De: Comité de Seguretat LOPD
A: Tots
Data: Abril 2018
Objecte: Manual de Bones Pràctiques en matèria de protecció de dades i confidencialitat.

1. Introducció

Amb l'objectiu de garantir la confidencialitat i seguretat de les dades personals tractades per l'Hospital Clínic de Barcelona (en endavant "HCB"), i per tal de donar compliment Reglament Europeu 2016/679, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques en el que respecta el tractament de dades personals i a la lliure circulació d'aquestes dades (en endavant el "Reglament"), així com a la seva normativa de desenvolupament, s'estableixen les directrius següents que han de complir tots els treballadors/es o col·laborador/es de l'HCB.

El compliment del Reglament implica a tots els treballadors/es i col·laborador/es de l'HCB, i a través d'aquest Manual de Bones Pràctiques l'HCB pretén donar directrius per a facilitar-ne el seu compliment. Així mateix, trobareu més informació relativa al compliment de la normativa de protecció de dades a l'espai de protecció de dades de Serveis Jurídics de l'intranet.

La versió actualitzada d'aquest document la podreu trobar a la intranet.

2. Deure de confidencialitat

Queda prohibit l'ús o la divulgació d'informació confidencial de l'HCB. Aquesta prohibició afecta a la informació o documentació referent a persones físiques i, per tant, susceptible de ser protegida per la normativa de protecció de dades.

A excepció de la presa d'imatges amb finalitats assistencials, queda prohibida la presa d'imatges o la gravació de veus de pacients, professionals o altres persones en les instal·lacions de l'HCB, sense el seu consentiment. Així mateix, queda prohibida la presa de qualsevol tipus d'imatge en zones d'hospitalització i d'atenció als pacients. En cas que es consideri d'interès la presa d'imatges per a activitats d'investigació, docents o de divulgació científica caldrà obtenir el consentiment firmat del pacient i, per a això, es poden trobar models de consentiment a l'espai de protecció de dades de Serveis Jurídics de la intranet.

Tots els professionals sanitaris estan sotmesos al deure de secret professional recollit pels respectius codis deontològics. A més, tots els treballadors/es que en el desenvolupament de les seves funcions tingui accés a dades personals queda obligat al deure de secret. El deure de confidencialitat es mantindrà al llarg de tota la relació laboral i continuarà vigent una vegada finalitzada la mateixa.

3. Mesures informàtiques

Les dades personals a les que tenen accés els treballadors/es seran utilitzades garantint el compromís de confidencialitat i l'ètica professional.

Cada usuari amb accés a fitxers informàtics que continguin dades personals, tindrà cura que quan aquestes es visualitzin per pantalla o s'imprimeixin, no puguin ser visualitzades per persones no autoritzades.

La informació sempre s'ha de desar a les unitats de xarxa (:/F, :/U, etc.) dels ordinadors, de les que es fa còpia de seguretat de manera automàtica.

La creació de bases de dades fora del SAP, que continguin dades de pacients o de treballadors identificables, requerirà l'autorització de Sistemes d'Informació a través de la sol·licitud corresponent.

Queda prohibit l'ús de dispositius compartits, pendrive, memòries extraïbles o eïnes d'emmagatzemament al núvol (ondrive, dropbox, google drive i similars) per a l'emmagatzemament de dades de pacients o treballadors identificables.

No està permès enviar dades de salut identificables per fax. La informació relativa a la salut es podrà enviar sempre i quan no s'identifiqui al titular de les dades. Per tant, la informació es podrà enviar per fax sempre i quan estigui anonimitzada o dissociada mitjançant un codi.

No es permetrà l'enviament de la informació escanejada a través de les impressores multi-funció a adreces externes diferents a la del domini corporatiu "clinic.cat.".

