**ANNEX 3**

**MODEL DE CONTRACTE D’ENCARREGAT DEL TRACTAMENT**

**REUNITS**

El Sr. **........**, major d’edat, en nom i representació del **Consorci Sanitari del Maresme**, en endavant **CSdM**, en qualitat de **gerent** de l’entitat, amb domicili a carretera de Cirera 230, 08304, Mataró proveït de NIF **Q5856428G** i com a Responsable del Tractament.

El Sr. **.........,** major d’edat, en nom i representació de ............, en endavant **Entitat\_ET** en qualitat de . ........., amb domicili a ......., ....... amb NIF/CIF .......... i com a Encarregat de Tractament.

i

**ACORDEN**

**1. Objecte de l’encàrrec del tractament**

Mitjançant aquestes clàusules s’habilita l’entitat **Entitat\_ET**, encarregada del tractament, per tractar per compte del CSdM, responsable del tractament, les dades de caràcter personal necessàries per prestar el servei de dosimetria personal pels professionals sanitaris del Consorci Sanitari del Maresme.

**El tractament consistirà en:**

Concreció dels tractaments a realitzar:

No Recollida No Registre

No Estructuració No Modificació

No Conservació No Extracció

SI Consulta No Comunicació per transmissió

No Difusió No Interconnexió

No Acarament No Limitació

No Supressió No Destrucció

No Comunicació No Altres .........

**2. Identificació de la informació afectada**

Per executar les prestacions derivades del compliment de l’objecte d’aquest encàrrec, l’entitat **CSdM**, responsable del tractament, posa a disposició de l’entitat **Entitat\_ET,**  encarregada del tractament, la informació que es descriu a continuació:

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **Finalitat del tractament** | | | |
|  | Gestió de nòmines |  | Enviament de comunicacions electròniques |
|  | Selecció de personal |  | Destrucció informació i/o documentació |
|  | Formació |  | Transport i emmagatzematge d’informació i/o documentació |
|  | Gestió administrativa de pacients i dades de contacte dels familiars |  | Enquestes de satisfacció i/o qualitat del servei |
|  | Gestió clínica dels pacients |  | Gestió fiscal i/o administrativa de les donacions |
|  | Prevenció riscos laborals | X | Altres (especificar): dades identificatives dels pacients a efectes de comptabilitat i facturació. |
|  | Atenció religiosa |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **Tipologia de dades** | | | |
| X | Dades identificatives |  | Dades d’ocupació laboral |
|  | Dades de salut |  | Dades econòmic-financeres i d’assegurances |
|  | Dades relatives a infraccions o sancions penals |  | Dades relatives a transaccions de béns i serveis |
|  | Dades de característiques personals |  | Informació comercial |
|  | Dades de circumstàncies socials |  | Dades biomètriques |
|  | Dades acadèmiques i professionals |  | Religió o conviccions filosòfiques |
|  | Dades de gestió de visites o altres dades de gestió no econòmiques |  | Altres categories especials de dades: origen racial o ètnic, opinions polítiques, afiliació sindical, orientació/vida sexual |
|  | Dades genètiques |  | Altres (especificar) |

Categories de persones interessades: *pacients*

**3. Durada**

Aquest contracte té una durada vinculada a la vigència de l’expedient **CSdM 16/25-ASS.**

**4. Obligacions de l’encarregat del tractament**

L’encarregat del tractament i tot el seu personal s’obliga a:

1. Utilitzar les dades personals objecte de tractament, o les que reculli per a la seva inclusió, només per a la finalitat objecte d'aquest encàrrec. En cap cas pot utilitzar les dades per a finalitats pròpies.
2. Tractar les dades d’acord amb les instruccions del responsable del tractament.

Si l'encarregat del tractament considera que alguna de les instruccions infringeix l’RGPD o qualsevol altra disposició en matèria de protecció de dades de la Unió o dels estats membres, l'encarregat n’ha d’informar ense dilació indegudael responsable.

