# Manual de Bones Pràctiques respecte a la protecció de dades de caràcter personal

| | | | |
|---|---|---|---|
| **Data aprovació (entrada en vigor)** | 29 gener 2020 | **Data revisió** | 25 maig 2022 |
| **Data propera edició:** | 25 maig 2025 | **Persona responsable** | Dra. Assumpció Boniquet |
| **Estàndards relacionats:** | 5d-19<br>**RGPD** (Reglament (EU) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016 relatiu a la protecció de les persones físiques en allò que respecta al tractament de dades personals i la lliure circulació d'aquestes dades) | | |
| **Elaborat per** | **Comissió documentació clínica i confidencialitat** | | |
| **Revisat per:** | **Sra. Lali Garcia**<br>**Dra. Assumpció Boniquet** | | |
| **Aprovat per:** | **Sr. Francesc Guerra** | | |

# Manual de Bones Pràctiques respecte a la protecció de dades de caràcter personal

Amb l'objectiu de garantir la confidencialitat i la seguretat de les dades personals de l'entitat, i donar compliment als preceptes del Reglament (UE) 679/2016, de Protecció de dades (en endavant, el "Reglament" o "RGPD" indistintament) i a la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (en endavant, "LOPDiGDD"), l'entitat Fundació Sant Hospital ha establert les mesures preventives que recull el Manual de Bones Pràctiques, que haurà de complir tot el personal contractat, així com el personal col·laborador.

El Reglament defineix com a **dada personal** tota informació sobre una persona física identificada o identificable. Es considera persona física identificable tota persona que la seva identitat pugui determinar-se, directa o indirectament, en particular mitjançant un identificador, com per exemple un nom, un número d'identificació, dades de localització, un identificador en línia o un o varis elements propis de la identitat física, fisiològica, genètica, psíquica, econòmica, cultural o social d'aquesta persona.

## MESURES INFORMÀTIQUES:

1. Les dades de caràcter personal a les quals hi té accés el personal i col·laboradors només seran utilitzades amb la finalitat de la prestació dels serveis del centre, garantint el compromís de confidencialitat i ètica professional.

2. Pel que fa als mecanismes de transmissió de la informació únicament s'utilitzaren els que estan descrits al *Document de seguretat* i, per tant, autoritzats per l'Entitat.

   Està totalment prohibit fer tramesa d'informes/documents per FAX amb dades de caràcter personal, sobre tot informació relativa a diagnòstics, de sospita o de certesa, del titular de les dades.

   Donat que el correu electrònic ens permet encriptar les dades, es podrà fer ús d'aquest mitjà quan la urgència mèdica així ho requereixi i sempre que el metge responsable del pacient ho sol·liciti, utilitzant el programari específic per aquesta tasca, de manera que el document que s'enviï per correu electrònic sempre haurà d'estar encriptat. Per aquells usuaris que ho necessitin, l'Entitat disposa d'un protocol d'actuació.

3. Cada usuari amb accés informàtic a les dades dels fitxers, tindrà cura de que les dades que es visualitzin per pantalla o que s'imprimeixin, no puguin ser visualitzades per persones no autoritzades al seu accés.

4. Cada usuari que té accés a dades de caràcter personal, quan accedeixi a aquestes dades mitjançant la seva clau d'usuari informàtic, haurà de procurar que aquesta clau no sigui visualitzada per ningú que la pugui utilitzar sense autorització.

5. Cada usuari és responsable de la confidencialitat de la seva clau d'accés. En el cas que aquesta sigui coneguda per persones no autoritzades, haurà de notificar-ho i registrar-ho com a incidència i procedir al seu canvi.

6. Cada treballador/col·laborador haurà de procedir al canvi de la seva paraula de pas quan el sistema així ho requereixi.

7. El bloqueig de pantalla s'activa automàticament, com a norma general, i sol·licitarà introduir la contrasenya per poder desactivar el bloqueig.

