CODI DE CONDUCTA: MESURES PREVENTIVES I BONES PRÀCTIQUES

En relació al Reglament (UE) 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 a la lliure circulació d'aquestes, i en aplicació de la normativa estatal i sectorial afectada en la matèria, la Fundació Els Tres Turons dissenya el present **Codi de Conducta: Mesures preventives i bones pràctiques** amb l'objectiu d'acomplir amb *la responsabilitat proactiva o accountability* i establir-ne normativa interna vers el tractament de les dades personals.

Índex

A qui afecta?

El **Codi de Conducta: Mesures preventives i bones pràctiques** afectarà a:

- Personal laboral (independentment de la tipologia del contracte)
- Personal prestador de serveis (contractació mercantil) o col·laboradors
- Voluntaris
- Alumne en pràctiques
- Qualsevol altra persona que, independentment de la relació amb l'entitat, tracti dades per compte d'aquesta.

Les disposicions que a continuació s'enumeraran se li aplicaran en allò que, per raó de la professió, contracte o tasques sigui d'aplicació.

Principis generals vers la Protecció de Dades

Qualsevol actuació realitzada haurà d'enfocar-se considerant-ne els següents principis en relació a les dades personals:

- S'hauran de tractar de forma lícita, lleial i transparent: és important que tractem les dades dels usuaris d'acord allò que se'ls informa i sota un pretext definit, és a dir, és important que les dades de qualsevol persona siguin emprades amb el seu consentiment, o bé, sota el pretext d'un contracte, obligació legal... No es poden tractar dades, per exemple, agafades d'internet o xarxes socials.
- S'han de recollir amb finalitats determinades, explicites i legitimes: les dades que volem o necessitem tractar per una determinada finalitat prèviament a la seva captació s'ha d'informar a l'usuari, detalladament, dels següents extrems: ¿per a què volem les dades? ¿en base a què volem les seves dades (contracte, el seu consentiment, interès legítim, la llei ens obliga / habilita...)?. En aquest punt, informant-lo de la finalitat implica que aquestes mateixes dades no podran emprar-se per altres finalitats incompatibles, excepte en cas d'arxiu en interès públic, investigació científica i històrica o finalitats estadístiques.
- En el formulari de captació de les dades en tot cas s'haurà de demanar les dades estrictament necessàries, sense excedir de la informació que podem necessitar. Per exemple: en cas d'iniciar un curs d'anglès seria excessiu sol·licitar dades referents a si algun familiar seu estudia o ha estudiat anglès, el seu nom i referencies. Davant qualsevol formulari que volem facilitar, llavors, s'ha de minimitzar les dades que demanem a les estrictament necessàries.

- No s'han d'emmagatzemar dades personals més enllà del temps necessari per a la finalitat del tractament. En definitiva, s'ha de procurar no emmagatzemar dades personals amb una expectativa relativa a llarg termini de poder necessitar-los.

- Per últim, s'ha de garantir la seguretat adequada de les dades personals, inclosa la protecció contra el tractament no autoritzat o il·lícit i contra la seva pèrdua, destrucció o dany accidental.

Obligacions generals

1.- S'ha de guardar el necessari secret respecte a qualsevol tipus d'informació de caràcter personal, empresarial i tècnica coneguda en funció del treball desenvolupat, inclòs un cop finalitzada la relació laboral. El personal ha de tractar (accedir, consultar...etc.) única i exclusivament aquelles dades que siguin necessàries per prestar el servei a l'usuari, limitant-se els tractaments d'acord amb les funcions i categoria professional de cada treballador/a vers els usuaris que es troben sota la seva responsabilitat. No poden tractar-se dades d'usuaris sinó és amb una finalitat estretament vinculada a la prestació assistencial o del servei de que es tracti.

2.- No s'ha de divulgar ni comunicar informació personal coneguda en funció del treball desenvolupat a terceres persones no vinculades a l'organització o persones que, encara que siguin internes i a raó de les seves tasques, no hagin de conèixer aquesta.