1. Portar, per escrit, un registre de totes les categories d’activitats de tractament efectuades per compte del responsable, que contingui:
2. El nom i les dades de contacte de l'encarregat o dels encarregats i de cada responsable per compte del qual actua l'encarregat i, si escau, del representant del responsable o de l’encarregat i del delegat de protecció de dades.
3. Les categories de tractaments efectuats per compte de cada responsable.
4. Si escau, les transferències de dades personals a un tercer país o organització internacional, inclosa la identificació d’aquest país o aquesta organització internacional, i en el cas de les transferències indicades a l'article 49, apartat 1, paràgraf segon de l’RGPD, la documentació de garanties adequades.
5. Una descripció general de les mesures tècniques i organitzatives de seguretat relatives a:

* La seudonimització i el xifrat de dades personals.
* La capacitat de garantir la confidencialitat, la integritat, la disponibilitat i la resiliència permanents dels sistemes i serveis de tractament.
* La capacitat de restaurar la disponibilitat i l’accés a les dades personals de forma ràpida, en cas d’incident físic o tècnic.
* El procés de verificació, avaluació i valoració regulars de l’eficàcia de les mesures tècniques i organitzatives que garanteixen l’eficàcia del tractament.

1. No comunicar les dades a terceres persones, tret que tingui l'autorització expressa del responsable del tractament, en els supòsits legalment admissibles.

L'encarregat pot comunicar les dades a altres encarregats del tractament del mateix responsable, d'acord amb les instruccions del responsable. En aquest cas, el responsable ha d’identificar, prèviament i per escrit, l'entitat a la qual s'han de comunicar les dades, les dades a comunicar i les mesures de seguretat que cal aplicar per procedir a la comunicació.

Si l'encarregat ha de transferir dades personals a un tercer país o a una organització internacional, en virtut del dret de la Unió o dels estats membres que li sigui aplicable, ha d’informar el responsable d'aquesta exigència legal de manera prèvia, tret que aquest dret ho prohibeixi per raons importants d'interès públic.

1. Subcontractació

No subcontractar cap de les prestacions que formin part de l'objecte d'aquest contracte que comportin el tractament de dades personals, tret dels serveis auxiliars necessaris per al normal funcionament dels serveis de l'encarregat.

Si cal subcontractar algun tractament, aquest fet s’ha de comunicar prèviament i per escrit al responsable, amb una antelació de **15 dies**. Cal indicar els tractaments que es pretén subcontractar i identificar de forma clara i inequívoca l'empresa subcontractista i les seves dades de contacte. La subcontractació es pot dur a terme si el responsable no manifesta la seva oposició en el termini establert.

El subcontractista, que també té la condició d'encarregat del tractament, està obligat igualment a complir les obligacions que aquest document estableix per a l'encarregat del tractament i les instruccions que dicti el responsable. Correspon a l'encarregat inicial regular la nova relació, de manera que el nou encarregat quedi subjecte a les mateixes condicions (instruccions, obligacions, mesures de seguretat…) i amb els mateixos requisits formals que ell, pel que fa al tractament adequat de les dades personals i a la garantia dels drets de les persones afectades. Si el subencarregat ho incompleix, l'encarregat inicial continua sent plenament responsable davant el responsable pel que fa al compliment de les *obligacions.*

1. Mantenir el deure de secret respecte de les dades de caràcter personal a les quals hagi tingut accés en virtut d’aquest encàrrec, fins i tot després que en finalitzi l’objecte.
2. Garantir que les persones autoritzades per tractar dades personals es comprometen, de forma expressa i per escrit, a respectar la confidencialitat i a complir les mesures de seguretat corresponents, de les quals cal informar-los convenientment. Es facilita models de documents veure Annex II - *document “Bones Pràctiques en l’ús de les TIC’s i en l’accés i Tractament de la informació” (annex II), així com annex II - document d’ “Informació i Compromís confidencialitat col·laboradors externs” i Annex IV - document de “Teletreball i Mesures de Protecció de Dades”.*
3. Mantenir a disposició del responsable la documentació que acredita que es compleix l'obligació que estableix l'apartat anterior.
4. Garantir la formació necessària en matèria de protecció de dades personals de les persones autoritzades per tractar dades personals.
5. Assistir el responsable del tractament en la resposta a l'exercici dels drets següents:
6. Accés, rectificació, supressió i oposició
7. Limitació del tractament
8. Portabilitat de dades
9. A no ser objecte de decisions individualitzades automatitzades (inclosa l’elaboració de perfils)

Quan les persones afectades exerceixin els drets d'accés, rectificació, supressió i oposició, limitació del tractament, portabilitat de dades i a no ser objecte de decisions individualitzades automatitzades, davant l'encarregat del tractament, aquest ho ha de comunicar per correu electrònic a l'adreça **lopd@csdm.cat**. La comunicació s’ha de fer de forma immediata i en cap cas més enllà de l’endemà del dia laborable en què s’ha rebut la sol·licitud7, juntament, si escau, amb altres informacions que puguin ser rellevants per resoldre la sol·licitud. (Veure Annex I – Dades de contacte Delegats de Protecció de Dades)

1. Dret d’informació

Correspon al responsable facilitar el dret d'informació en el moment de recollir les dades.

