Amb l'objectiu de garantir la confidencialitat i seguretat de les dades personals de l'Entitat, i donar compliment a la normativa vigent en matèria de protecció de dades personals i garantia de drets digitals, l'Entitat estableix les mesures preventives següents, que ha de complir tot el personal contractat o col·laborador.

**MESURES INFORMÀTIQUES:**

1. Les dades personals a què té accés el personal i col·laboradors només seran utilitzades per a les activitats d'investigació i docència inherents a la finalitat de FIDMAG Germanes Hospitalàries, garantint el compromís de confidencialitat i ètica professional.

2. Cada usuari amb accés informàtic a les activitats de tractament, 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. Pel que fa als mecanismes de transmissió de la informació únicament s'utilitzaren els que estan descrits al Document de Seguretat i per tant autoritzats per l'entitat.

3. És totalment prohibit fer enviaments de dades de nivell alt per FAX.

4. Quan un empleat o 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.

5. Cada usuari 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.

6. Cada usuari 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 i registrar-ho com incidència i procedir al seu canvi.

7. Cada treballador/col·laborador haurà de procedir al canvi del seu *password* quan el sistema així ho requereixi. Així mateix, es mantindrà el bloqueig de pantalla que s'activarà automàticament i com a norma general cada 10 minuts sense activitat.

8. Quan l'usuari d'un lloc de treball l'abandoni temporalment caldrà que activi manualment el protector de pantalla (Ctrl + Alt + Supr). La tornada al seu lloc de treball implicarà la desactivació de la pantalla protectora amb la introducció del corresponent *password*.

9. Qualsevol modificació en els sistemes d'informació (SI), i en concret a la informació inventariada als documents de seguretat, s'haurà de comunicar al responsable de seguretat scalvet@fidmag.com i al delegat de protecció de dades dpd@fidmag.com

**MESURES RESPECTE L'ÚS DEL CORREU ELECTRÒNIC**

10. El personal al servei de FIDMAG Germanes Hospitalàries ha de fer un bon ús del correu electrònic que li ha estat atribuït per a l'exercici de les seves funcions. Cada persona treballadora que té un compte de

correu assignat es configura com a persona usuària d'aquests sistemes i és responsable d'aquests recursos que té assignats i de totes les accions que es duguin a terme en la seva utilització.

11. En supòsits d'enviament de dades de nivell alt a través de correu electrònic serà requerida la prèvia dissociació de dades identificatives de l'afectat i si no es pogués dissociar es disposa de sistemes de xifratge en la mesura que esdevindria una situació excepcional. Donat que el correu electrònic ens permet encriptar les dades, es podrà fer ús d'aquest mitjà quan així es requereixi i sempre que el metge responsable del pacient ho sol·liciti, utilitzant el programari específic per aquesta tasca definit en el Document de Seguretat de la Entitat.

**ACCÉS A INTERNET:**

12. L'accés a Internet es limitarà als temes directament relacionats amb l'activitat que presta l'Entitat i amb el lloc de treball de l'usuari.

13. Queda prohibit realitzar debats en temps real (Chat/IRC), donada l'alta perillositat que suposa pel sistema la instal·lació del programari que permet els accessos no autoritzats al sistema informàtic.

14. 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 l'usuari.

15. 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.

16. En tot cas, per a qualsevol actuació respecte als anteriors supòsits serà requisit indispensable l'autorització expressa del Delegat de Protecció de Dades.

**MESURES RESPECTE DADES EN SUPORT FÍSIC:**

17. S'haurà de garantir el destí últim del paper inservible o duplicat 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.

18. Els suports informàtics que tinguin dades personals, (per exemple: dades de nòmines per les entitats financeres, dades de declaracions tributàries per Hisenda en disquets o CD) 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.

19. Tots els suports amb dades de nivell mitjà/alt que surtin del centre s'hauran d'anotar al Registre d'entrades i sortides de Suports tal com s'indica al document de seguretat.

**MESURES RESPECTE LES HISTÒRIES CLÍNIQUES:**

20. 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 en cap lloc accessible per persones no autoritzades.

21. Cada empleat/col·laborador amb accés a les Històries Clíniques en suport paper haurà d'indicar al registre d'entrades i sortides (informàtic o paper) de les Històries Clíniques de l'arxiu amb els mecanismes que l'entitat li ha indicat en el Document de Seguretat.

22. Durant el període en que la Història Clínica es troba fora de l'arxiu central, tot el personal ha de vetllar per evitar qualsevol accés per part de persones no autoritzades.

23. La devolució de les Històries Clíniques a l'arxiu ha de realitzar-se immediatament després de la circumstància que va motivar la seva petició.

24. Està absolutament prohibit treure la Història Clínica fora del centre sense autorització expressa del Responsable de Tractament.

