ID document	PC-3-SI-LPD-047000-CA	**Versió**	5.0	
Tipus de document	Procediment	**Procés i Subprocés**	Sistemes d'Informació i Coneixement	Llei Orgànica de Protecció de Dades
Àrees i àmbits d'aplicació	Serveis Informàtics [Àrees consultores]	**Requeriment**	Llei Orgànica de Protecció de Dades	

Bones pràctiques amb les dades de caràcter personal

Resum del contingut *[explicar el propòsit del document (màxim 10 línies)]*

El Protocol de "Bones Pràctiques per a professionals i col·laboradors de l'Institut Guttmann per a la protecció i seguretat de les dades de caràcter personal" té per objectiu garantir l'ús correcte, la confidencialitat i la seguretat de les dades personals i sanitàries relatives als pacients, als membres de l'organització i als que amb aquesta es relacionen.

Elabora o Revisa	Javier Remacha Fuentes **Coautors** [Cadena de Coautors]		
Aprovat per [1] *(Cap d'àrea, unitat...)*	Javier Remacha Fuentes **Òrgan que revisa**	**Data** **Acta**	19/10/2021
Aprovat per [2] *(Comitè de direcció; gerència)* **Validat per** [*]	Montse Caldés Santamaria **Òrgan que aprova**	**Data** **Acta**	15/11/2021
Validat per [*]	[Aprovador de nivell 3]	**Data**	[Data d'aprovació nivell 3]
Vigent fins	15/11/2024		

[1] *Documents aprovats per caps d'àrea, unitat, procés o directament des de la direcció o gerència.*
[2] *Documents prèviament aprovats per altres àrees o processos i que requereixen l'aprovació del comitè de direcció o gerència, si s'escau*
[*] *Documents requerits pels diferents processos externs (JCI; ACH; RSC; AQU; ISO-EMAS; CSUR...) que es validaran per part de l'àrea de qualitat i acreditacions, si s'escau.*

Resum de versions i modificacions

Versions		Autors	Resum de les modificacions més rellevants fetes al document respecte a la versió anterior. Incloure els apartats i pàgines que han estat modificats.
Nº Versió	Data Aprovació		
1.0 (V.O)	2012	Montoliu R.; Vidal C.	
5.0	2019	Vidal C.; Remacha J.	Revisió anual
6.0	2021	Remacha J.	Revisió anual

***Es mantindran, com a mínim, el detall de la primera versió elaborada i les dues versions últimes. Nota important:** La versió ubicada a la intranet és la única versió vàlida i controlada d'aquest document. Qualsevol copia impresa podria no ser la versió final i per tant no incloure les modificacions de la versió en format electrònic.*

Índex

A. PROPÒSIT 4
B. ABAST/ÀMBIT D'APLICACIÓ 4
C. ESTRATÈGIA DE COMUNICACIÓ/DIFUSIÓ 4
D. DESCRIPCIÓ DEL CONTINGUT 5
1. MESURES DE CARÀCTER GENERAL; CONSIDERADES GREUS I MOLT GREUS 5
2. ACCÉS A INTERNET 6
3. MESURES PER A L'ÚS DE LA DOCUMENTACIÓ A LA INTRANET 7
4. MESURES PER AL CORREU ELECTRÒNIC 7
5. MESURES RESPECTE DADES EN SUPORT FÍSIC 8
6. MESURES RESPECTE ALS DISPOSITIUS MÒBILS QUE TINGUIN DADES DE PACIENTS 9
7. MESURES RESPECTE ALS TREBALLS D'INVESTIGACIÓ 9
8. MESURES RESPECTE LES HISTÒRIES CLÍNIQUES 10
9. PERSONAL DE RECEPCIÓ O ADMISSIONS 10
10. ALTRES RECOMANACIONS 10
E. MÈTODE D'AVALUACIÓ 11
F. REFERÈNCIES/BIBLIOGRAFIA 11
G. ALTRES PROTOCOLS/PROCEDIMENTS RELACIONATS 11

Nota important: *aquest format porta incorporat* ***l'índex de paginació automàtic****, recordeu de actualitzar la taula quan acabeu de redactar el document.*

És molt recomanable que en l'elaboració del contingut es segueixin en la mesura que sigui possible els apartats següents com a guia.

