta clar que és el consentiment del participant, ja que posteriorment a registrar-se haurà d'acceptar expressament una informació sobre el tractament de les dades i tindrà l'opció manifesta de clicar "No hi estic d'acord" i deixar de formar part de l'estudi. El document que ha d'acceptar el participant es diu "*Full d'informació per als voluntaris participants de l'estudi Barcelona Brain Health Iniciative*", que conté també una informació exhaustiva sobre l'estudi, les seves fases i les seves implicacions. En aquest full s'informa a bastament sobre la finalitat del tractament, que en l'anterior avís legal de la web es presentava més difús i poc clar. No obstant, el compliment de l'art. 13 RGPD es feia a través del primer avís legal.

- **Blanqueig de capitals**

Aquest tractament respon a la necessitat legal de conservar les dades de les persones que fan donacions econòmiques, en compliment de la Llei 10/2010, de 28 d'abril, de prevenció del blanqueig de capitals i del finançament del terrorisme. Per tant, la base legítima del tractament és el compliment d'una obligació legal. En realitat, més que una activitat de tractament completa, és la conservació d'unes dades obtingudes en una altra activitat de tractament.

Quan els donants són persones físiques, com per exemple els "*Amics de l'Institut Guttmann*", que poden fer donacions a través de la web, seria convenient que s'informés d'aquest tractament en l'avís legal que hi ha al costat del formulari. Ara mateix no es proporciona aquesta informació.

Les dades que es conserven són les mínimes imprescindibles, i es mantenen durant el temps de conservació prevista a la llei.

- **Empremtes digitals**

En alguns casos, es recull la dada de l'empremta digital del treballador. Aquest tractament no està descrit en un document de seguretat, però, d'acord amb la informació proporcionada, la dada de l'empremta digital es faria servir a GUTTMANN per garantir l'accés de determinats membres del personal a certes zones restringides, com ara el quiròfan, el gimnàs, l'àrea mèdica i l'àrea d'infermeria. La base jurídica del tractament seria l'exercici de potestats de control per part de l'empresa.

No consta en la documentació proporcionada que es faci servir un model d'informació sobre l'ús de la dada de l'empremta digital o que hi hagi un procediment de legitimació definit prèviament pel responsable del tractament. No consta que hi hagi hagut tampoc una revisió de la necessitat de realitzar una avaluació d'impacte sobre l'ús de l'empremta digital, malgrat tractar-se d'una dada sensible que pot requerir la realització obligada d'aquesta anàlisi, també segons el criteri de l'Autoritat Catalana de Protecció de Dades. Per tant, en aquest cas, és necessari realitzar aquesta revisió i plantejar-se la necessitat de realitzar una avaluació d'impacte sobre aquest tractament, d'acord amb els criteris legals ja descrits anteriorment.

No conformitat

▼	Vegeu els comentaris anteriors, especialment les parts subratllades, que són les que fan referència de forma més específica a àrees d'incompliment i millora.

5.7. DRETS DE LES PERSONES INTERESSADES

Base legal: Articles 13-23RGPD

Situació actual

L'entitat ja disposa dels models i ja té un protocol definit per a l'exercici dels drets de les persones interessades, com es pot comprovar en l'apartat corresponent de tots els documents de seguretat. A l'annex 7 dels documents de seguretat hi ha els diferents formularis i models corresponents als drets d'accés, rectificació, supressió, oposició, limitació i portabilitat. Per tant, ja està previst a GUTTMANN un procediment actualitzat i ajustat al RGPD per a l'exercici dels drets d'accés, rectificació, oposició, supressió, limitació del tractament i portabilitat de les dades.

En general, el procediment preveu que el contacte amb el DPD per a l'exercici d'un dret es faci enviant un correu electrònic a protecciodades@guttmann.com.

D'acord amb les informacions proporcionades, a l'àrea d'admissions s'atendrien de forma ordinària peticions d'accés o de rectificació de dades de la història clínica, d'acord amb un procediment que garanteix la identitat i el registre, i només en cas necessari es demanaria la intervenció del DPD.

Per ara, no consten procediments d'exercici de drets tramitats formalment segons el procediment determinat pel responsable. En tot cas, el DPD és qui s'encarregaria de gestionar, registrar i contestar aquestes peticions, d'acord amb el procediment previst.

No detectada

▲	

5.8. NOTIFICACIONS DE VIOLACIONS DE SEGURETAT

Base legal: Articles 24 i 33 RGPD

Situació actual

L'entitat aporta evidències i proporciona informació que acrediten l'existència d'un procediment intern de registre d'incidències que es gestiona des de l'àrea de sistemes informàtics. En tots els documents de seguretat s'hi descriu el procediment relatiu a la comunicació interna, anàlisi i registre d'incidències de seguretat. S'hi descriu també què s'entén per incidència i com s'han de registrar, però no consta documentat un procediment de notificació de violacions de seguretat a l'autoritat de control que correspongui al DPD. No hi consta tampoc que això sigui una de les funcions del DPD.

A través d'un annex 4 s'aporten evidències de diferents incidències en el tractament de les dades que han estat comunicades i registrades per l'entitat, que inclouen la detecció d'un error en la data d'un curs clínic, l'alta d'un nou usuari per connexió remota o la impossibilitat d'accedir a una aplicació. En general, totes són incidències de tipus informàtic i es gestionen com a tal, malgrat que també puguin tenir una transcendència des del punt de vista de protecció de dades.

