GUIA DE BONES PRÀCTIQUES EN MATÈRIA DE SEGURETAT I PROTECCIÓ DE DADES PER ALS PROFESSIONALS I COL·LABORADORS D'ASPACE

Aquest document de Bones Pràctiques s'ha d'entendre com un codi de conducta per a tots els treballadors i col·laboradors d'ASPACE a fi d'acomplir amb el Reglament (UE) 2016/679 General de Protecció de Dades (en endavant, RGPD) així com per assegurar una millora contínua en la pràctica professional vers aquest àmbit, mitjançant l'establiment d'unes pautes de conducta i fomentant una major conscienciació dels treballadors en el tractament de les dades de caràcter personal dels usuaris atesos.

Les bones pràctiques són aplicables a totes les dades, i particularment a les de caràcter personal. Amb l'entrada en vigor del nou reglament europeu no distingim en nivells de seguretat de les dades ni en mesures específiques a aplicar en funció del nivell de seguretat de les dades. El que sí cal tenir present és que ASPACE tracta amb dades especialment sensibles i per tant s'han d'establir les mesures que calgui per tal d'evitar els riscos que poden suposar les operacions de tractament de dades per als drets i les llibertats fonamentals de les persones.

Aquest document de Bones Pràctiques està basat en el RGPD i en la Política de Seguretat de la Informació d'ASPACE, on consta procediments, mesures de seguretat, protocols i conseqüències en cas d'incompliment de les mesures.

A continuació detallem les **mesures de seguretat i bones pràctiques** que tot treballador que tracta amb Dades de Caràcter Personal (DCP) ha de tenir present.

1. CONFIDENCIALITAT (punt 8 de la Política de Seguretat)

a. Tots els treballadors i voluntaris d'ASPACE, com a usuaris que tenen accés i tracten DCP, tenen l'OBLIGACIÓ PERSONAL DE CARÀCTER PERMANENT DEL **DEURE DE SECRET** (inclús finalitzada la relació contractual amb ASPACE).

b. Degut a que a ASPACE es treballa amb dades especialment sensibles, és molt important que abans de plantejar qualsevol nova activitat o tractament de les mateixes, de forma proactiva s'avaluïn els **riscos** que aquest tractament pot suposar per a la seva privacitat, i s'apliquin les **mesures** necessàries per a evitar o minimitzar aquests riscos. Tots els treballadors són corresponsables de la privacitat de les dades.

c. Tot treballador ha de comunicar al seu responsable qualsevol **incidència** o situació que comporti un risc per als drets i llibertats de qualsevol persona (ex. trobar un document amb dades personals en un lloc accessible a tothom) i aquest ho haurà de comunicar al Delegat de Protecció de Dades de l'entitat per tal de comunicar-ho a l'Autoritat competent (Agència Catalana de Protecció de Dades) i gestionar la incidència o violació de dades. El nou Reglament obliga a notificar les Violacions de Seguretat a les autoritat de control en un màxim de 72 hores.

2. CAPTACIÓ DE DADES (punt 5.2 de la Política de Seguretat)-ús adequat de les dades

a. DRET A INFORMACIÓ. Sempre s'haurà d'**informar** a l'usuari atès, quan sol·licitem les seves dades, de qui és el Responsable de tractament (ASPACE) de les seves dades personals, el contacte del Delegat de Protecció de Dades de l'entitat, la finalitat del tractament, la base jurídica o legitimació, els destinataris a qui se cedirà aquesta informació (si s'escau), els seus drets vers aquestes dades i el termini de conservació de les dades que sol·licitem.
El consentiment tàcit no serveix, i s'ha d'obtenir consentiment per tractar les dades per a cada finalitat diferenciada. Hem d'informar de manera clara i senzilla.

b. Les dades recollides només podran ser utilitzades amb la **finalitat** amb la qual van ser captades. Per tant, si per exemple es van recollir amb una finalitat d'assistència mèdico-sanitària, no podran fer-se servir per altres finalitat com ara recerca, docència, difusió de l'entitat, etc. En cas necessari caldrà tornar a demanar consentiment exprés indicant la finalitat concreta de la captació de les dades personals.

c. Per a la investigació o docència, s'haurà de disposar d'un consentiment exprés de la família o pacient (no serveix el consentiment que signa el pacient amb la finalitat d'assistència sanitària).

d. Qualsevol informació de caràcter personal que arribi per qualsevol canal (paper, e-mail, etc.) i que no s'hagi d'incorporar als fitxers (o per la que no es disposi d'autorització) s'haurà de **destruir** de forma immediata d'acord amb el procediment establert sobre Destrucció de dades (5.4.11. de la Política de Seguretat)

e. No es podrà fer servir els **telèfons mòbils personals** per **captar imatges o vídeos** de pacients ni usuaris encara que es faci servir per finalitats assistencials. En el cas de voler gravar vídeos amb finalitats assistencials, s'haurà d'utilitzar les càmeres d'ASPACE o haurà d'estar autoritzat per la direcció d'ASPACE. En aquest darrer cas que s'utilitzi com a excepció sempre s'haurà d'eliminar / destruir un cop gravat en el servidor d'ASPACE el més aviat possible.

f. Les dades sol·licitades hauran de ser **pertinents, adequades i no excessives**, això vol dir que no hem de sol·licitar dades que no siguin necessàries per a la finalitat amb les que les demanem.