En cas que s'hagin d'enviar correus electrònics amb dades de salut, les dades han d'anar encriptades. El Servei d'Atenció a l'Usuari disposa d'un manual per encriptar els adjunts de correu, i se'ls hi pot demanar al 2729 o a SAU@clinic.ub.es

Quan un treballador/a finalitzi la seva jornada laboral o deixi el seu lloc de treball durant un període de temps determinat, tancarà les aplicacions amb les que ha estat treballant, finalitzarà la seva sessió com a usuari i apagarà l'equip informàtic (excepte que aquest sigui de contingència).

Si des de la Direcció de Sistemes d'informació es detecta un equip que no s'hagi aturat, amb la sessió bloquejada, i que presenta un temps d'inactivitat superior a les 24 hores, la Direcció de Sistemes d'informació podrà adoptar la mesura d'aturar l'equip.

Els treballadors/es, quan accedeixin a dades personals mitjançant la seva clau d'usuari informàtic, hauran de procurar que aquesta no sigui visualitzada per ningú que la pugui utilitzar sense autorització. **Cada usuari és responsable de la confidencialitat de la seva clau d'accés. Aquesta clau no s'ha de proporcionar a ningú, no ha de ser enviada per correu electrònic, ni s'ha d'introduir en servidors que no siguin de l'HCB**. En cas que sigui coneguda per persones no autoritzades, haurà de notificar-

ho i registrar-ho com incidència i procedir al seu canvi. El procediment de notificació d'incidències està detallat al Document de Seguretat.

Quan el treballador/a abandoni el lloc de treball temporalment, caldrà que **activi manualment el bloqueig de la pantalla** (per bloquejar la pantalla s'hauran de prémer simultàniament tecla Windows + L), **protegit amb contrasenya**.

Accés a internet i ús del correu electrònic

La xarxa de l'HCB, els sistemes d'informació de l'HCB, el telèfon, el mòbil, els terminals, els equips informàtics el correu electrònic i l'accés a internet són eines que es posen a disposició dels empleats amb la finalitat de donar compliment a les seves atribucions laborals.

Aquestes eines puntualment i de manera raonable es podran utilitzar amb finalitats personals, d'acord amb els usos socials comunament acceptats.

Està prohibit introduir, descarregar d'Internet, reproduir, utilitzar o distribuir programes informàtics no autoritzats o sense llicència. Per instal·lar qualsevol programari es requereix l'aprovació de la DSI.

En casos que existeixin raons fonamentades, la Direcció de l'Hospital podrà exercir la seva capacitat de control per tal d'evitar l'abús o l'ús indegut de les eines posades a disposició dels empleats. En cas de constatar comportaments abusius o indeguts serà d'aplicació el règim disciplinari.

A tal efecte, les dades o arxius amb finalitats personals que els empleats puguin desar, no tindran el caràcter de confidencials, de manera que es podran revisar en exercici de la capacitat de control esmentada.

4. Mesures en relació a les dades en suport paper

El treballador usuari, quan s'absenti de la seva taula de treball o bé quan finalitzi la seva jornada laboral, haurà de guardar tots aquells documents que continguin informació que pogués ser de caràcter personal o confidencial.

En utilitzar impressores o fotocopiadores, haurà de recollir els documents originals en finalitzar i que no quedin documents amb dades de caràcter personal o confidencial en la safata de sortida. Si les impressores són compartides amb altres usuaris sense accés a les dades que estan sent impreses, s'hauran de retirar els documents conforme vagin sent impresos.

De la mateixa manera, en utilitzar els escàners haurà de recollir els documents originals i, si la carpeta de destinació es compartida amb usuaris sense accés a aquestes dades, ha d'eliminar l'arxiu d'aquesta carpeta i traslladar-ho a una altra carpeta amb un nivell de seguretat concorde a les dades que contenen.

S'haurà de garantir la destrucció segura de la documentació que contingui dades personals i ja no tingui utilitat, així com de la documentació duplicada, mitjançant les

màquines destructores de paper o els containers metàl·lics de destrucció de documentació confidencial ubicats a les dependències de l'Hospital.