A. PROPÒSIT

El deure de confidencialitat es configura, a l'àmbit de la salut, com la prohibició de la revelació de dades de les persones en raó de l'exercici d'activitats sanitàries, ja siguin de prevenció, diagnòstic o tractament.

Aquest és un deure exclusiu de tots els professionals i col·laboradors que formen part de l'Institut Guttmann que puguin tenir coneixement, ja sigui directa o indirectament, de les dades de pacients, membres de l'organització i d'altres persones amb que aquesta es relaciona, en atenció a la feina que duen a terme, ja sigui implicats en el procés assistencial o no assistencial.

És per això que obligatòriament s'han d'implantar determinades mesures de seguretat dels tractaments, automatitzats o no, que continguin aquest tipus dades relatives als pacients, als membres de l'organització o a la resta de persones amb que aquesta es relaciona en l'exercici de la seva activitat.

Aquestes mesures han de ser del nivell més alt que preveu la normativa vigent sobre seguretat dels tractaments automatitzats de protecció de dades de caràcter personal: normativa de seguretat documentada, registre d'incidències, responsable de seguretat, submissió periòdica a auditoria dels sistemes de informació, identificació personalitzada dels usuaris que vulguin accedir al sistema i registre d'accessos. Fins i tot s'ha de restringir l'accés dels usuaris del sistema només a aquelles dades que necessitin tenir coneixement per raó de les seves funcions, diferenciant les assistencials de les administratives.

Amb l'objectiu de garantir la confidencialitat i seguretat de les dades personals a l' Institut Guttmann, i donar compliment als preceptes de la normativa vigent de Protecció de Dades Personals, a continuació es detallen les mesures preventives bàsiques d'obligat compliment per a tots els professionals i col·laboradors de l'Institut Guttmann.

En cas d'incompliment per part del personal s'estarà allò que disposa el Capítol de "Règim disciplinari" del conveni col·lectiu de treball en vigor aplicable i allò que disposa la normativa vigent de Protecció de Dades sobre la tipificació de les infraccions (veure apartat CONSEQÜÈNCIES DE L'INCOMPLIMENT DE LES FUNCIONS I OBLIGACIONS al final del document).