8. Quan l'usuari d'un lloc de treball l'abandoni temporalment, caldrà que activi manualment el protector de pantalla (amb la tecla Windows apretada, prémer la tecla L). La tornada al seu lloc de treball implicarà la desactivació de la pantalla protectora, que presenta el missatge de Ctrl+Alt+Supr i demana la introducció de la corresponent contrasenya

9. Quan un empleat o col·laborador finalitzi la seva jornada laboral o deixi el seu lloc de treball durant un període de temps que preveu llarg, tancarà les aplicacions amb les que ha estat treballant, finalitzarà la seva sessió com a usuari i apagarà l'ordinador.

10. Qualsevol modificació en els sistemes d'informació (SI), i en concret a la informació inventariada als documents de seguretat, s'haurà de comunicar a l'Entitat, concretament al Responsable de Sistemes d'Informació mitjançant un correu electrònic a informatica@fsh.cat amb còpia a la Delegada de Protecció de Dades (dpd@fsh.cat).

**ACCÉS A INTERNET:**

11. L'accés a Internet es limitarà als temes directament relacionats amb l'activitat sanitària, sociosanitària i de serveis socials que presta l'Entitat i amb el lloc de treball de l'usuari.

12. Queda prohibit realitzar debats en temps real (tipus: Chat/IRC), donada l'alta perillositat que suposa pel sistema la instal·lació del programari que permet els accessos no autoritzats al sistema informàtic.

13. L'accés a pàgines web (www), grups de notícies (Newsgroups) i altres fonts d'informació com FTP, etc., es limita a aquells que tinguin informació relacionada amb l'activitat de l'entitat o amb el lloc de treball de l'usuari.

14. Queda prohibit introduir, descarregar d'Internet, reproduir, utilitzar o distribuir programes informàtics no autoritzats per part de l'Entitat o qualsevol tipus d'obra o material on els drets de la propietat intel·lectual o industrial pertanyin a tercers, quan no es disposi de l'autorització pertinent.

15. En tot cas, per a qualsevol actuació respecte als anteriors supòsits serà requisit indispensable l'autorització expressa de l'Entitat, concretament al Responsable de Sistemes d'Informació mitjançant un correu electrònic a informatica@fsh.cat amb còpia a la Delegada de Protecció de Dades (dpd@fsh.cat).

**MESURES RESPECTE DADES EN SUPORT FÍSIC:**

16. Quan s'enviï documentació en suport físic a institucions o a particulars que hi tenen dret d'accés, s'ha de gestionar la tramesa amb el Registre de documentació de secretaria de direcció.

17. S'haurà de garantir el destí últim del paper, inservible o duplicat o fruit de l'expurgo segons la legislació vigent en matèria de conservació de la documentació clínica mitjançant la seva destrucció a través d'una empresa externa especialitzat i acreditat per aquest servei. Aquesta mesura és necessària per garantir la confidencialitat i per evitar que existeixi el risc d'accés per part de personal no autoritzat.

    - ✓ Circuit de destrucció de documentació en suport paper
        - ✓ Documentació amb dades bàsiques de filiació i dades administratives (nivell bàsic de seguretat) i/o amb dades clíniques (nivell alt de seguretat) com ara diagnòstics, resultats de proves, analítiques, informes mèdics, notes d'evolució, etc., es dipositen als *contenidors de documentació confidencial* que s'han distribuït a les diferents unitats de la FSH i que, un cop plens es custodien en un magatzem tancat fins que l'empresa externa contractada els destrueixi en condicions de seguretat i, posteriorment, emeti el corresponent certificat de destrucció. En cap cas s'han de llençar a les papereres de dipòsit de deixalles.

    - ✓ Circuit de destrucció de documentació en suport informàtic (CDs, disquets)
        - ✓ Si en tenim un nombre elevat per destruir, s'han de lliurar al departament d'Informàtica.
        - ✓ Si en tenim pocs per destruir, es poden dipositar als contenidors de documentació confidencial i es destruiran igual que el paper que els envolti.