Mentre hi hagi documentació clínica fora del seu lloc d'arxiu, el treballador/a que la custòdia ha de vetllar per evitar qualsevol accés per part de persones no autoritzades.

En el cas de les històries clíniques la devolució de qualsevol documentació clínica a l'Arxiu ha de realitzar-se immediatament després de la circumstància que va motivar la seva petició, i conforme les instruccions donades a la Guia per l'Ús de la Documentació Clínica.

Està totalment prohibit treure documentació clínica fora de l'HCB sense autorització expressa del Cap de Documentació Clínica.

En l'àmbit de l'HCB, la documentació continguda en les històries clíniques s'utilitzarà exclusivament amb finalitats assistencials. Qualsevol altre ús s'haurà de fer de conformitat amb l'establert a la Guia per l'Ús de la Documentació Clínica.

5. Lliurament de documentació clínica i informació relativa a pacients

Les dades relatives a l'assistència del pacient són de la seva propietat i l'HCB en té la custòdia. En conseqüència, la informació relativa als pacients sols podrà lliurar al pacient, a altres persones degudament autoritzades per ell, o legalment autoritzades.

L'HCB disposa de protocols de lliurament d'informació assistencial, que especifica els diversos procediments a seguir i els requisits que han de complir els sol·licitants d'informació. També disposa d'un model d'autorització per al lliurament d'informació a tercers. Aquests protocols es troben a la intranet, a l'espai de protecció de dades de Serveis Jurídics.

L'accés a la informació dels pacients i treballadors, s'ha de fer únicament amb finalitats laborals. Els accessos a informació de pacients i treballadors queden registrats, i en cas que es detecti que s'han realitzat amb finalitats no laborals suposen un incompliment del deure de confidencialitat i poden tenir conseqüències laborals i penals.

6. Notificació d'incidències en matèria de seguretat de dades personals

Amb l'entrada en vigor del nou Reglament qualsevol incidència que afecti a la seguretat de les dades personals s'ha de comunicar en un termini de 72 hores a l'Agencia de Protecció de Dades. Per aquest motiu l'HCB disposa d'un procediment per a la gestió i notificació d'incidències, que es basa en la col·laboració de tots els seus empleats que en cas de detectar una incidència ho a han de comunicar a través de l'adreça protecciodades@clinic.cat.

Entenem per incidència qualsevol anomalia que afecti o pugui afectar a la seguretat de les dades personals, ja siguin de pacients, treballadors o estudiants, tant si estan guardades en suport informàtic com en un suport físic.

7. Drets en matèria de protecció de dades

Tota persona té reconeguts els drets d'accés, rectificació, limitació, supressió, portabilitat i oposició.

Els pacients que vulguin exercir aquests drets s'hauran de dirigir a Atenció al Client, i els treballadors a la Direcció de Recursos Humans. Tanmateix, també disposem de la bústia de correu protecciódades@clinic.cat .

Les condicions d'exercici d'aquests drets es troben recollides en un protocol a la Intranet a l'espai de protecció de dades de Serveis Jurídics.

8. Delegat de Protecció de Dades

El Reglament crea una nova figura d'obligat compliment a l'HCB, el Delegat de Protecció de Dades (DPD), que assumirà competències en coordinació, suport i control del compliment de la normativa de protecció de dades, així com ser el nexe de connexió entre l'HCB i l'Autoritat Catalana de Protecció de Dades.

Podeu contactar amb el DPD a través de l'adreça de correu electrònic protecciodades@clinic.cat.

9. Conseqüències de l' incompliment

El personal de l´Hospital que intervingui en qualsevol fase del tractament de la informació i que incompleixi el descrit en el present document, o si escau en els documents normes o procediments relacionats amb la seguretat i amb la protecció de dades de caràcter personal, haurà de saber que podrà ser sotmès al règim sancionador/disciplinari existent en el centre, tot i això sense perjudici de les possibles conseqüències civils i penals derivades de l' incompliment, si escau.