Als apartats de bones pràctiques i codi ètic dels manuals d'acollida, on trobem les instruccions que es proporcionen a treballadors, voluntaris, personal del MIR i altres col·lectius que intervenen en el tractament de les dades de GUTTMANN, no hi apareix una instrucció sobre la necessitat de comunicar incidències o violacions de seguretat.

No consta, d'acord amb les informacions proporcionades, que hi hagi hagut fins ara una violació de seguretat que hagi hagut de ser comunicada a l'autoritat de control, en aplicació de l'obligació legal de comunicar violacions de seguretat.

Durant els treballs de camp, el personal entrevistat coneix generalment la necessitat de comunicar a l'àrea de sistemes informàtics incidències relatives al tractament de les dades.

Àrees de millora

▼	El procediment que té implementat l'entitat respon sobretot als paràmetres de l'antic Reglament de protecció de dades, que preveia la necessitat i l'obligació de mantenir un registre d'incidències com a mesura de seguretat. Malgrat tot, el registre és una mesura de seguretat adequada i necessària, que permet a l'entitat tenir coneixement de les incidències que es van produint i solucionar-les de manera oportuna. No obstant, hem de tenir en compte que el nou RGPD preveu l'obligació de comunicar a l'autoritat de control les violacions de seguretat que es detectin a l'entitat, i és el DPD la persona encarregada de dur a terme aquestes comunicacions. Per tant, cal adaptar el procediment actual de manera que incorpori la supervisió i participació del DPD, que haurà de valorar, en cada cas, si procedeix o no realitzar la comunicació de la incidència registrada a l'autoritat de control com a violació de seguretat. En aquest sentit, seria convenient que la supervisió, control i notificació de les incidències de seguretat es definís com a una funció pròpia

	del DPD també als documents de seguretat. D'altra banda, tot i que es pot comprovar que el personal en general té coneixement sobre l'existència de la necessitat de comunicar les incidències, recomanem que es proporcionin per escrit a tot el personal les oportunes instruccions sobre la seva obligació de comunicar incidències i violacions de seguretat de forma immediata al DPD. Aquestes instruccions poden incorporar-se idealment al manual de bones pràctiques o codi ètic que es proporciona en els procediments d'acollida.

5.9. DIFUSIÓ DE FUNCIONS I OBLIGACIONS

Base legal: Articles 24 i 25 RGPD

Situació actual

D'acord amb les evidències aportades (procediments d'acollida, manuals de bones pràctiques disponibles a la intranet, documents de formació sobre protecció de dades, etc.) l'entitat ja ha realitzat suficients accions de difusió destinades a proporcionar informació i instruccions als treballadors sobre les seves obligacions en matèria de protecció de dades i les mesures de seguretat aplicables.

Tots els procediments d'acollida que se segueixen a GUTTMANN (tant pel que fa a personal laboral, com mercantil, estudiantil o voluntari) preveuen proporcionar per escrit instruccions fonamentals i directrius sobre protecció de dades ja des d'un moment inicial. Aquestes instruccions tenen la consideració de bones pràctiques o codi ètic, segons el procediment d'acollida. També dins els procediments d'acollida es preveu proporcionar una formació inicial sobre protecció de dades. D'aquesta manera, es garanteix un coneixement fonamental sobre mesures de seguretat, funcions i obligacions del personal en matèria de privacitat i seguretat. Tots aquests documents, d'altra banda, es troben sempre disponibles a la intranet per a tot el personal.

En definitiva, resulta clar que s'estaria complint la necessitat de difondre les obligacions i les mesures de seguretat específiques que tot el personal ha de conèixer i aplicar. Només com a aspecte a millorar, tal com s'ha evidenciat en el punt anterior, es troba a faltar una definició del procediment de registre d'incidències i notificació de violacions de seguretat en les citades instruccions proporcionades durant els procediments d'acollida.

Àrees de millora

●	Tot i que el manual de bones pràctiques previst per l'entitat ja inclou mesures de seguretat adequades, recordem que caldria incloure-hi l'obligació del personal de comunicar qualsevol incidència o violació de seguretat al DPD, tal com hem comentat al punt anterior.

II – BLOC DE MESURES DE SEGURETAT

5.10. DILIGÈNCIES DELS ACCESSOS

L'establiment del control de l'accés de persones autoritzades a les dades personals: evitar pantalles desateses, documents en zones d'accés públic, etc. Cal procedir a bloquejar el dispositiu o bloquejar la sessió en absentar-se del lloc de treball.

Situació actual

La política sobre restricció d'accessos es troba definida en bona mesura als documents de seguretat de l'entitat i al document "*Annex 17 Sistema de seguretat i pla de contingències*". En aquests documents es fan constar els diferents recursos informàtics que es fan servir a l'organització i els controls que s'apliquen en el seu accés.

Tal com es pot comprovar a la documentació citada, l'entitat ja ha previst la necessitat que l'accés a les dades i recursos del lloc de treball estigui limitat en funció de les responsabilitats laborals de cadascú.