3.- S'han de desar tots els documents o suports que continguin informació personal en llocs segurs quan aquest no siguin utilitzats. En aquest sentit, és obligatori seguir una política de taules netes per la qual al final de la jornada tota informació amb dades de caràcter personal sigui desada en armaris o arxivadors amb clau.

Mesures informàtiques

4.- Les dades personals a les que té accés el personal professional i col·laboradors **només seran utilitzades amb la finalitat de la prestació dels serveis assistencials** del centre, garantint el compromís de confidencialitat i ètica professional.

El personal administratiu amb permís per accedir al Ekon ho farà exclusivament per dur a terme les tasques vinculades al seu perfil professional. Tals com la recollida de dades identificatives i de contacte dels usuaris, realitzar la tramesa d'aquestes al gestor documental i obrir nous expedients als mateixos. Fora d'aquestes tasques bàsiques, no es permet l'accés a dades personals contingudes en els expedients dels usuaris com diagnòstics o demés dades de caire assistencial.

5.- Tota persona amb accés informàtic a les dades, 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.

6.- Pel que fa als mecanismes de transmissió de la informació únicament s'utilitzaran els que estan autoritzats per l'entitat.

7.- No està permès copiar qualsevol informació o dades personals que constin als sistemes informàtics, en particular a l'EKON, en un ordinador personal, portàtil, USB... per a la seva sortida de l'entitat, centre o servei de treball, incloent-hi la sortida de dades personals per **FAX** .

8.- Donat que el correu electrònic ens permet encriptar les dades, es podrà fer ús d'aquest mitjà quan la urgència ho requereixi, **utilitzant el programari corresponent** per aquesta tasca (word, excel, adobe acrobat, etc...).

9.- Quan el personal professional o col·laborador finalitzi la seva jornada laboral o deixi el seu lloc de treball, **tancarà les aplicacions amb les que ha estat treballant, finalitzarà la seva sessió com a usuari i apagarà l'ordinador.** També, quan el personal abandoni temporalment el seu lloc de treball caldrà bloquejar manualment aquest (teclejar la tecla Win ⊞ + L). A la tornada, la desactivació de la pantalla protectora es realitzarà ingressant la seva contrasenya.

10.- Es prohibeix, sotmès a autorització del cap corresponent, prèvia valoració de la necessitat i conveniència, així com la intervenció del personal informàtic, instal·lar qualsevol tipus de programa informàtic.

11.-Els professionals han de desar la informació generada a **les carpetes de la xarxa (T) i simultàniament fer la tramesa de les mateixes a Ekon, mai a l'escriptori o les carpetes de perfil**. Si aquestes carpetes del perfil contenen molta informació es poden generar problemes en el funcionament del sistema. S'han de generar **accessos directes** dels documents des de les carpetes de xarxa, no desar el documents en les carpetes de perfil.

12.- Cada professional/col·laborador 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.**

13.- Cada professional/col·laborador haurà de procedir al canvi del seu contrasenya **quan el sistema així ho requereixi**. Així mateix, es mantindrà el bloqueig de pantalla que s'activarà automàticament i com a norma general cada 5 minuts sense activitat. El sistema sol·licitarà contrasenya per poder reactivar el bloqueig. Per als casos de persones que treballen de cara al públic, el bloqueig de pantalla s'activarà automàticament als 2 minuts d'inactivitat. Ambdós casos el sistema sol·licitarà la clau per poder reactivar el bloqueig. **Cada professional tindrà el seu popi compte i contrasenya els quals seran personals i intransferibles**, havent de guardar cura de la confidencialitat dels mateixos el titular d'aquests.

Ús d'Internet

14.-L'accés a Internet es limitarà als temes directament relacionats amb l'activitat socio-sanitària que presta l'Entitat i amb el lloc de treball de *cada professional*.