B. ABAST/ÀMBIT D'APLICACIÓ

Tot el personal de la Institució

C. ESTRATÈGIA DE COMUNICACIÓ/DIFUSIÓ

Cursos on line, difusió via revista interna, intranet, recordatoris via email

D. DESCRIPCIÓ DEL CONTINGUT

1. MESURES DE CARÀCTER GENERAL; CONSIDERADES GREUS I MOLT GREUS

1. Les dades personals a les que tenen accés tots els professionals de l'Institut Guttmann només seran utilitzades amb la finalitat de la prestació dels serveis assistencials del centre i per fer possible el normal funcionament de l'organització, garantint el compromís de confidencialitat i ètica professional amb l'única finalitat del desenvolupament de la seva tasca professional ja sigui assistencial o administrativa.
2. Cada usuari amb accés informàtic a les dades dels tractaments, tindrà cura que les dades que es visualitzen per pantalla o que s'imprimeixen no puguin ser visualitzades per persones no autoritzades.
3. Pel que fa als mecanismes de transmissió de la informació únicament s'utilitzaran els que estan descrits al document de seguretat i per tant autoritzats per la institució.
4. Qualsevol transmissió d'informació confidencial, protegida per la llei, haurà de ser comunicada al responsable del tractament perquè quedi registrat.
5. S'ha de garantir que les trameses d'Informes per fax han d'arribar, únicament i exclusiva, a la persona destinatària de l'informe, indicant-ne sempre el contingut confidencial de la tramesa. Aquestes dades confidencials (ja siguin de pacients, professionals, etc...) han de ser dissociades.
6. Quan un col·laborador 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'ordinador.
7. Cada persona és responsable de preservar la confidencialitat de la seva contrasenya i procurar que aquesta no sigui visualitzada per ningú més, deixant sota la seva pròpia responsabilitat l'ús indegut que un altre pugui fer-ne en cas que sigui coneguda de manera fortuïta o fraudulentament. Cada membre de l'organització, professional o col·laborador, haurà de procedir al canvi de la seva contrasenya quan el sistema ho requereixi.
8. Automàticament, es mantindrà el bloqueig de pantalla que s'activarà automàticament i com a norma general cada 10 minuts sense activitat en els departaments administratius. Per als casos de persones que treballen de cara al públic, el bloqueig de pantalla s'activarà automàticament als 5 minuts d'inactivitat. Als ordinadors on es processin dades assistencials, les aplicacions es tancaran automàticament als 3 minuts de no registrar activitat. Els llocs de treball que estiguin de cara al públic, hauran de procurar que el contingut de la pantalla no pugui ser visualitzat per aquelles persones que no siguin usuàries de l'ordinador o del propi departament.

9. Els usuaris que gravin documents en el seu disc dur i hagin de fer còpies de seguretat, per raons estrictament professionals, ho hauran de comunicar al departament d'informàtica.
10. Queda prohibida la presa d'imatges, gravacions en vídeo i/o d'àudio de pacients, acompanyants i d'altres persones a la totalitat del recinte i de les instal·lacions de l'Institut Guttmann, sense contar prèviament i per escrit amb el consentiment de les mateixes. En els casos promoguts o autoritzats per la Direcció de la institució caldrà comptar, sempre i en tots els casos, amb el consentiment previ i per escrit de les persones implicades que siguin alienes a l'organització; caldrà, a més, que l'actuació sigui supervisada per el personal de Comunicacions del centre.
11. Queda prohibida la presa d'imatges, gravacions en vídeo i/o d'àudio de companys, professionals i col·laboradors de l'organització sense previ advertiment i sense comptar amb el seu consentiment.

2. ACCÉS A INTERNET

1. L'Institut Guttmann proporciona als seus professionals l'accés a internet com a eina bàsica per al desenvolupament de la seva tasca professional i com a facilitador de la seva activitat diària. No obstant això, la connexió a Internet a través dels servidors de l'empresa, no es podrà utilitzar amb finalitats il·legals, il·lícites, ofensives, atemptatòries contra la dignitat humana, contra els drets fonamentals, contra la pròpia entitat o altres circumstàncies que puguin ser susceptibles de ser considerades com a delicte.
2. Queda prohibit realitzar debats en temps real (xat), donada l'alta perillositat que suposa pel sistema la instal·lació del programari que permet els accessos no autoritzats al sistema informàtic. Seran excepcions les eines per fer telerehabilitació, teletreball, reunions per videoconferència, l'assistència tècnica o qualsevol altre activitat que hagi estat prèviament autoritzada pel propi departament d'informàtica.
3. Queda totalment prohibit utilitzar programes tipus P2P (Emule, Limewire, Azureus, Bit Torrent, etc.). Aquest tipus de programes comparteixen carpetes de l'ordinador local amb milions d'usuaris i són una amenaça molt seriosa per la seguretat de les dades.
4. Queda totalment restringit l'ús de les xarxes socials a aquelles finalitats exclusivament professionals per les quals la persona hagi estat prèviament autoritzada i sempre limitada a l'activitat que li està encomanada a l'organització.
5. L'Institut Guttmann enregistra automàticament tota la informació de les connexions als servidors de l'empresa. En aquest sentit, la institució podrà accedir a les dades de connexió a Internet dels empleats emmagatzemades en els nostres servidors en temps real. L'Institut Guttmann es reserva, preservant les garanties legals pertinents, la facultat de fer revisions periòdiques dels registres de connexió a internet, tant pel que fa al contingut com al temps emprat, podent ser motiu de sanció aquelles actuacions

incorrectes recollides al punt 1.10, o les que representin un ús abusiu, privat i indegut d'aquesta eina en hores de treball.