Els entorns informàtics fonamentals a què ha d'accedir el personal per al tractament de les dades són el domini, el correu electrònic (si és personal intern) i les aplicacions assistencials, si és el cas. Quan entra un treballador nou a l'entitat, responsables de recursos humans informen al responsable informàtic sobre el perfil d'accés que ha de tenir. Aleshores, se li assigna al nou usuari un nom d'usuari i una contrasenya i se li comuniquen en un sobre tancat. En el mateix sobre té instruccions per canviar la contrasenya durant el primer accés.

Per a l'accés als entorns de tractament de dades, sempre es requereix la introducció de contrasenya unipersonal, que caduca i ha de renovar-se cada 3 mesos. La contrasenya ha de complir determinats requisits de complexitat (ha de tenir un mínim de 8 caràcters i contenir caràcters alfanumèrics). S'aplica una limitació dels intents d'accés fallits que fa que després de 3-5 intents d'accés fallits (segons l'entorn) es bloquegi la contrasenya. Finalment, també és important tenir en compte que està implementat un sistema de bloqueig per inactivitat com a política de domini, el qual bloqueja l'estació de treball després de 10 minuts d'inactivitat. En el cas de les aplicacions assistencials, aquest temps és de 3 minuts.

Els entorns informàtics disposen d'antivirus Windows McAffee i Antispam Beluga, i l'accés a internet està controlat per Firewalls perimetrals.

El document de bones pràctiques que es proporciona al personal també preveu mesures de seguretat i control que tots els treballadors i col·laboradors han de complir, sobretot en relació als accessos segurs a les dades i al manteniment d'una política adequada de confidencialitat. S'hi preveuen, per exemple, diverses polítiques de control i registre de suports i dispositius que es facin servir per al tractament de dades i una política de pantalla i taula netes.

Per a l'accés físic a les instal·lacions, està previst que només el personal autoritzat pugui accedir als llocs en què es trobin instal·lats els equips físics que donin suport als sistemes d'informació. En general, per a l'accés a determinats espais els membres del personal han de fer servir targetes magnètiques unipersonals, que també els serveixen per fitxar. L'accés a determinades zones restringides també disposa d'un control d'empremta digital.

Els proveïdors externs, per accedir físicament a les instal·lacions, s'han de donar d'alta prèviament en una aplicació de control d'accés, que controla la necessitat de l'accés i emet un passi, que el proveïdor es pot descarregar i que li servirà per poder entrar.

El procediment per donar de baixa un membre del personal també es realitza a través d'una comunicació per correu electrònic que realitzen responsable de recursos humans al responsable informàtic. Aquesta comunicació sempre té lloc de forma immediata a la modificació o cessament en la prestació de serveis per part d'un treballador. Està previst que en determinats casos determinades baixes siguin temporals. Llavors, l'usuari es manté prudencialment, però deshabilitat i, al cap de 3 mesos, el responsable informàtic pregunta si la baixa temporal ha esdevingut definitiva, a fi i efecte de donar de baixa l'usuari. Un cop l'any els responsables informàtics fan un repàs de tots els usuaris i accessos vigents per confirmar que es corresponen amb la realitat. En general, durant aquesta acció, es repassen sobretot els usuaris deshabilitats per veure si són definitius. No es detecta el risc que, degut a una mala comunicació, un usuari no autoritzat que ja no formi part de l'entitat pugui continuar accedint.

Pel que fa a les dades més sensibles que tracta l'entitat, les relatives a salut dels pacients i participants dels projectes de recerca, es preveuen mesures de seguretat addicional, com ara el control, registre i revisió periòdica de tots els accessos i intents d'accessos, de què s'aporta evidència. El DPD repassa els informes d'accessos que se li proporcionen des de l'àrea informàtica.

Pel que fa a la documentació en paper, es troba tota desada en despatxos tancats amb clau, dins armaris, ordenada alfabèticament. Es constata, per tant, que tots els espais, magatzems, despatxos i àrees de l'entitat que contenen o guarden documentació amb dades de caràcter personal disposen de sistemes de tancament, de manera que la informació es troba conservada de forma segura i fora de l'abast d'usuaris no autoritzats. El personal coneix la seva obligació de tancar les sales i despatxos que continguin informació confidencial, quan ja no es fan servir o quan acaba la jornada laboral.

Finalment, la sala de servidors de Badalona disposa d'accés amb clau, si bé es troba habitualment oberta, mentre que la de Barcelona s'hi pot accedir per clau electrònica i/o mecànica.

Àrees de millora

	Com a únic aspecte a millorar, cal destacar la necessitat que la sala de servidors estigui per defecte tancada i no accessible.

5.11. MANTENIMENT DE LES XARXES

Els dispositius i ordinadors utilitzats per a la conservació i el tractament de les dades personals hauran de mantenir-se actualitzats. En aquests dispositius es disposarà d'un sistema d'antivirus instal·lat i degudament actualitzat.

Situació actual

Tots els recursos i sistemes utilitzats a GUTTMANN per al tractament de les dades es troben degudament actualitzats.

El document "*Annex 21 Esquema de la xarxa*" conté un diagrama de xarxa de GUTTMANN a Badalona i una relació dels servidors que es fan servir a l'entitat, juntament amb una descripció de la seva ubicació dins les instal·lacions i de les mesures de seguretat que s'hi apliquen. En general, la xarxa està basada en tecnologia Gigabit Ethernet i disposa de 5 racks, un dels quals és el CPD, mentre que els altres fan funcions de distribució. L'enllaç entre els racks és de fibra òptica i doble (redundant). Segons les informacions proporcionades, la xarxa de Barcelona és pràcticament igual.