15- No està permès de debats en temps real (Chat/IRC. Messenger,etc), donada l'alta perillositat que suposa pel sistema la instal·lació del programari que permet els accessos no autoritzats al sistema informàtic.

16-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 cada professional.*

17.-Està prohibit introduir, descarregat d'Internet, reproduir, utilitzat o distribuir programes informàtics no autoritzats o sense llicència 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.

Registre d'Accessos

18.- Es prohibeix l'accés per part dels professionals a les històries o expedients de pacients / usuaris (informatitzats) quan l'accés no estigui justificat per motiu d'assistència o activitat.

19.- Es procedirà, de forma sistemàtica, a la revisió dels accessos realitzats a l'EKON i històries clíniques / expedients, escollint-se de forma aleatòria, per tal de verificar que els accessos esdevinguts són deguts en aplicació a la mesura anterior. En cas de detectar-ne un ús indegut s'iniciarà un procés d'investigació en el que el professional serà escoltat per determinar les causes i conseqüències d'aquest ús .

20.- És important tenir en compte que el fet de detectar-ne un ús indegut de les bases de dades informatitzades podria esdevenir la necessitat de notificar a l'Autoritat de Control (Autoritat Catalana de Protecció de Dades o Agència Espanyola de Protecció de Dades) una fuita de seguretat o, depenent de la casuística, al/s interessat/s afectat/s per aquest ús indegut, amb la corresponent possibilitat de ser incoat un procés d'investigació que derivés en una sanció econòmica. Per tant és important tenir en compte que:

"encara que, a raó del perfil del professional, aquest tingui permís per accedir a determinada informació personal, no necessàriament significa que es pugui accedir a aquesta. Únicament estarà legitimat l'accés a la informació quan sigui a raó de motiu assistencial o tractament continuat del pacient".

Respecte l'ús de l'USB

21.- Els ports USB no es troben habilitats. Si donades les funcions de l'usuari el port del seu equip de treball es troba obert, l'usuari haurà de prendre les següents cauteles:

- 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.
- Als dispositius USB no es podran emmagatzemar dades personals.
- El personal amb permís a accedir a aquests tipus de suports haurà de ser prèviament autoritzat per poder dur a terme un control.
- Els USB aniran clarament identificats, inventariant-se conjuntament amb l'inventari d'actius de la institució.

Respecte l'ús de tablets i telèfons mòbil

22.- Únicament el personal autoritzat pel Responsable del Tractament podrà tenir aquests dispositius.

23.-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. L'entitat es guarda la facultat de realitzar controls aleatoris sobre els dispositius per tal de verificar el correcte ús dels mateixos per part dels professionals.

24.-En el cas que resulti necessari emprar aquest tipus de suports, el Responsable del Tractament l'autoritzarà i en registrarà o inventariarà conjuntament amb l'inventari d'actius de la institució.

25.-Aquests dispositius hauran de disposar de contrasenya o codi d'accés.

26.-No és permesa la descàrrega de documents que continguin dades personals en aquests suports. Pel cas que resultés necessari fer la descàrrega, un cop realitzada i finalitzada la necessitat que la motivà caldrà eliminar les dades del dispositiu.

27.- 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.

28.-Resta prohibit enregistrar imatges amb els dispositius mòbils o tabletes que no siguin propietat de la institució (sempre que no sigui amb una finalitat directament vinculada amb les tasques del personal).

29.- Pel que fa a l'ús de apps de missatgeria instantània, aquest s'ha de restringir el màxim possible i sempre fent-se ús estrictament com a mitjà de difusió. En cap cas es podran compartir dades personals de caràcter sensible o bé documentació que contingui aquesta tipologia de dades. L'eina principal per a realitzar aquests enviaments telemàtics serà el correu electrònic corporatiu

Correu electrònic

30.-L'ús del correu electrònic serà el necessari per l'exercici de les funcions dels professionals

31.- Els professionals hauran de revisar la safata d'entrada, per sistemàtica, i com a mínim trimestralment, per tal d'eliminar els missatges que no s'hagin de conservar i arxivar-ne la resta, especialment els que poden tenir contingut personal.