25. Si es detecten accessos no autoritzats a les històries clíniques o un mal ús de les dades a que tenen accés els treballadors/col·laboradors de FIDMAG Germanes Hospitalàries, sempre serà necessària la presència de l'afectat per justificar o no el que en principi és un accés no autoritzat o incompliment del règim intern de la seguretat de la informació. Amb tot, si l'accés esdevé com no autoritzat o una violació de la normativa de protecció de dades de l'entitat, FIDMAG Germanes Hospitalàries podrà adoptar les mesures disciplinàries convenients d'acord amb allò que estableixi el conveni laboral d'aplicació i en funció de les circumstàncies concurrents a cada cas. El Conveni de la SISCAT preveu diversos "tipus" infractors que permetrien qualificar les conductes relacionades com a infracció lleu, menys greu, greu i molt greu.

**RESPECTE L'ÚS DE L'USB:**

Els ports per els dispositius USB es troben tancats. 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:

26. 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.

27. Els dispositius USB que tinguin dades personals confidencials hauran d'estar clarament identificats, a través d'un codi per exemple, amb el qual es pugui saber quines són les dades contingudes en el mateix i la data en que van ésser guardades. Els criteris d'identificació de la informació que contenen han de impedir la identificació per al personal no autoritzat.

28. En el cas que resulti necessari emprar aquest tipus de suports, el Responsable de Tractament donarà instruccions al Responsable de l'Àrea corresponent de l'Entitat per a què sigui l'encarregat d'autoritzar la idoneïtat del seu ús. Així mateix es designarà un responsable per a cada cas encarregat de controlar les entrades i sortides dels mateixos.

29. El Document de Seguretat ha de preveure el personal autoritzat a accedir a aquests tipus de suports.

30. Aquests moviments d'USB's hauran de quedar anotats al Registre d'entrades i sortides de suports. En tot cas, les entrades i sortides que s'hagin de fer hauran de deixar constància al document de seguretat.

31. Els dispositius d'emmagatzematge dels suports que continguin dades de caràcter personal hauran de disposar de mecanismes que obstaculitzin la seva obertura. Quan les característiques físiques no permetin adoptar aquesta mesura, el Responsable de Tractament adoptarà mesures que impedeixin l'accés de persones no autoritzades.

32. De la mateixa manera, s'hauran de xifrar les dades que continguin els dispositius portàtils, mitjançant una contrasenya, quan aquests es trobin fora de les instal·lacions que estan sota el control del Responsable de Tractament.

33. 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.

**RESPECTE L'ÚS DE TABLETS I DE TELÈFONS MÒBIL AMB ACCÉS A INTERNET**

34. Únicament el personal autoritzat podrà tenir aquests dispositius. L'entitat disposa de registre.

35. 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.

36. En el cas que resulti necessari emprar aquest tipus de suports, el Responsable de Tractament donarà instruccions al Responsable de l'Àrea corresponent de l'Entitat per a què sigui l'encarregat d'autoritzar la idoneïtat del seu ús.

37. El Document de Seguretat ha de preveure el personal autoritzat a accedir a aquests tipus de suports.

38. Aquests suports hauran de disposar de contrasenya o codi d'accés.

39. Cal evitar la descàrrega de documents que continguin dades de caràcter personal en aquests suports. Pel cas que resultés necessari fer la descàrrega, un cop realitzada i finalitzada la necessitat que la motivà caldrà procedir a eliminar les dades de caràcter personal del dispositiu.

40. 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.

**RESPECTE L'ÚS DEL MATERIAL**

41. Tot treballador, ja sigui personal intern contractat, així com personal col·laborador extern com estudiants en pràctiques, especialistes en formació en el període de rotació, becaris, adscrits a altres Institucions, personal d'altres centres de Germanes Hospitalàries, o d'altres, que en compliment de les funcions que té atribuïdes tingui que realitzar una sortida de documents, ja sigui en suport manual o automatitzat, haurà de ser registrada en el Registre d'entrada i sortida de FIDMAG Germanes Hospitalàries, i ser autoritzada de forma expressa pel Delegat de Protecció de Dades d'acord amb el compliment de les mesures de seguretat estipulades en el Document de Seguretat de FIDMAG Germanes Hospitalàries, entre elles el xifratge del suport portàtil si parlem de memòries USB o dispositius portàtils, i si és en paper, prenent les mesures de seguretat que evitin la sostracció, pèrdua o accés indegut.

42. El responsable de la sortida queda igualment compromès al retorn obligat de la documentació, un cop finalitzat el motiu que provoca la sortida.

**Davant l'incompliment de les funcions i obligacions que corresponen als usuaris, en matèria de protecció de dades de caràcter personal i garantia de drets digitals, resultaran d'aplicació les conseqüències previstes al Conveni Laboral aplicable per a l'incompliment de les obligacions laborals.**

En Barcelona, __ de ____ de 20__

Recibí,

**NOM: _____**
**DNI: _____**