1. Notificació de violacions de la seguretat de les dades

L'encarregat del tractament ha d’informar el responsable del tractament, sense dilació indeguda i en qualsevol cas abans del termini màxim de **48hores**, i a través de correu **lopd@csdm.cat** , de les violacions de la seguretat de les dades personals al seu càrrec de les quals tingui coneixement, juntament amb tota la informació rellevant per documentar i comunicar la incidència. (Veure Annex I – Dades de contacte Delegats de Protecció de Dades).

La notificació no és necessària quan sigui improbable que aquesta violació de la seguretat constitueixi un risc per als drets i les llibertats de les persones físiques.

La notificació ha de detallar:

1. Descripció de la naturalesa de la violació de la seguretat de les dades personals, incloses, quan sigui possible, les categories i el nombre aproximat d'interessats afectats i les categories i el nombre aproximat de registres de dades personals afectats.
2. Nom i dades de contacte del delegat de protecció de dades o d'un altre punt de contacte en el qual es pugui obtenir més informació.
3. Descripció de les possibles conseqüències de la violació de la seguretat de les dades personals.
4. Descripció de les mesures adoptades o proposades per posar remei a la violació de la seguretat de les dades personals, incloses, si escau, les mesures adoptades per mitigar els possibles efectes negatius.

Si no és possible facilitar la informació simultàniament, i en la mesura en què no ho sigui, la informació s’ha de facilitar de manera gradual sense dilació indeguda.

Correspon al **responsable del tractament comunicar les violacions de seguretat de les dades a l'autoritat de protecció de dades**, així com **als interessats**, quan sigui probable que la violació suposi un alt risc per als drets i les llibertats de les persones físiques.

La comunicació s’ha de fer en un llenguatge clar i senzill i, com a mínim, cal:

1. *Explicar la naturalesa de la violació de dades.*
2. *Indicar el nom i les dades de contacte del delegat de protecció de dades o d’un altre punt de contacte en què es pugui obtenir més informació.*
3. *Descriure les possibles conseqüències de la violació de la seguretat de les dades personals.*
4. *Descriure les mesures adoptades o proposades pel responsable del tractament per posar remei a la violació de la seguretat de les dades personals, incloses, si escau, les mesures adoptades per mitigar els possibles efectes negatius.*
5. Donar suport al responsable del tractament a l’hora de fer les avaluacions d'impacte relatives a la protecció de dades, quan escaigui.
6. Donar suport al responsable del tractament a l’hora de fer les consultes prèvies a l'autoritat de control, quan escaigui.
7. Posar a disposició del responsable tota la informació necessària per demostrar que compleix les seves obligacions, així com per realitzar les auditories o les inspeccions que efectuïn el responsable o un altre auditor autoritzat per ell.

Implantar les mesures de seguretat següents:

**CSdM** manifesta i garanteix a **ENTITAT\_ET** que ha adoptat els mecanismes necessaris que es preveuen en el RGPD per preservar la confidencialitat, seguretat i integritat de les Dades Personals, tot això tenint en compte l'estat de la tècnica i el cost de la seva aplicació pel que fa als riscos i la naturalesa de les Dades Personals.

**ENTITAT\_ET** manifesta i garanteix a **CSdM** que té els coneixements especialitzats, fiabilitat i recursos, de cara a l'aplicació de **mesures tècniques i organitzatives** que compleixin els requisits del RGPD, inclosa la seguretat del tractament, necessaris per complir amb les obligacions d'aquest Contracte en relació a les Dades Personals.