32.- No s'hauran de desactivar filtres de correus i altres opcions de seguretat que s'hagin configurat pel departament informàtic.

33.-En cas de rebre missatges sospitosos, no obrir-los i comunicar-ho immediatament al personal informàtic o direcció.

34.- Valorar, i en el seu cas, emprar l'opció de còpia oculta (CCO), per enviar un correu electrònic a múltiples destinataris, especialment quan no pertanyin a la Fundació.

35.-En cas de reenviament d'un correu electrònic rebut, s'haurà d'eliminar les adreces anteriors per no difondre-les, així com revisar el contingut de la conversació per evitar accessos indeguts.

36.- Quan sigui necessari es podrà emprar el correu electrònic per enviar dades de caràcter personal. L'enviament sempre s'ha de realitzar només quan es tinguin garanties de que el destinatari del correu està autoritzat a accedir a les dades que contingui el correu o la documentació adjunta. Quan el correu contingui dades especialment protegides o categoria especial de dades (origen ètnic o racial, opinions polítiques, conviccions religioses o filosòfiques, afiliació sindicals, genètiques o biomètriques, de salut, socials, de vida sexual o orientació sexual) l'enviament haurà de ser realitzat emprant el programari específic per a la seva encriptació a través de contrasenya, la qual s'haurà de facilitar al destinatari a través de telèfon, intentant evitar emprar sempre el mateix. S'ha d'evitar l'enviament de la clau de pas a la documentació encriptada en un segon correu, de manera que la informació encriptada i la clau de pas es facilitin per canals diferents.

Mesures Físiques

37.- S'haurà de garantir el destí últim del paper inservible o duplicat que continguin dades personals (mai originals de documentació que integri l'expedient de l'usuari) mitjançant la seva destrucció a través de la màquina trituradora de paper o un servei extern especialitzat. Aquesta mesura és necessària per garantir la confidencialitat i per evitar que existeixi el risc d'accés per part de personal no autoritzat. L'entitat recorda que s'està implementat la política de zero paper en l'activitat diària, de manera que els professionals han de minimitzar l'ús de paper en la seva tasca de treball i prioritzar l'ús de la informació en pantalla (Ekon, gestor documental, servidors...etc.).

38.- Els suports informàtics que tinguin dades personals, (per exemple: dades de nòmines per les entitats financeres, dades de declaracions tributàries per Hisenda en CD o d'altres suports) 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. A més, aquest suport, haurà d'estar custodiat en un armari o dispositiu sota clau.

39.-Tots els suports i/o documents amb dades personals que, per raons autoritzades i, independentment de la tipologia de les dades, surtin del centre s'hauran d'anotar al Registre d'entrades i sortides d'acord al protocol configurat a tal efecte.

Respecte els expedients de les persones usuàries

40.- Els arxius on estiguin ubicats els expedients dels usuaris han d'estar tancats sota clau. La clau ha de quedar sota la custòdia d'administració i, en cas d'incident amb aquesta, s'haurà de notificar.

41.-La consulta d'un expedient en format paper ha de ser anotada en el document de registre que es gestiona des de recepció / administració, en cas contrari no s'entregarà la clau de l'arxiu.

42.-Es prohibeix fer còpies de les claus sense autorització expressa de la direcció, així com deixar-les en cap lloc accessible per persones no autoritzades.

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

44.-La devolució dels expedients a l'arxiu ha de realitzar-se immediatament després de la circumstància que va motivar la seva petició.