Els racks 1, 2, 3 i 4 estan situats en quatre despatxos de la planta -2, distanciats de manera equidistant entre ells. El rack 0 es troba situat a la planta 1 i forma part del CPD.

Al Rack 1, a part de la centraleta telefònica i les entrades de les línies de telèfons, hi ha el commutador central de la xarxa, que és un Cisco 4510R+E, connectat a un router Cisco 2821. A través d'aquest router es manté la connexió a Internet a través de l'Anella Científica i a la Història Clínica Compartida de Catalunya i a la Recepta Electrònica a través del Nus Sanitari, que fa les funcions de tallafocs.

Com a mesures de seguretat, l'entitat disposa de Firewalls perimetrals i utilitza els serveis d'Antivirus McAffee, que escaneja tot el correu electrònic.

No detectada

▲	

5.12. CENTRE DE PROCESSAMENT DE DADES

S'establiran mecanismes de restricció d'accés a la sala on es trobin els servidors (CPD).

Situació actual

D'acord amb el document "*Annex 17 Sistema de seguretat i pla de contingències*" i les informacions proporcionades, la sala de servidors es troba a la primera planta i només és accessible per mitjà de clau mecànica per mitjà dels usuaris autoritzats.

El CPD disposa de tres armaris RACK, sistema de refrigeració redundant (dos aparells d'aire condicionat) i un dispositiu de control de temperatura amb alarma acústica i lògica. També es constata que hi un extintor de pols i una càmera de seguretat.

El CPD disposa d'un SAI, dotat amb un sistema de control de temperatura, que permetria disposar d'un corrent elèctric alternatiu durant vint minuts per al cas improbable d'una interrupció sobtada i imprevista del subministrament ordinari. També hi ha dos grups electrògens, que també podrien proporcionar un subministrament elèctric alternatiu bàsic a l'hospital (només es podria endollar als endolls vermells, que són els considerats bàsics).

No detectada

▲	

5.13. EMMAGATZEMATGE DE FITXERS

Com a norma general, els fitxers que continguin dades personal s'emmagatzemaran en un servidor de fitxers i no en els dispositius dels usuaris de forma local.

Situació actual

Al manual de bones pràctiques o codi ètic que es dona en tots els procediments d'acollida al personal laboral i extern i que és accessible en tot moment a través de la intranet corporativa, ja consten instruccions específiques sobre com emmagatzemar dades de caràcter personal en els equips locals o dispositius i sobre com s'han de fer servir de manera responsable determinats suports i dispositius. El punt número 9, per exemple, permet gravar documents al disc dur del suport i fer-ne còpies de seguretat, només si es comunica al departament d'informàtica. El punt 33 conté la previsió d'esborrar informació que s'hagi pogut gravar localment en un portàtil per a una presentació o qualsevol altra feina.

D'altres previsions del manual de bones pràctiques estableixen l'obligació de registrar les sortides de suports que continguin dades de pacients i la necessitat que les dades de pacients que es trobin en un dispositiu o suport mòbil de qualsevol tipus estiguin xifrades.

No detectada

▲	

5.14. CÒPIES DE SEGURETAT

Periòdicament (mínim setmanal) es duran a terme processos de còpia de seguretat de les dades personals en un suport diferent al que s'utilitza pel treball diari. Es disposarà d'una còpia de seguretat en un lloc diferent d'on s'emmagatzemen les dades.

Situació actual

D'acord amb el document "*Annex 17 Sistema de seguretat i pla de contingències*" i les informacions proporcionades, l'entitat té implementats diversos procediments de realització de còpies de seguretat, que apareixen en el citat document profusament descrites.

D'una banda, com a primer procediment, es fa una còpia en un servidor a part i després a la nit s'envia a un Data Center de Badalona en condicions de seguretat. També es fan còpies de retenció en funció del servei, poden variar en freqüència i durada.

També es realitzen còpies a través d'un sistema de "snapshots", segons el qual es realitzen còpies de la màquina virtual cada 6 mesos.

Finalment, hi ha un tercer procediment de còpia manual dels arxius, segons el qual es realitzen còpies en discs i CDs com a suport. Aquesta còpia es realitza mensualment sobre totes les bases de dades assistencials i no assistencials.

El responsable d'informàtica fa una revisió mensual per comprovar l'aplicació correcta de tots els procediments de còpia i recuperació. Els elements a controlar responen a una selecció aleatòria.

No detectada

▲	Seria recomanable que els informes sobre les revisions, en cas de detectar errors, es fessin arribar al delegat de protecció de dades, el qual podria proposar mesures correctores, en cas necessari.

5.15. PERFILS

S'establiran perfils d'usuaris amb diferents nivells d'accés a dades personals segons les funcions del treballador; Quan un dispositiu s'utilitzi per al tractament de dades personals i fins d'ús personal, es recomana establir perfils diferents. Es recomana disposar de perfils amb drets d'administració per a la instal·lació i configuració del sistema i usuaris sense privilegis.