Les mesures de seguretat en l’ accés a la historia clínica electrònica del CSdM ( HCE) :

* *Identificar el personal que es necessari que tinguí accés des de l’ENTITAT\_ET per la coordinació. Han de ser el menys possibles.*
* *Informar a CSdM de les dades personals necessàries d’aquest treballadors per poder facilitar l’acreditació a la HCE. CSdM facilitarà les credencials de forma individualitzada i son intransferibles.*
* *Mantenir actualitzada la relació de personal que realitza el servei. S’informarà a CSdM de qualsevol alta, baixa o modificació de funcions del personal assignat a aquestes tasques. Mínim un cop a l’any es demanarà ratificació de les persones assignades.*
* *Tota persona que presti el servei, haurà d’ estar assabentat i signar el document “Bones Pràctiques en l’ús de les TIC’s i en l’accés i Tractament de la informació” (annex II), així com document d’ “Informació i Compromís confidencialitat col·laboradors externs” (annex III) i document de “Teletreball i Mesures de Protecció de Dades” (annex IV).*
* *Per la consulta a la HCE, entre altres mesures recomanades a document de Teletreball, podem destacar:*
* *Accés des d’un lloc de treball segur i confidencial, protegit de l’accés/visualització de tercers.*
* *Mantenir l’accés a internet i el lloc de treball amb eines de protecció de cibersegurat (antivirus i/o EDR’s), Firewalls, ...*
* *Accés exclusiu a la persona autoritzada, no facilitar l’accés a terceres persones. Tots els accessos son monitoritzats i queden registrats per posteriors auditories d’accessos, i per tant l’usuari identificat en el accés és el responsable del mateix.*
* *Accés via VPN i amb doble factor a correu institucional de la ENTITAT\_ET*
* *Seguir les instruccions de seguretat de CSdM respecte a l’accés.*
* *Qualsevol vulnerabilitat de la confidencialitat o seguretat informar a lopd@csdm.cat.*

En tot cas, cal implantar mecanismes per:

1. Garantir la confidencialitat, integritat, disponibilitat i resiliència permanents dels sistemes i serveis de tractament
2. Restaurar la disponibilitat i l'accés a les dades personals de forma ràpida, en cas d'incident físic o tècnic.
3. Verificar, avaluar i valorar, de forma regular, l'eficàcia de les mesures tècniques i organitzatives implantades per garantir la seguretat del tractament.
4. Seudonimitzar i xifrar les dades personals, si escau.

Facilitar documentació a **CSdM** dels sistemes passius i actius de protecció

També ha d’adoptar totes aquelles altres mesures que, tenint en compte el conjunt de tractaments que duu a terme, siguin necessàries per garantir un nivell de seguretat adequat al risc.

1. Designar un delegat de protecció de dades i comunicar-ne la identitat i les dades de contacte al responsable.
2. Destí de les dades

Destruir les dades, una vegada complerta la prestació. Una vegada destruïdes, l'encarregat n’ha de certificar la destrucció per escrit i ha de lliurar el certificat al responsable del tractament.

No obstant això, l'encarregat pot conservar-ne una còpia, amb les dades degudament bloquejades, mentre es puguin derivar responsabilitats de l'execució de la prestació.

**5. Obligacions del responsable del tractament**

Correspon al responsable del tractament:

1. Lliurar a l'encarregat les dades a les quals es refereix la clàusula 2 d'aquest document.
2. Fer una avaluació de l'impacte en la protecció de dades personals de les operacions de tractament que ha d’efectuar l'encarregat.
3. Fer les consultes prèvies que correspongui.
4. Vetllar, abans i durant tot el tractament, perquè l’encarregat compleixi l’RGPD.
5. Supervisar el tractament, inclosa l’execució d’inspeccions i auditories.

**Com a prova de conformitat tot dues parts signen el present document, en** la data que consta en les signatures electròniques.

**Responsable de Tractament Encarregat del tractament**

**Nom:**   **Nom:**

**Càrrec:** Gerent  **Càrrec:**

**Entitat:** Consorci Sanitari del Maresme **Entitat:**

**Annex I Dades de contacte dels Delegats de Protecció de Dades**

* **Respecte la Protecció de Dades del Consorci Sanitari del Maresme**

Pàgina Web**: www.csdm.cat**

Adreça de contacte: Carretera de Cirera, 230, 08304 Mataró.

Telèfon de contacte: 937 417 700.

Email de contacte: **lopd@csdm.cat**

Email de contacte del Coordinador de Protecció de Dades: **dpd@csdm.cat**

Email de contacte del Delegat de Protecció de Dades: **dpd@ticsalutsocial.cat**

* **Respecte la Protecció de Dades de** NOM\_ENTITAT**.**

Pàgina Web**:** ???????

Adreça de contacte: ??????????.

Telèfon de contacte: ?????.

Email de contacte: **?????**

Email de contacte del Delegat de Protecció de Dades: **????**