6. Queda prohibit introduir, descarregar d'Internet, reproduir, utilitzar o distribuir programes informàtics no autoritzats per part de la Institució 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. En tot cas, per a qualsevol actuació respecte a l'anterior supòsit, serà requisit indispensable l'autorització expressa del responsable de seguretat de l'Àrea d'Informàtica.
7. Quan el sistema avisi d'algun problema relacionat amb un virus, s'haurà d'avisar immediatament al departament d'informàtica.

3. MESURES PER A L'ÚS DE LA DOCUMENTACIÓ A LA INTRANET

1. Tots els documents i/o informació allotjada a la intranet són d'ús únicament professional i pertanyents a l'organització, qui comparteix la propietat intel·lectual amb l'autor del mateix. Els documents d'accés obert per a tota la comunitat d'usuaris a la intranet es troben al seu abast per al seu ús estrictament professional relacionat amb la seva activitat a l'Institut Guttmann. Sempre que es facin servir fora de l'àmbit estrictament de l'organització s'haurà de fer constar de manera fefaent el nom de la institució com a font de procedència. Considerant el caràcter sensible i confidencial d'aquesta informació, no està permès l'ús inadequat o incorrecte de la mateixa d'acord amb el que queda establert en aquest document.
2. Els documents d'accés restringit, en cap cas poden ser fets servir fora de la institució sense l'autorització expressa de la Direcció, i requeriran la signatura d'acords de confidencialitat entre l'Institut Guttmann i l'entitat receptora (persones amb representació legal de cadascuna de les entitats signants).

4. MESURES PER AL CORREU ELECTRÒNIC

1. L'Institut Guttmann proporciona a cada un dels seus professionals una adreça individual de correu electrònic. Aquest és un instrument bàsic per a la prestació dels serveis professionals i una eina de millora de l'activitat diària de l'organització en el seu conjunt. El correu electrònic és propietat de l'Institut Guttmann, i com a tal, haurà de ser utilitzat fonamentalment amb finalitats professionals.
2. El correu electrònic que es posa a disposició dels membres de l'organització, professionals i col·laboradors, a través del servidor d'empresa, no es podrà utilitzar en cap cas, per a enviar missatges il·legals, il·lícits, ofensius, atemptatoris contra la dignitat humana, contra els drets fonamentals, contra la pròpia entitat o altres circumstàncies que siguin susceptibles de ser considerades com a delicte.

3. El correu electrònic és d'ús exclusivament personal i cap altre usuari del sistema informàtic de l'Institut Guttmann podrà suplantar la identitat d'una altre persona a l'hora de fer-ne ús.
4. En el moment de l'extinció de la relació contractual, s'interromprà l'accés a la bústia de correu professional que s'hagi posat a disposició del professional o col·laborador, i els serveis tècnics procediran a esborrar íntegrament el seu contingut.
5. Els correus electrònics queden tots automàticament registrats i emmagatzemats al servidor propietat de l'Institut Guttmann durant un any, i queden sotmesos, en el cas que així es considerés necessari, a la seva supervisió i/o auditoria sempre amb la preservació de les garanties legals pertinents (per instruir expedients interns de l'organització o donar resposta a requeriments legals, policials, judicials...)
6. Queda prohibit enviar dades confidencials dels pacients als quals tinguem accés per motius estrictament professionals per correu electrònic ja que és un medi que no garanteix la confidencialitat. Només es podrà fer ús d'aquest mitjà quan les dades s'enviïn xifrades, dissociades i als destinataris autoritzats. També queda prohibit enviar dades confidencials dels pacients a través de smartphones a no ser que s'enviïn amb l'aplicació Medxat.
7. No està permès obrir els missatges de remitents desconeguts, sobretot si en l'apartat "assumpte" no apareix cap indici que es pugui relacionar amb la nostre activitat professional.