Situació actual

En funció de les responsabilitats i funcions atribuïdes a cada persona dins l'entitat, ja hi ha diferents perfils d'accés a entorns informatitzats, aplicacions i dades de caràcter personal. Així, per exemple, els perfils assistencials (personal que s'ocupa del tractament dels pacients) tenen un accés als programes assistencials, que, en canvi, no té el personal administratiu.

Segons el document "*Annex 17 Sistema de seguretat i pla de contingències*", s'han definit a la xarxa usuaris i grups d'usuaris i tots ells tenen un nivell de lectura o escriptura sobre les dades que poden visualitzar o manipular. Cada grup d'usuaris només pot accedir a les dades que prèviament s'ha decidit que puguin ser accessibles per ells. La relació d'usuaris amb accés a dades de caràcter personal i la definició dels seus perfils d'accés es troba sota control dels responsables de l'àrea informàtica, que són els que s'encarreguen de mantenir actualitzada aquesta relació.

D'acord amb les informacions proporcionades, des de l'àrea informàtica es fan revisions sobre els accessos de forma proactiva. En general, es fan revisions dels usuaris dels usuaris en situació de baixa temporal, i es fan revisions anuals de tots els accessos, a fi de comprovar que es troben actualitzats, d'acord també amb la informació de recursos humans.

En general, tal com comentàvem al punt anterior, és quan s'incorpora una persona nova a GUTTMANN que s'apliquen uns protocols d'acollida i es defineix el seu perfil d'accés en funció de les dades i recursos a què hagi d'accedir.

No detectada

▲	

5.16. IDENTIFICACIÓ I AUTENTICACIÓ

S'establiran mecanismes d'autenticació personalitzats per accedir als sistemes mitjançant, per exemple, un usuari i contrasenya específic per a cada treballador (identificació inequívoca).

La contrasenya tindrà almenys 8 caràcters (números i lletres) i l'empresa decidirà la complexitat d'aquestes claus. Es canviaran les contrasenyes, com a mínim, un cop l'any.

Situació actual

Segons les informacions i documentació proporcionades, tots els usuaris ja estan identificats i registrats, i ja hi ha un control sobre el nivell d'accés autoritzat que pot tenir cadascú.

En general, el procediment d'alta d'un nou usuari autoritzat de les dades s'acompanya sempre d'un procediment d'acollida en què des de l'àrea de recursos humans es defineixen els accessos i recursos a què ha de tenir accés i n'informa els responsables informàtics perquè ho apliquin. Aquesta informació consta en una relació d'usuaris amb accessos autoritzats. Aleshores, els responsables de sistemes informàtics apliquen el perfil d'accés que correspongui d'acord amb les funcions atribuïdes.

Per a la primera alta al directori actiu, es defineix un nom d'usuari, que consisteix generalment en la inicial del nom + cognom + segon cognom (en alguns casos, quan cal), que es lliure a l'usuari en un sobre tancat juntament amb una contrasenya provisional i les instruccions per canviar-la. Fonamentalment hi ha tres entorns informàtics que estan protegits per nom d'usuari i contrasenya i que permeten establir diferents perfils d'accés, que són el domini, el correu electrònic i les aplicacions assistencials, a banda d'altres aplicacions més específiques.

D'acord amb el document "*Annex 17 Sistema de seguretat i pla de contingències*" les contrasenyes de l'usuari autoritzat han de complir determinats requisits de robustesa i complexitat. Han de tenir un mínim de 8 caràcters i contenir aquests tres tipus de caràcters: lletres (A-Z), números (0-9) i caràcters especials (!, $, #,...). Caduquen al cap de tres mesos, de manera que s'han de renovar per part de l'usuari de forma trimestral. D'altra banda, les contrasenyes es guarden encriptades.

D'altra banda, per a l'accés al domini s'apliquen mesures de limitació per intents d'accés fallit, que restringeix a 3-5 (en funció del tipus d'entorn) els intents d'accés amb contrasenya abans de bloquejar-se. D'altra banda, també s'aplica una mesura de bloqueig per inactivitat, que s'activa al cap de 10 minuts en la majoria dels entorns i de 3 minuts en aplicacions assistencials.

No detectada

▲	

5.17. ACCESSOS REMOTS

Per evitar accessos remots indeguts a les dades personals es prendran les mesures corresponents com l'existència de Firewall.

Situació actual

GUTTMANN permet a determinats usuaris, per raons justificades de les seves responsabilitats laborals, que accedeixin remotament als sistemes.

D'acord amb les informacions proporcionades, a partir de la crisi sanitària provocada per la Covid-19 i la impossibilitat que els treballadors puguin desplaçar-se al seu lloc de treball, sorgeix la necessitat de garantir el teletreball a una part important de la plantilla. D'aquesta manera, en un primer moment, com a solució de xoc, es va permetre a aproximadament 100 treballadors accedir remotament als seus ordinadors físics a través d'una solució BW System. Aquesta solució es va preveure com a provisional, tot i que està dotada d'un control d'accés amb una contrasenya específica. De mica en mica, però, s'ha avançat cap a una solució VPN, que implica més control, seguretat i rendiment.

L'accés a través de VPN suposa accedir a un escriptori remot. En aquest cas, com a mesura de seguretat, l'ordinador físic resta bloquejat, tan bon punt s'activa l'accés remot a través de VPN. La VPN està configurada amb l'usuari i la contrasenya d'accés a la xarxa.

