|  |  |
| --- | --- |
| **Data:** | Setembre de 2018  |
| **Objecte:** | **Procediment ús de recursos externs per a tractar dades de pacients en el marc de les activitats assistencials i de recerca.** |

L’objectiu d’aquest procediment es donar les pautes a seguir quan es vulgui utilitzar un producte o un servei (aplicatiu o app per exemple) d’un tercer per tractar dades de pacients.

En el cas de l’ús del *núvol* o de servidors externs per emmagatzemar dades, s’ha de veure els criteris establerts en el document *FAQ’s de protecció de dades i recerca,* disponible a la Intranet.

# Normativa d’Aplicació

S’ha de tenir en conte Reglament 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 RGPD), així com la normativa interna espanyola vigent en matèria de protecció de dades, i els criteris de seguretat establerts per la DSI de l’Hospital Clínic de Barcelona.

# Procediment

Quan es vulgui utilitzar un producte o un servei ( per exemple una app...) d’un tercer per tractar dades de pacients identificades o codificades s’haurà de seguir el procediment que es descriu en aquest document. S’excepcionarà l’aplicació d’aquest procediment a les dades anonimitzades (implica que s’ha trencat el vincle i no es possible la re identificació del titular de les dades).

*Nota prèvia per a projectes de recerca*

Com a criteris general hem de partir que les dades de pacients utilitzades per projectes de recerca, recollides i emmagatzemades per necessitats metodològiques del projecte degudament justificades, **no han d’aparèixer** en cap moment *el* ***nom i cognoms del pacient****,* ni les ***seves inicials***, ni la ***data de naixement*** (*en format dia, mes i any*), ni el ***codi postal*** de la residència dels pacients. En l’àmbit de la recerca la identificació d’un malalt per relacionar les seves dades s’ha de fer mitjançant un **número seqüencial o aleatori** sense cap mena de significació generat per l’aplicació del promotor (o investigador si és el mateix promotor).

Si per raons del projecte, degudament justificades, cal custodiar la identificació real del pacient i la seva relació amb l’identificador generat per l’aplicació del promotor, es farà sempre **conservant única i exclusivament el numero d’història clínica i el número assignat per l’aplicació del promotor**. El sistema que conservi aquesta relació haurà d’estar **necessàriament custodiat per una única persona que tingui alhora relació contractual amb l’HCB i el centre on es realitza la investigació, i formi part de l’equip investigador** responsable del projecte.

Aquestes dades també han de seguir aquest procediment.

1. En primer lloc el proveïdor del servei/producte haurà de complimentar el formulari Excel que s’adjunta com annex 1. Si el risc que dona és acceptable (verd) es podrà passar al pas 2 d’aquest procediment. Si no el risc no és acceptable (color taronja/vermell) s’haurà de demanar les millores corresponents al proveïdor del servei/producte o buscar un alternativa.
2. Una vegada s’hagi complimentat el formulari Excel indicat en el punt anterior i annex a aquest procediment, i sempre i quan el risc resultant sigui acceptable, el proveïdor haurà de signar la clàusula de protecció de dades que s’indica a continuació:

*“A l'efecte del que es disposa en el Reglament (UE) 2016/679 de 27 d'abril relatiu a la protecció de les persones físiques en relació al tractament de les seves dades personals (d'ara endavant el "Reglament") i la corresponent normativa de desenvolupament, les Parts fan constar que les dades personals contingudes en el present Acord o en els documents previs preparatius del mateix, seran d'ús exclusiu a l'efecte de les recíproques relacions entre les Parts, no se cediran i seran conservats durant el temps que duri aquest Acord. A l'efecte de l'establert en el Reglament les dades de contacte dels Delegats de Protecció de Dades són:*

* *Delegat de Protecció de Dades de l’HCB: protecciodades@clinic.cat.*
* *Delegat de Protecció de Dades de [\*]*

*Les Parts es comprometen a traslladar als titulars de les dades facilitades aquesta informació, així com indicar-los que podran dirigir-se per escrit, identificant la seva identitat, als respectius domicilis assenyalats en l'encapçalament del present contracte per exercitar els seus drets d'accés, rectificació, supressió, oposició, limitació i portabilitat.*

*[\*] es compromet al compliment de les obligacions que en matèria de protecció de dades s'estableixen en el Reglament, en el marc del desenvolupament de l'objecte d'aquest Acord, així com els requisits interns establerts per l’HCB, i que són:*