45.-<u>Està absolutament prohibit treure els expedients de les persones usuàries fora del centre.</u>

Personal de recepció o admissions

46.-El personal *que realitza les acollides dels usuaris* ha d'informar-los, sobre l'existència dels tractaments duts a terme sobre les seves dades personals, la finalitat de la recollida de les dades i els destinataris de la informació, i farà signar a l'usuari el "Full d'informació i consentiment".

47.- Queda expressament prohibida la difusió de dades, sense autorització expressa del *usuari/a* o representant.

48.- De tot això es deriva certs criteris en el moment de resposta a preguntes telefòniques com presencials:

- Preguntes per <u>telèfon</u> i actitud a prendre: si pregunten per un/una *usuari/a d'algun dels nostres serveis*:

  A. Informar als *usuaris/es* sobre la pràctica del centre de passar trucades a *als diferents tallers o activitats*. En el cas de que el *usuari/usuària* es negui es recollirà per escrit i es respectarà el seu dret a la confidencialitat.

  B. Quan alguna persona demani per un usuari/a directament, prèviament es parlarà amb l'educador de referència per tal de demanar-li si pot passar la trucada.

- preguntes en <u>presència física</u> i actitud a prendre: si pregunten presencialment per un/una *usuari/a d'algun dels nostres serveis*:

  A. Si l'usuari/a es troba vinculat en l'actualitat a alguns dels serveis de la Fundació, se li comunicarà al professional de referència que hi ha una persona que demana per l'usuari/a. **En cap cas es conduirà a la persona a les àrees de treball.**

  B. Si l' usuari/a per qui es pregunta no es troba vinculat a l'actualitat a cap dels nostres serveis igualment es contactarà amb el professional de referència o amb el responsable del servei en el que havia estat perquè doni les explicacions pertinents. **En cap cas es donarà informació de cap usuari/a.**

Demandes d'informació sobre les persones usuàries i tràmits administratius

49- Donat l'alt nivell de confidencialitat de les dades amb que es treballa s'haurà de tenir en compte:

A. Les peticions d'informes les ha de fer el propi usuari, si ho fa una tercera persona, ha de: En el cas que es tracti d'una altra persona que el representi haurà d'estar acompanyat d'una autorització signada pel propi usuari i còpia del DNI.

B. Només es podrà transmetre informació sobre l'usuari a altres professionals vinculats a dispositius soci-sanitaris i relacionats amb el seu pla de treball.

Mesures sobre la comunicació de dades als Forces i Cossos de Seguretat

50.- La cessió de dades de caràcter personal als membres de les Forces i Cossos de Seguretat no vulnera la normativa en matèria de protecció de dades sempre que es compleixin les següents condicions:

- Acreditació suficient del perill o delicte (atestat, resolució policial, resolució judicial...)
- Petició concreta i específica, adreçada al cas concret (no massiva)
- Deguda motivació de la petició, que acrediti la relació amb el perill o delicte exposat

Conseqüències de l'incompliment de les funcions i obligacions

51.- El compliment d'aquest decàleg de mesures preventives i bones pràctiques és important degut al règim sancionador que preveu el Reglament (UE) 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 a la lliure circulació d'aquestes, així com el desenvolupament que en realitza la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals.

Encara que la responsabilitat sobre una infracció derivada d'aquesta normativa és del Responsable del Tractament, també se'n poden derivar responsabilitats de caràcter penal i civil, les quals podrien afectar el treballador, així com prendre's mesures laborals d'acord a la normativa laboral general i sectorial, en particular, a allò que disposa el Conveni Col·lectiu de treball dels Hospitals d'Aguts, centres d'Atenció Primària, centres Sociosanitaris i centres de Salut Mental, concertats amb el Servei Català de Salut.