El responsable informàtic manté una relació actualitzada dels usuaris autoritzats a accedir remotament. El document "*Annex 38 Relació d'Accessos Remots*" conté les mesures de seguretat que s'apliquen en aquests accessos.

A través d'un acord de teletreball, que s'ha proporcionat a tot el personal i que s'ha revisat en aquesta auditoria, es regulen les condicions de teletreball de manera segura, amb un compromís específic de seguretat per part del treballador.

Com a mesura de seguretat rellevant, recordem que hi ha implementada una mesura de bloqueig per inactivitat tant al domini com en les aplicacions assistencials. D'aquesta manera, es minimitza notablement la possibilitat d'accessos indeguts des de fora de les instal·lacions i mitjançant dispositius o equips que escapin al control de l'entitat.

També és important assenyalar que el sistema està protegit per dos Firewalls transversals de Cisco-FTP, en un sistema redundant. Aquest model també s'aplica exactament respecte a la xarxa de Barcelona de l'entitat (amb dos Firewalls més).

No detectada

▲	

5.18. REGISTRE D'ACCESSOS INFORMÀTICS

Categories especials de dades: es durà a terme un registre d'accessos d'aquest tipus de dades.

Situació actual

D'acord amb les evidències i mostres aportades i les explicacions facilitades, s'aplica una mesura de seguretat de registre d'accessos sobre els programes que es fan servir per al tractament de dades de salut. D'acord amb aquesta mesura, el responsable informàtic genera un informe mensual dels accessos als programes assistencials i a la plataforma GNPT. Aquest informe es trasllada al DPD, que el revisa, hi fa propostes de correcció, en cas necessari, i després ho remet a direcció.

S'aporten diferents evidències en arxius Excel i pdf de com són aquests registres d'accessos, tant en relació al programa de gestió assistencial com pel que fa la plataforma GNPT. En aquests registres hi consten el PC, el login, el codi d'usuari, la data i l'hora i la història accedida. També és possible visualitzar en aquests registres els accessos que s'han realitzat per perfils.

El procediment previst per GUTTMANN és correcte i garanteix en bona mesura que no es realitzin accessos indeguts.

No detectada

▲	

5.19. INVENTARI

Es disposarà d'un inventari actualitzat dels diferents suports/dispositius que continguin dades personals.

Situació actual

Tots els suports i dispositius que es fan servir a GUTTMANN per tractar i conservar dades de caràcter personal ja estan degudament identificats, etiquetats i inventariats.

Totes les màquines, dispositius i suports que es fan servir estan inventariats i duen una etiqueta física, que els identifica. El document de bones pràctiques que es proporciona al personal, al seu punt 30, estableix l'obligació del personal d'aplicar etiquetes en els termes següents: "*Els suports informàtics que tinguin dades personals, (per exemple: dades de nòmines per les entitats financeres, dades de declaracions tributàries per Hisenda, imatges radiogràfiques, etc.) hauran d'estar clarament identificats amb una etiqueta externa que informi de les da-des contingudes i la data en que es van guardar en el suport informàtic*".

D'acord amb les informacions proporcionades, la mateixa aplicació que es fa servir per gestionar i registrar les incidències ja inclou l'inventari de suports i dispositius, cosa que permet relacionar-hi les incidències. En tot cas, es porta un control i registre de les persones a qui s'han assignat els equips, suports i dispositius. També es registra quan l'usuari recull o ha de traslladar un dispositiu o suport que conté dades de caràcter sensible.

En general, segons informacions proporcionades, ja es preveu l'actualització i control dels inventaris de suports i dispositius informàtics.

No detectada

▲	

5.20. DESTRUCCIÓ DE SUPORTS

No es llençaran documents o suports electrònics amb dades personals sense garantir-ne la seva destrucció.

Situació actual

D'acord amb el punt 29 del manual de bones pràctiques que s'aplica a tot el personal, "*en cas de voler destruir qualsevol document que contingui informació o dades confidencials s'ha de fer necessàriament mitjançant el circuit descrit en el document "Annex 17: Sistema de seguretat informàtic i pla de contingències. Apartat 'Destrucció de discs i papers i protecció de dades*"."En efecte El document a què remet aquest punt ja conté les mesures previstes per l'entitat per a la destrucció segura de suports. Segons aquest document, ja hi ha un seguit de previsions de destrucció, que comentem a continuació.

Els procediments establerts a l'Annex 17 preveuen que els discs durs siguin formatats quan hagin de ser destruïts o canviats d'ordinador i, que per a la seva destrucció física, es desmuntin i es trenquin fins a esdevenir inservibles. Pel que fa a la documentació confidencial, s'ha de dipositar en una caixa especial destinada específicament a documentació confidencial, que posteriorment acaba destruïda a la trituradora de paper. També s'hi preveu que els suports que s'han d'eliminar es sotmetin a processos previs d'esborrat o destrucció, per tal d'impedir-ne una possible recuperació posterior de les dades que s'hi emmagatzemen. El mètode de destrucció consisteix en esborrar i formatar els discos i, en cas necessari, realitzar una nova instal·lació del programari; les cintes es tallen; els Cdroms i DVDs es ratllen i trenquen. Si s'han de llençar discs o be llapis òptics, es trenquen i ratllen abans de llençar-los. Els suports eliminats es dipositen o traslladen a llocs de reaprofitament informàtic o, si això no és possible, es llencen a les escombraries. Totes les sortides de suports per a eliminació es fan constar al registre d'entrades i sortides, i la baixa del dispositiu es gestiona com a una incidència.