3. EMMAGATZEMAMENT DE LES DADES (punt 5.3 de la Política de Seguretat)

a. Els arxius i servidors on estigui ubicada la informació 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 a persones no autoritzades.

b. La informació en suport paper s'emmagatzemarà en els arxius designats a tal efecte, a on només tindran accés les persones responsables i autoritzades per la direcció d'ASPACE. No es permetrà fer-ne còpies ni traslladar la informació sense l'autorització expressa del responsable del fitxer.

c. La informació en suport electrònic s'ha d'emmagatzemar als servidors i aplicacions d'Aspace. No es pot emmagatzemar en els discos locals (P Ex. Carpeta "mis documentos", escriptori, etc)

ni en dispositius portàtils o extraïbles (p.ex: pendrives, discos externs, CD), i mai s'ha d'extreure aquesta informació fora de les instal·lacions d'Aspace, llevat de les excepcions previstes a la política de seguretat d'Aspace. En aquests casos excepcional s'hauria de complir els següents requisits:

a. Sempre de **forma temporal**
b. Amb una raó **justificada**
c. Amb autorització per part de la direcció d'ASPACE

Un cop la raó desapareix la informació cal traspassar-la de nou al servidor, assegurant-se que no es perdin modificacions que es puguin haver fet al servidor i que a l'equip local no quedi cap rastre de la informació.

d. En aquells casos que s'accepti la gravació i transport d'informació per mitjà de suports informàtics, aquests sempre han de ser propietat d'Aspace (i mai suports particulars), i han d'estar etiquetats pel Departament TIC. En els casos que continguin informació de nivell alt també caldrà encriptar-los i protegir-los per contrasenya per tal de minimitzar-ne el risc d'accessos indeguts en cas de pèrdua o sostracció

e. Mentre la documentació física no es troba arxivada en el seu arxiu, la persona o treballador que es trobi a càrrec de la informació serà responsable de la custòdia de la informació i d'impedir-ne l'accés no autoritzat.

4. ACCÉS A LES DADES DE CARÀCTER PERSONAL (punt 5.5 de la Política de Seguretat)

EN SUPORT PAPER

a. Només podran accedir a la informació present en els arxius físics les persones degudament autoritzades per la direcció d'ASPACE. Per tant, està prohibit accedir a dades que, d'acord amb les funcions a desenvolupar, corresponguin a un altre perfil d'accés.

b. Els accessos a la informació dels arxius físics s'hauran d'indicar al registre d'entrades i sortides d'acord amb els procediments indicats a la Política de Seguretat.

c. Les entrades i les sortides de les històries clíniques en format paper, tant de l'arxiu físic com de qualsevol centre d'ASPACE (casos excepcionals) hauran d'estar degudament autoritzades per la direcció d'ASPACE.

d. Durant el període en què la informació es troba fora del seu arxiu, tot el personal ha de vetllar per evitar qualsevol incidència.

e. La devolució de la informació a l'arxiu ha de realitzar-se immediatament després de la circumstància que va motivar la seva petició. No es podrà transferir aquesta informació entre professionals sense que quedi registrada la corresponent entrada i sortida.

EN SUPORT INFORMÀTIC

a. Només podran accedir a la informació present en els servidors informàtics les persones degudament autoritzades per la direcció d'ASPACE. Cada treballador només tindrà accés als recursos que necessiti per al desenvolupament de les seves funcions. Per tant, està prohibit accedir a dades que, d'acord amb les funcions a desenvolupar, corresponguin a un altre perfil d'accés. En cas de detectar un accés innecessari o dubtós, cal reportar-ho com a possible incidència de seguretat.

b. A aquestes persones se'ls assignarà un codi d'usuari i una clau personal i **intransferible**, que haurà de procurar que no sigui visualitzada per ningú que la pugui utilitzar sense autorització.

c. Cada treballador 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 per correu electrònic al departament d'informàtica per tal que s'enregistri com a incidència i es pugui procedir al seu canvi.

d. Cada treballador haurà de procedir al canvi de la seva clau d'accés quan el sistema així ho requereixi.

e. Quan un treballador finalitzi la seva jornada laboral, tancarà les aplicacions amb les que ha estat treballant, finalitzarà la seva sessió com a usuari i apagarà l'ordinador.

f. Quan deixi el seu lloc de treball temporalment, bloquejarà la seva sessió (fent CTRL-ALT-SUPR) de forma que ningú altre pugui accedir a les dades en la seva absència.

g. En general, no ha de poder sortir del centre de treball cap documentació o suport generat a la feina, sense l'autorització de la direcció d'ASPACE. S'ha de registrar qualsevol entrada o sortida de suports que incorporin dades de caràcter personal, inclús si van adreçades a un altre centre d'ASPACE.