* *Les dades han de ser emmagatzemades i analitzades en servidors segurs (servidors que no tinguin vulnerabilitats amb un score CVE > 8*[[1]](#endnote-1)*). Serà necessari aportar una certificació de seguretat.*
* *L’accés a les dades emmagatzemades en servidors segurs s’ha de realitzar de manera segura. S’hauran de definir i descriure les mesures de seguretat aplicades a l’accés, detallant qui accedeix a les dades, quan, com i on s’emmagatzemen.*
* *Si la base de dades s’emmagatzema al núvol, (p. ex. Amazon, Google o similars), en un web, o en una app; les dades estaran en tot moment emmagatzemades en “l’Espai Econòmic Europeu” i bè es tindrà un Acord amb el país o l’empresa titular de recurs que segons la normativa de protecció de dades consideri que es un dsetí segur (p.ex Privacy Shield) i estaran seudonimitzades.*
* *No es podran fer usos secundaris a les dades que allà s’hi emmagatzemin, ni a elaborar perfils, ni cedir-les a tercers.*
* *El Sistema Operatiu dels servidors com les aplicacions instal·lades en el servidor han de seguir la política d’actualització de pegats definida per l’HCB i que s’exposa a continuació:*
	+ *Bimensualment, els responsables de les plataformes instal·laran els pegats de seguretat recomanats.*
	+ *Quan un pegat crític o vulnerabilitat (CVE > 8) siguin detectats per part de la DSI de l'HCB o bé pel proveïdor/responsable, aquest pegat o vulnerabilitat haurà de ser instal·lat/corregit en el termini màxim d’una setmana.*
* *El codi desenvolupat per a les aplicacions ha d’utilitzar tècniques d’ofuscament de codi, sobretot en aplicacions mòbils, per a que una descompilació de l’aplicació no doni informació de manera directa d’accessos a APIs de serveis, i per tant a dades del projecte.*
* *Les aplicacions desenvolupades han de seguir metodologies de desenvolupament segures com per exemple OWASP (Open Web Application Security Project, projecte de codi obert dedicat a determinar i combatre les causes que fan que el software sigui insegur).*

*[\*] col·laborarà amb l’HCB a fi que aquest pugui realitzar les verificacions que siguin necessàries per a comprovar el compliment de les mesures de seguretat establertes per la normativa de protecció de dades i per la normativa interna de seguretat de l’HCB, incloent el dret de poder realitzar auditories de seguretat de les aplicacions per a avaluar la seguretat de la plataforma.*

*Cap disposició d’aquest document s’haurà d’interpretar com una cessió o transferència de cap dret de PI pertanyents a l’HCB, en conseqüència, [\*] es compromet a respectar els drets de propietat de l’HCB.*

*En compliment de l'objecte d'aquest Acord [\*] haurà d'accedir a les dades del HCB pel que es constituirà com a encarregat de tractament, i d'acord amb l'establert en el Reglament haurà de signar el contracte d'encarregat de tractament.*

*L’incompliment de qualsevol punt d’aquesta clàusula es considerarà com a un incompliment d’una condició essencial d’aquest acord i donarà dret a l’HCB a resoldre de forma immediata el present acord, sens perjudici de reservar-se el dret a interposar les accions que siguin pertinents per a reclamar els danys i perjudicis que l’actuació de [\*] li hagi pogut ocasionar.”*

Aquesta clàusula s’inclourà en l’acord que hi hagi amb el proveïdor.

Aquest procediment s’entén sens perjudici de la necessitat de signar el contracte d’encarregat de tractament quan ens trobem en un servei que implica l’accés a dades o de l’obligació de seguir els circuits de contractació publica quan així ho demani la legislació vigent.

1. CVE (Common Vulnerabilities and Exposures); així com “score CVE”, que correspondria a CVSS, “Common Vulnerability Scoring System” proporciona un mecanisme per capturar les característiques principals d’una vulnerabilitat i produeix una nota numèrica que reflexa la severitat d’aquesta. La nota numèrica es pot traduir en representacions qualitatives (com pot ser baixa, mitjana, alta, i crítica) per ajudar les organitzacions a avaluar i prioritzar adequadament els seus processos de gestió de vulnerabilitats.” [↑](#endnote-ref-1)