18. Els suports informàtics que tinguin dades personals (per exemple: dades de nòmines per les entitats financeres, dades de declaracions tributàries per Hisenda en disquets o CD), hauran d'estar clarament identificats amb una etiqueta externa que informi de les dades contingudes i la data que es van guardar en el suport informàtic.

19. Tots els suports amb categories especials de dades que surtin del centre s'hauran d'anotar al *Registre d'entrades i sortides de suports,* tal com s'indica al *Document de seguretat*.

**MESURES RESPECTE LES HISTÒRIES CLÍNIQUES:**

20. Els arxius on estiguin ubicades les Històries Clíniques han d'estar tancats sota clau. Caldrà tenir cura de la clau, no fer-ne còpia sense autorització expressa ni deixar-la en cap lloc accessible per persones no autoritzades.

21. Cada empleat/col·laborador amb accés a les Històries Clíniques en suport paper (HCP) haurà d'indicar al registre d'entrades i sortides (informàtic o paper) de les Històries Clíniques de l'arxiu amb els mecanismes que l'Entitat li ha indicat en el *Document de Seguretat*.

22. Durant el període en que la HCP es troba fora de l'arxiu central, tot el personal ha de vetllar per evitar qualsevol accés per part de persones no autoritzades.

23. La devolució de les HCP a l'arxiu ha de realitzar-se immediatament després de la circumstància que va motivar la seva petició. Si escau retenir la HCP més temps del previst o si canvia d'ubicació, cal informar-ne a l'Arxiu.

24. Està absolutament prohibit treure la HCP fora del centre sense autorització expressa de l'Entitat.

**RESPECTE L'ÚS DE L'USB:**

25. L'ús de dispositius USB per a dades personals està absolutament prohibit. En cas que un departament ho necessiti ha de sol·licitar autorització al responsable del departament d'informàtica justificant el motiu.

**RESPECTE L'ÚS DE TABLETS I DE TELÈFONS MÒBILS AMB ACCÉS A INTERNET**

26. Únicament el personal autoritzat al *Document de Seguretat* podrà tenir aquests dispositius.

27. Aquests tipus de dispositius seran utilitzats única i exclusivament amb la finalitat de la prestació dels serveis i tasques del centre, garantint el compromís de confidencialitat i l'ètica professional.

28. L'ús de missatgeria instantània, com ara WhatsApp o Telegram, com a eina de comunicació de dades personals està absolutament prohibit, tret que hi hagi una autorització concreta.

29. En el cas que resulti necessari emprar aquest tipus de suports, el Responsable del Tractament donarà instruccions al Responsable de l'Àrea corresponent de l'Entitat per a què sigui l'encarregat d'autoritzar la idoneïtat del seu ús.

30. El *Document de Seguretat* ha de preveure el personal autoritzat a accedir a aquests tipus de suports i ha d'estar registrat en un inventari.

31. Aquests suports hauran de disposar de contrasenya o de codi d'accés.

32. Cal evitar la descàrrega de documents que continguin dades de caràcter personal en aquests suports. Pel cas que resultés necessari fer la descàrrega, un cop realitzada i finalitzada la necessitat que la va motivar caldrà procedir a eliminar les dades de caràcter personal del dispositiu.

33. Quan es deixin d'utilitzar aquests suports o s'esborri la informació que contenen, s'hauran d'adoptar les mesures que evitin l'accés a la informació continguda o la seva recuperació posterior.

## CONSEQÜÈNCIES DE L'INCOMPLIMENT DE LES FUNCIONS I OBLIGACIONS

El personal de l'Entitat Fundació Sant Hospital amb accés a dades de caràcter personal ha de conèixer les conseqüències que es poguessin derivar i les responsabilitats en què puguin incórrer en cas d'incompliment de la normativa de seguretat, que podria derivar en sancions.

L'empresa pot realitzar una auditoria interna del bon ús dels recursos digitals (correu electrònic, unitats d'emmagatzematge digital, etc.) sempre respectant, la proporcionalitat i justificant la necessitat.