5. MESURES RESPECTE DADES EN SUPORT FÍSIC

1. S'haurà de garantir el destí últim del paper inservible o duplicat (mai originals de documentació que integri la Història Clínica o Documentació Clínica) mitjançant la seva destrucció a través del destructor de paper. Aquesta mesura és necessària per garantir la confidencialitat i per evitar que existeixi el risc d'accés per part de personal no autoritzat. En tant no es destrueixi, aquesta documentació és responsabilitat tant de l' autor del document com de la persona responsable del contenidor de paper en que s'hi trobi.
2. En cas de voler destruir qualsevol document que contingui informació o dades confidencials s'ha de fer necessàriament mitjançant el circuit descrit en el document "Annex 17: Sistema de seguretat informàtic i pla de contingències. Apartat 'Destrucció de discs i papers i protecció de dades".
3. Els suports informàtics que tinguin dades personals, (per exemple: dades de nòmines per les entitats financeres, dades de declaracions tributàries per Hisenda, imatges radiogràfiques, etc.) hauran d'estar clarament identificats amb una etiqueta externa que informi de les dades contingudes i la data en que es van guardar en el suport informàtic.

4. Els suports informàtics, tinguin o no dades confidencials, hauran de ser examinats per un antivirus abans d'introduir-los al nostre sistema informàtic.
5. Tots els suports amb la informació de pacients que surtin del centre s'hauran d'anotar al registre d'entrades i sortides de suports tal com s'indica al document de seguretat.

6. MESURES RESPECTE ALS DISPOSITIUS MÒBILS QUE TINGUIN DADES DE PACIENTS

1. Sempre que es faci ús d'un portàtil aliè per fer una presentació o alguna altra feina relacionada o que apareguin dades de pacients, haurem d'esborrar automàticament les dades que haguéssim pogut gravar per efectuar aquest treball.
2. Qualsevol dada de pacient que estigui en un dispositiu mòbil (portàtil, memòria USB, CD/DVD, disc dur gravable, tabletes, etc.) haurà d'estar xifrada o dissociada.
3. És recomanable que els portàtils tinguin una clau d'accés a l'arrancar, a més del xifrat dels arxius que continguin dades sensibles.

7. MESURES RESPECTE ALS TREBALLS D'INVESTIGACIÓ

1. Només es poden utilitzar les dades de salut de les Històries Clíniques dels pacients de manera anònima, dissociada i/o amb un codi propi de l'investigador que estigui realitzant el projecte de manera que no es pugui vincular mai la identitat del pacient amb la dada mèdica corresponent. La participació d'altres organitzacions o professionals en projectes o treballs col·laboratius permetrà el seu accés al tractament d'aquestes dades un cop signat els pertanyents acords de confidencialitat. En cap cas, es considera aquesta participació i aquest accés com una cessió de les dades i els col·laboradors no podran fer ús de les mateixes fora del marc del projecte o treball en qüestió.
2. Només serà possible utilitzar dades identificades o identificables si es compta amb el consentiment exprés de l'usuari al qui pertanyen aquestes dades.
3. L'autorització expressa per tractar les dades amb finalitats de recerca no implica que s'autoritzi la cessió de les dades de caràcter personal dels participants a tercers; excepcionalitat que també hauria de ser especialment autoritzada per l'usuari.
4. El tractament i la cessió de les dades, identificables o identificades, de pacients comptant amb la seva autorització no pressuposen la possibilitat de crear tractaments de dades específics; per fer-ho, cal la corresponent legalització d'aquests tractaments, cosa que correspon a l'Institut Guttmann i sempre que es comuniqui prèviament a la persona responsable de seguretat del Departament d'Informàtica.
5. No està permès sol·licitar cap mena de consentiment a l'usuari (per tractar o cedir dades en relació a activitats de recerca) sense el coneixement i autorització de l'Institut Guttmann, així com generar cap tractament amb aquestes dades.