En general, als departaments que generen i fan servir documentació en paper, com ara el de recursos humans, disposen d'una màquina trituradora, on poden destruir la documentació que contingui dades de caràcter personal.

No detectada

▲	

5.21. SORTIDA DE DADES

Categories especials de dades: quan calgui realitzar l'extracció de dades personals fora del recinte on es realitza el seu tractament, ja sigui per mitjans físics o electrònics, s'haurà de valorar la possibilitat d'utilitzar un mètode d'encriptació.

Situació actual

D'acord amb les instruccions que es proporcionen al personal a través del manual de bones pràctiques, ja hi ha un seguit de mesures que s'han d'aplicar necessàriament en la comunicació i sortida de dades. El punt 26 estableix la prohibició d'enviar dades de pacients per correu electrònic, a menys que s'hi apliqui algun sistema de xifrat. Un altre punt rellevant és el 32, que determina que totes les sortides de suports que continguin dades de caràcter personal hauran de registrar-se en un registre d'entrades i sortides, de conformitat també amb allò establert als documents de seguretat. Finalment, el punt 34 estableix la necessitat d'encriptar les dades de pacients, sempre que es facin servir dins un dispositiu mòbil, i el punt 45 prohibeix treure històries clíniques fora del centre sense el coneixement i permís del responsable del tractament.

Els documents de seguretat relatius als tractaments de dades sensibles (dades de salut o de recerca) també preveuen mesures d'encriptació per a suports, documents i dispositius que s'hagin de traslladar fora del centre, de manera molt semblant a com ho fa el manual de bones pràctiques. Segons aquests documents, Les dades de pacients que s'envien telemàticament, s'han d'enviar encriptades o dissociades. El departament d'Admissions i Atenció a l'Usuari i l'àrea Mèdica, que son les que tenen més necessitat d'enviar dades de pacients, ho fan amb PDFs xifrats amb AES 128 o AES 256 per substituir els fax. També fan servir el programa Winzip amb xifrat AES 256.

No detectada

▲	

5.22. EMMAGATZEMATGE EN SUPORT PAPER

Els documents en paper i suports electrònics s'emmagatzemaran en lloc segur (armaris, calaixos o estances d'accés restringit).

Situació actual

En general, a l'entitat es tracta cada cop menys documentació en paper, però s'apliquen mesures de seguretat en relació a la documentació que encara es fa servir i es conserva.

En general, tota la documentació es troba desada en armaris que sempre estan tancats amb clau i amb accés restringit als responsables del seu tractament autoritzat.

Els espais i despatxos en què es guarda la documentació en paper i els suports informàtics disposen sempre d'un control d'accés físic, com és el cas dels accessos a les instal·lacions i a les oficines. Per a l'accés a aquests espais només es poden fer servir les targetes magnètiques dels treballadors, l'empremta digital per a determinades zones o les claus físiques, en determinats casos. En qualsevol cas, tots aquests espais romanen tancats i restringits, quan no se'n fa ús.

No es constata durant els treballs de camp l'existència de documentació que no es trobi degudament desada o custodiada.

No detectada

▲	

5.23 REGISTRE D'ACCESSOS DOCUMENTAL

Categories especials de dades: es restringirà l'accés a aquest tipus de documentació, s'habilitaran mètodes per a la seva destrucció i es durà a terme un registre d'accés a aquests documents.

Situació actual

D'acord amb les informacions proporcionades, la documentació en suport paper que es fa servir a l'entitat es troba generalment desada als seus corresponents armaris, situats en despatxos, que es troben sempre tancats, quan no es fan servir. També hi ha un arxiu històric al soterrani. En qualsevol cas, cada cop es conserva menys documentació en paper.

Pel que fa a dades de categoria especial (dades de salut corresponent als projectes de recerca, per exemple), la documentació que es pot arribar a conservar en paper és generalment accessòria o circumstancial, ja que gairebé tota la informació necessària es recull, es tracta i es conserva de forma informatitzada a través de les aplicacions corresponents. Segons les informacions proporcionades, no entra ni surt documentació de l'arxiu de forma habitual.

Els documents de seguretat de pacients i investigació estableixen que l'accés a la documentació en paper es limita al personal autoritzat, i es refereixen als documents "*Annex 30 Funcionament de l'arxiu en suport paper*" i "*Annex 27 arxiu històries clíniques*", que s'aplicarien en aquest cas per a la regulació del registre d'accessos. El manual de bones pràctiques que es proporciona al personal estableix al punt 42 que "*tots els membres de l'organització, professionals i col·laboradors, que necessitin consultar les Històries Clíniques en suport paper, hauran d'indicar el seu accés al registre d'entrades i sortides de les Històries Clíniques de l'arxiu corresponent i amb els mecanismes que l'entitat indica en el document de seguretat*".

L'entitat ja té mitjans per a la destrucció de documentació confidencial, sobretot màquines trituradores en les àrees que es fa servir documentació en paper. D'acord amb la documentació aportada a aquesta auditoria, hi ha una previsió clara de destruir tota la documentació que tingui dades de caràcter personal a través d'aquest mitjà, la qual cosa ja ha estat també instruïda al personal a través del manual de bones pràctiques.