52.- El règim de multes administratives regulat pel Reglament de Protecció de Dades es troba a l'article 83 del text normatiu sancionant comportaments, en especial com a molt greus, el fet de no informar els interessats dels drets ARCO o del tractament de les dades, o no demanar el consentiment quan sigui necessari, o bé no donar curs a la notificació de fuites de seguretat. Les multes administratives a les quals es poden arribar assoleixen la quantitat de 20.000.000EUR com a màxim o bé, si és una empresa, una quantitat equivalent al 4% com a màxim del volum de negoci total anual global de l'exercici financer anterior, optant-se per la quantitat més gran.

Règim disciplinari (laboral)

53.- En tant al règim disciplinari, el qual afectarà els professionals en cas d'incompliment del present Codi de Conducta o qualsevol dels protocols reguladors d'aspectes relacionats amb protecció de dades, es regirà pel Conveni Col·lectiu de treball dels Hospitals d'Aguts, centres d'Atenció Primària, centres Sociosanitaris i centres de Salut Mental, concertats amb el Servei Català de Salut.

i. INFRACCIONS

Segons aquest text normatiu, les infraccions poden ser (entre d'altres):

Lleus	Inobservança intranscendent de normes o mesures reglamentàries i d'higiene.
Menys greus	Reiteració o reincidència en la comissió de faltes lleus, no es posa cura en la prestació d servei amb la diligència que cal, la mera desobediència als superiors en qualsevol matèria del servei, sempre que la negativa no fos manifestada expressament, cas en què qualificarà com a falta greu, o bé la imprudència en el treball respecte del que preveu qualsevol de les normes sobre seguretat.
Greus	Reiteració o reincidència en la comissió de faltes menys greus, les d'indiscreció negligència o d'ètica professional, sempre que no motivin reclamació per part de tercers o impliquin perjudicis irreparables, cas en què es qualificaran com a faltes molt greus.
Molt Greus	Indisciplina o desobediència a la feina.

ii. SANCIONS

Les sancions que corresponen a les infraccions del punt que precedeix són les següents (art. 62 del conveni).

Lleus	Amonestació verbal o per escrit; suspensió de sou i feina fins a dos dies.
Menys greus	Suspensió de sou i feina de 3 a 10 dies.
Greus	Suspensió de sou i feina d11 a 20 dies.
Molt Greus	Suspensió de sou i feina de 21 a 60 dies; trasllat de departament o servei per un període 3 mesos fins a un any; inhabilitació per ascendir de categoria durant tres anys com màxim; acomiadament.

Aspectes finals

El present Codi de Conducta esdevé un text genèric de mesures i conductes que s'han de tenir en compte, però durant les tasques diàries de tots els professionals i treballadors de la Fundació es podrien donar casuístiques les quals no sigui d'aplicació el que es preveu en aquest text. Per això, s'ha habilitat un correu electrònic per adreçar les consultes que es puguin tenir en relació a la protecció de dades, podent dirigint-nos al Delegat de Protecció de Dades a dpd@els3turons.org

A més del decàleg d'aquest text, no obstant això, el professional a més tindrà en compte tots els protocols, instruccions, annexos... que es posin al seu abast i que podrien complementar el que estableix el present Codi de Conducta, en especial els que fan referència a fuites de seguretat (o incidències) així com drets ARCO, entre d'altres. Per últim, si l'usuari troba una contradicció entre el present Codi de Conducta i un protocol, instrucció, annex específic sobre una matèria tractada en aquell, tindrà més rellevància el que estableixi la norma especial, és a dir, el protocol, instrucció, etc.

El present Codi de Conducta serà revisat de forma anual, o bé, davant situacions substancials que motivin la seva revisió i modificació extraordinària. Qualsevol canvi produït en aquest serà comunicat als usuaris a través del correu corporatiu.

Barcelona, març 2021.

FUNDACIÓ ELS TRES turons
Fastenrath, 208-212 - BCN 08032
tel. 93 429 32 10 - fax: 93 420 86 96
NIF: G-63027411
www.els3turons.org
fundació@els3turons.org

Signa i aprova aquest document:

Alfons J. Santos Rodríguez

Director.