8. MESURES RESPECTE LES HISTÒRIES CLÍNIQUES

1. Els arxius on estiguin ubicades les Històries Clíniques han d'estar tancats sota clau. Caldrà tenir cura de la clau, no fer-ne còpia sense autorització expressa ni deixar-la a cap lloc accessible a persones no autoritzades. (Veure Manual de la Història Clínica Electrònica HCE).
2. Tots els membres de l'organització, professionals i col·laboradors, que necessitin consultar les Històries Clíniques en suport paper, hauran d'indicar el seu accés al registre d'entrades i sortides de les Històries Clíniques de l'arxiu corresponent i amb els mecanismes que l'entitat indica en el document de seguretat.
3. Durant el període en el que la Història Clínica es trobi fora de l'arxiu central, tot el personal ha de vetllar per evitar qualsevol accés per part de persones no autoritzades.
4. La devolució de les Històries Clíniques a l'arxiu ha de realitzar-se immediatament després de la circumstància que va motivar la seva petició.
5. Està absolutament prohibit treure cap Història Clínica fora del centre sense autorització expressa del responsable del tractament.

9. PERSONAL DE RECEPCIÓ O ADMISSIONS

1. El personal d'Admissions ha d'informar els pacients, sobre l'existència d'un tractament o tractaments on s'introduiran les seves dades personals, la finalitat de la recollida de les dades i els destinataris de la informació, i farà signar al pacient el "Full d'Informació i Consentiment".
2. Queda expressament prohibida la difusió de dades, sense autorització expressa del pacient o representant.

10. ALTRES RECOMANACIONS

1. Es recomana facilitar qualsevol tipus d'informació al pacient i/o persones vinculades en un lloc discret i reservat.
2. Es recomana no tenir llistats de pacients, informes o qualsevol altre tipus de documentació a la vista del públic o altra persona aliena a l'organització.
3. En abandonar per un temps limitat el lloc de treball, es recomana evitar l'exposició de documents confidencials a la vista d'altres persones. En cas que el document no es pugui arxivar, es recomana, com a mínim, mantenir-lo en un lloc ocult o privat.
4. En acabar la jornada laboral cap document confidencial haurà de quedar sobre la taula, a la vista o a accés indegut de qualsevol persona, sota responsabilitat personal de les accions que se'n poguessin derivar.

5. No comentar informació sobre els pacients en llocs de concurrència (passadissos, ascensor, cafeteria, etc.) ja sigui en presència de públic en general o qualsevol altre personal de l'hospital.
6. No està permès donar mai cap mena d'informació telefònica que afecti a les dades confidencials del pacient.

CONSEQÜÈNCIES DE L'INCOMPLIMENT DE LES FUNCIONS I OBLIGACIONS

Definides i tipificades als articles 83 i 84 del Reglament Gral. de Protecció de Dades (679/2016).

La incorporació a la dinàmica de l'empresa dels principis rectors de la Protecció de Dades de Caràcter Personal, adquireix una gran importància des del moment en què les conseqüències del seu incompliment comporten grans responsabilitats tant per l'Organització com per al personal que tracta o accedeix a les dades de caràcter personal, és a dir, les sancions ja no només són administratives i dirigides a l'Organització en si, sinó que a més d'elles es poden derivar responsabilitats civils, penals i laborals.

E. MÈTODE D'AVALUACIÓ

Curs d'obligat compliment On Line. Anual.

F. REFERÈNCIES/BIBLIOGRAFIA

- Autoritat Catalana de Protecció de dades
- Agencia Española de Protección de Datos
- Reglament General de Proteccio de Dades
- I 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 la Salut

G. ALTRES PROTOCOLS/PROCEDIMENTS RELACIONATS

Documentació del Sistema de Gestió de la Protecció de Dades.