5. ÚS ADEQUAT DELS EQUIPS DE TREBALL (punt 4.3 de la Política de Seguretat)

a. Queda prohibit introduir, descarregar d'Internet, reproduir, utilitzar o distribuir programes informàtics no autoritzats o sense llicència 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.

b. L'accés a internet i el correu electrònic ha de ser d'ús exclusivament professional.

c. No es permet al personal d'Aspace l'ús **d'eines de sincronització i còpia de seguretat (Dropbox, Google Drive, SkyDrive, etc.)** per a emmagatzemar dades de caràcter personal de qualsevol dels fitxers propietat d'Aspace.

d. No es permet al personal d'Aspace l'ús d'**eines de control i accés remot** per a connectar-se des de fora de les instal·lacions d'Aspace, llevat de les excepcions recollides a la Política de Seguretat.

6. ENTREGA D'INFORMACIÓ (punts 5.5.7 i 9 de la Política de Seguretat)

a. Com a norma general la informació no ha de sortir de l'entitat, llevat d'aquells casos que es justifiquin per a la prestació dels serveis d'Aspace, i sempre amb autorització.

b. Davant de requeriments de dades per part d'usuaris/pacients, només es podrà donar la informació al titular de les dades, al seu tutor legal en cas que la persona estigui incapacitada, o a una persona que hagi estat autoritzada pel titular o tutor. En cas de dubte, és millor no donar la informació.

c. També s'ha de donar informació en el cas que hi hagi obligació legal de donar-la (ex. jutjats, cossos de seguretat amb autorització judicial, etc.).

d. Tota persona que cedeix les seves dades (també els treballadors) pot exercir els drets que li reconeix el RGPD (accés, rectificació, oposició, supressió, portabilitat i limitació del tractament). Tots els treballadors d'Aspace han de comunicar al seu responsable qualsevol sol·licitud relativa a aquests drets per tal que se li pugui donar resposta en el termini establert (30 dies). En cas necessari es pot adreçar a la persona sol·licitant a la pàgina web www.aspace.cat/ca/protecciodedades, on s'explica la manera d'exercir aquests drets.

7. TRANSPORT I ENVIAMENT D'INFORMACIÓ (punt 5.3 de la Política de Seguretat)

a. Com a consideració inicial, sempre que sigui possible, cal optar per enviar la informació de forma telemàtica (e-mail). En aquest cas caldrà **encriptar** aquella informació que inclogui dades especialment protegides (salut, religió, etc.). Les dades de caràcter personal de tipus identificatiu, de contacte o per exemple un CV no cal encriptar-les. Mireu el document ***"Annex2-Procediment d'encriptació segura d'arxius"*,** on queda descrit el procediment d'encriptació i desencriptació d'arxius.

b. En cas que calgui transportar suports físics amb informació, cal prendre precaucions per tal d'evitar que la seva pèrdua o sostracció pugui propiciar accessos indeguts. El transport ha de ser segur i per a això hi ha dues opcions:
   - Mitjançant empresa de missatgeria o transport que garanteixi la confidencialitat i seguretat de la informació.
   - En cas de ser transportat per mitjans propis, cal fer servir sobres o altres contenidors tancats. En el cas que la informació sigui de nivell alt caldrà utilitzar un maletí o caixa de seguretat tancat amb clau.

c. És totalment prohibit fer tramesa d'Informació confidencial o sensible sense dissociar per FAX donat que és un mitjà intrínsecament insegur que no permet l'encriptació de la informació.

d. Si en algun cas no s'ha encriptat un arxiu o s'ha enviat per fax un document amb dades especialment protegides, perquè no s'ha pogut evitar, cal que el treballador ho comuniqui com a INCIDÈNCIA a través del correu protecciodedades@aspace.cat

Incompliment i Mesures associades

El no compliment de qualsevol de les mesures aquí descrites es considerarà com una infracció per desobediència de les normes internes d'ASPACE i donarà lloc a una falta.

Tota falta comesa per un/a treballador/a es classificarà com a lleu, greu o molt greu segons el conveni col·lectiu d'aplicació o la normativa de l'Estatut dels Treballadors i s'aplicaran les mesures disciplinàries atès el grau de les faltes.