No detectada

▲	

5.24. CRITERIS D'ARXIU

S'establiran criteris d'arxiu per a la documentació que contingui dades de caràcter personal, i es custodiarà de forma adequada quan no s'utilitzi aquesta documentació.

Situació actual

En general, els arxius en suport paper han de garantir la correcta conservació de la documentació, la localització i consulta de la informació, i fer possible l'exercici dels drets dels interessats respecte a l'accés, oposició, supressió, rectificació, limitació i portabilitat sobre les seves dades personals.

Tal com hem comentat als punts anteriors d'aquest informe, la documentació en paper que es pot guardar a l'entitat i que conté dades de categoria especial és residual. En general es guarda documentació del personal, d'administració i de pacients, però la major part de la gestió es du a terme de manera informatitzada.

Pacients: Pel que fa a la documentació mèdica, s'informa que l'única documentació que es guarda en paper és el full d'informació del pacient sobre protecció de dades, el consentiment informat i les proves que només puguin conservar-se en aquest suport documental. Tanmateix, també es guarden escanejats. La documentació mèdica en paper es troba a la sala d'arxiu de la planta -2, guardada segons un criteri ordenació per número d'història clínica, sense diferenciar l'actiu del passiu. El criteri per considerar la documentació com a passiva és que el pacient sigui èxitus. Aquesta documentació es conservaria de manera indefinida. La responsable d'aquest l'arxiu és la cap d'atenció a l'usuari i admissions.

Recerca: La documentació que encara es conserva dels participants als projectes de recerca, generalment consentiments informats, es troba emmagatzemada a la sala d'arxiu de la planta -2, ordenada segons la numeració de les històries clíniques. La documentació que encara es pugui fer servir relativa a projectes actuals, es trobaria als despatxos dels investigadors principals.

Personal: Es guarden expedients de tots els treballadors dins armaris tancats amb clau, ordenats alfabèticament, dins els espais de l'àrea de recursos humans. Els contractes es guarden indefinidament, però els justificants es destrueixen al cap de 2 anys. La cap de recursos humans seria la responsable d'aquest arxiu.

Administració: Llevat alguna documentació de facturació residual, que es tractaria a les oficines, la majoria de documentació en paper es troba a l'arxiu del soterrani, on es conserva per períodes de 7 anys i després és destruïda.

Externs: La documentació i expedients dels estudiants es troba desada i ordenada a l'àrea de docència segons cursos acadèmics i número de matrícula. Així mateix, s'organitzen en diferents carpetes segons sigui MIR, pràctiques, postgrau o Màster. El passiu es guarda al mateix departament, amb documentació que es remunta a 20 anys enrere. La responsable de l'arxiu és la coordinadora de docència.

Treball Social: La documentació que es fa signar als voluntaris i la que es genera dels treballs en benefici de la comunitat es troba emmagatzemada als despatxos de l'àrea de treball social, ordenada per departaments, serveis i dates, sense diferenciar distingir l'actiu del passiu. La

documentació es guarda de manera indefinida. La persona responsable d'aquest arxiu seria la mateixa cap de treball social.

Reclamacions: La documentació relativa als procediments de reclamació i suggeriment de pacients està desada a l'àrea d'Admissions. El criteri d'arxiu és per anys. La responsable de l'arxiu és la cap de Departament d'Admissions.

Àrees de millora

●	D'acord amb els principis de conservació de les dades i davant la possibilitat que es guardin dades més enllà del que seria necessari i justificat, amb els riscos que això implica per a la confidencialitat, caldria revisar l'oportunitat i la conveniència de dur a terme accions de destrucció segura de la documentació més antiga, sempre que es pugui acreditar que ja no és necessària la seva conservació. Molt lligat a això, caldria revisar també la necessitat d'establir criteris i terminis de conservació dels diferents projectes, sobretot d'aquells en què encara es conservin dades personals que permetin la identificació dels participants. Com sempre que sigui possible, tal com preveu el RGPD, seria convenient tenir en compte la necessitat d'aplicar mesures de seudonimització també en la conservació de la documentació en suport paper.

6. CONCLUSIONS

Després de realitzar totes les actuacions necessàries a les dependències de l'entitat, completar les entrevistes amb els corresponents responsables d'àrea, valorar la documentació aportada i avaluar els sistemes de tractament de la informació, l'equip auditor detecta que les àrees de millora i de no conformitat, d'acord amb la normativa vigent, són:

ÀREES DE MILLORA
I – BLOC GENERAL
5.1. Auditoria. 5.3. Definició de les mesures de seguretat per part del responsable del tractament. 5.5. Encarregats del tractament i proveïdors sense accés a dades. 5.9. Difusió de funcions i obligacions del personal.
II – BLOC DE MESURES DE SEGURETAT
5.10. Diligències dels accessos. 5.24. Criteris d'arxiu.
NO CONFORMITAT
I – BLOC GENERAL
5.6. Licitud del tractament, base jurídica, informació i consentiment. 5.8. Notificacions de violacions de seguretat.

Barcelona, 23 de juny de 2020

Pere Ruiz Espinós

- Soci -

Caterina Bartrons Pou

- Gerent -