L'incompliment de les obligacions establertes en el manual de normes de seguretat i en la normativa interna relacionada amb la protecció de dades personals, així com la comissió de les infraccions tipificades en la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades i garantia dels drets digitals (LOPDiGDD), podrà ser sancionat d'acord amb la legislació laboral, en concret, l'Estatut dels Treballadors, així com el Conveni Laboral d'Aplicació.

**Infraccions tipificades:**

Infraccions lleus (art. 74 LOPDIGDD)

- Incomplir el principi de transparència de la informació al no proporcionar la informació del article 13 i 14 RGPD, en el moment de recollida de les dades personals.
- Exigir el pagament d'un cànon excessiu per donar resposta a les sol·licituds d'exercici de drets.
- No atendre a la sol·licitud de l'interessat d'accés, rectificació, supressió, limitació, oposició o portabilitat de les seves dades, o no donar compliment a l'exercici.
- La manca de formalització per els corresponsables del tractament del acord que determini les obligacions, funcions i responsabilitats de les parts i no posar-lo a disposició dels afectats.
- Incompliment per part del Encarregat del tractament del contracte o acte jurídic que regula les instruccions.
- No disposar d'un Registre d'Activitats del Tractament, d'acord a l'article 30 RGPD.
- La notificació incompleta, amb retard o defectuosa a l'Autoritat de Control d'una violació de seguretat, així com l'incompliment del deure de documentar la violació de seguretat i l'incompliment del deure de comunicació al afectat de les dades d'alt risc per els drets i llibertats dels afectats.
- Facilitar informació inexacta a la Autoritat de Control en els supòsits en que el responsable del tractament hagi d'elevar a una consulta prèvia, conforme a l'article 36 RGPD.
- Quan el nomenament sigui exigible d'acord al article 37 RGPD, no publicar ni comunicar les dades de contacte del delegat de protecció de dades a l'autoritat de control.

Infraccions greus (art. 73 LOPDIGDD)

- El tractament de dades personals d'un menor sense recollir el seu consentiment o el del titular de la seva pàtria potestat o tutela, de conformitat amb l'article 8 RGPD.
- El impediment o obstaculització de manera reiterada d'atendre a les sol·licituds de drets dels interessats.
- La manca d'adoptar les mesures tècniques i organitzatives que resultin apropiades per aplicar de forma efectiva els principis de protecció de dades i adequades al risc del tractament.
- Contractar a un encarregat del tractament que no ofereixi les garanties suficients per aplicar les mesures tècniques i organitzatives apropiades, així com no tenir un contracte o acte jurídic escrit.
- La contractació per un encarregat del tractament d'altres encarregats sense comptar amb la autorització prèvia del responsable o incomplir amb el deure de notificar al responsable les violacions de seguretat.
- No disposar de Registre d'Activitats del tractament (RAT).
- No cooperar amb les Autoritat de Control, o no posar a la disposició de l'Autoritat quan ho sol·liciti el RAT.
- Incompliment del deure de notificació a l'Autoritat de Control i als afectats en els casos del article 33 i 34 RGPD.
- No realitzar una avaluació d'impacte quan sigui exigible.
- No designar a un DPD, quan sigui exigible d'acord al article 37 RGPD, o quan no es possibiliti al DPD realitzar les seves funcions.

Infraccions molt greus (art. 72 LOPDIGDD)

- Recollida de dades en forma enganyosa, fraudulenta, il·lícita, dades inadequades o impertinents.
- No disposar de licitud del tractament. Així com, no complir amb les condicions del article 7 que regula la base jurídica del consentiment.
- Ometre el deure d'informació al afectat sobre el tractament de les seves dades, d'acord als articles 13 i 14 RGPD.
- Vulnerar el deure de confidencialitat.
- Exigir el pagament d'un cànon per fer efectius els drets dels interessats, llevat lo establert en el article 12.5 RGPD o no atendre o obstaculitzar de manera reiterada de l'exercici de drets dels interessats.
- Transferir dades personals a tercers països, quan no es produeixin les garanties, requisits o excepcions dels articles 44 a 49 RGPD.
- Incompliment de resolucions de l'Autoritat de Control o de la funció inspectora de l'Autoritat de Control.
- Revertir de manera deliberada el procediment d'anonimització, amb la finalitat de permetre la re identificació dels afectats.

La incorporació a la dinàmica de l'empresa dels principis rectors de la Protecció de Dades de Caràcter Personal, adquireix una gran importància des del moment en què les conseqüències del seu incompliment comporten grans responsabilitats tant per l'entitat com per al personal que tracta o accedeix a les dades de caràcter personal, és a dir, les sancions ja no només són administratives i dirigides a l'entitat en si, sinó que a més d'elles es poden derivar responsabilitats civils, penals i laborals.

a) **Administratives**: Sancions contemplades en la LOPDIGDD i que són imposades per l'Autoritat de Control en l'exercici de les seves funcions, ja sigui per inspecció d'ofici o oberta a instància de part. Aquestes sancions són de caràcter econòmic i la seva quantia està entre 40.000 a 20.000.000 Euros o 4% volum de negoci total anual.

b) **Civils**: Articles del Codi Civil relatius a la Responsabilitat Contractual i Extracontractual (arts. 1902 i 1903 CC). Així quan determinat servei és contractat a un tercer aliè a la pròpia organització i impliqui un accés a dades de caràcter personal, haurà d'estar precedit del corresponent contracte d'encàrrec de tractament en el qual es limitin les facultats del tercer quant al tractament de les dades de caràcter personal, les dades personals que accediran, s'especifiquin les obligacions de les parts.

c) **Penals**: El Codi Penal tipifica els delictes contra la intimitat i concretament el descobriment i revelació de secrets en els articles 197 i següents.

d) **Laborals**: La fugida de dades, un tractament inadequat de les dades de caràcter personal, un accés no autoritzat a les dades, una protecció inadequada de les dades personals, poden venir derivades de qualsevol lloc laboral dins del si de l'entitat. Quan una cadena d'errors deriva en la imposició d'una sanció a l'entitat, és freqüent que a més es derivin responsabilitats laborals.

   El conveni laboral recull el règim disciplinari que aplica segons el tipus de falta comesa i les sancions que van associades al tipus de falta.

## Decàleg de protecció de dades per al professional sanitari i administratiu

1. Tracta les dades dels pacients com voldries que tractessin les teves.
2. Estàs segur que tens que accedir a aquesta història clínica? Pensa-ho. Només hi has d'accedir si és necessari per a la teva feina.
3. Recorda: els teus accessos a la documentació clínica queden enregistrats en el sistema. Se sap en quin moment i a quina informació has accedit. Els accessos són auditats posteriorment.
4. Evita informar a tercers sobre la salut dels teus pacients, fes-ho només si els pacients ho han consentit o si tens una justificació lícita.
5. Quan surtis del teu lloc de treball, assegura't de tancar la sessió oberta en el teu ordinador. No facilitis a ningú la teva clau d'accés i/o contrasenya; si necessites un accés urgent, contacta amb el departament d'informàtica.
6. No enviïs informació amb dades de salut per correu electrònic o per qualsevol xarxa pública o inhalàmbrica de comunicació electrònica; si és imprescindible, no oblidis encriptar les dades.
7. No llencis documents amb dades personals a la paperera; diposita'ls als contenidors específics de documentació confidencial per a la seva destrucció.
8. Quan acabis de passar consulta, tanca amb clau els armaris o arxivadors que continguin documentació clínica.
9. No deixis les històries clíniques a la vista sense supervisió
10. No creïs pel teu compte fitxers amb dades personals de pacients; consulta sempre amb el departament d'informàtica.

Treballador/Col·laborador:
(signatura)

La Seu d'Urgell a .....de ..... de 20...