Amb l'objectiu de garantir la confidencialitat i seguretat de les dades personals de l'**Entitat**, i donar compliment als preceptes de la Llei Orgànica 15/1999 de Protecció de Dades Personals, l'entitat estableix les mesures preventives següents que ha de complir tot el personal contractat o col·laborador. En el supòsit que s'incompleixi la normativa en protecció de dades, l'entitat prendrà les mesures corresponents a nivell laboral.

MESURES INFORMÀTIQUES:

1. Les dades personals a les que té accés el personal i col·laboradors només seran utilitzades amb la finalitat de la prestació dels serveis assistencials del centre, garantint el compromís de confidencialitat i ètica professional.
2. Cada usuari amb accés informàtic a les dades dels fitxers, 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. No està permès enviar dades personals de nivell alt per FAX.
4. En el cas de que s'hagin d'enviar e-mails amb dades personals de nivell alt, primer s'ha de comprovar que la comunicació està autoritzada per l'entitat i en cas de ser així l'enviament ha de ser xifrat (encriptat).
5. En el cas de d'enviament per missatgeria de seguretat també s'ha de comprovar que la sortida sigui autoritzada.
6. 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.
7. 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.
8. 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.

9. 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 5 minuts sense activitat. Per als casos de persones que treballen de cara al públic, el bloqueig de pantalla s'activarà automàticament als 2 minuts d'inactivitat. Ambdós casos el sistema sol·licitarà password per poder reactivar el bloqueig.

10. Quan l'usuari d'un lloc de treball l'abandoni temporalment caldrà que activi manualment el protector de pantalla. La tornada al seu lloc de treball implicarà la desactivació de la pantalla protectora amb la introducció del corresponent password.

11. En cas que es generi qualsevol tipus de fitxer temporal que contingui dades de caràcter personal es destruirà up cop deixi de ser necessari per la finalitat que va motivar la seva creació. Aquest fitxer en cap cas es podrà guardar en carpeta local.

ACCÉS A INTERNET:

12. L'accés a Internet es limitarà als temes directament relacionats amb l'activitat sanitària 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 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 de l'**Entitat**.

MESURES RESPECTE DADES EN SUPORT FÍSIC:

17. 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 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, CD o USB) 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. Aquest tipus de dispositius (CD o USB) 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.

19. Quan un suport informàtic hagi de ser rebutjat o reutilitzat se entregarà al departament d' Informàtica per la seva gestió.

20. Tots els suports amb dades de nivell mig o 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:

21. Els arxius on estiguin ubicades les Històries Clíniques han d'estar tancats sota clau. Caldrà tenir cura de la clau, no fer còpia sense autorització expressa ni deixar·la en cap lloc accessible per persones no autoritzades.

22. 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.

23. 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.

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

25. Esta absolutament prohibit treure la Història Clínica fora del centre sense autorització expressa del Responsable del Fitxer.

TRACTAMENT D'INCIDÈNCIES

26. En el moment que qualsevol treballador detecti una incidència que afecti a la seguretat de les dades haurà d'informar al seu superior immediat, que a la seva vegada donarà trasllat al departament d'administració.

PERSONAL DE RECEPCIÓ O ADMISSIONS:

27. El personal de recepció ha d'informar als pacients, sobre l'existència d'un fitxer o fitxers 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".

28. Queda expressament prohibida la difusió de dades, sense autorització expressa del pacient o representant. D'això es deriva certs criteris en el moment de resposta a preguntes telefòniques com presencials:

- **preguntes per <u>telèfon</u> i actitud a prendre:**

  a) si pregunten per una malalt ingressat (dins dels horaris establerts de comunicació telefònica):

  - Informar als pacients sobre la pràctica del centre de passar trucades a l'habitació. En el cas de que el pacient es negui es recollirà per escrit i es respectarà el seu dret a la confidencialitat sobre el seu ingrés i el seu estat de salut.

  b) si s'estan realitzant enquestes de satisfacció o algun altre tipus d'estudi:

  - Sempre demanarem per la persona en concret, sense identificar que es truca des de l'Hospital. No es donarà cap més informació a altres persones (familiars , amics, etc.).

  -

- **preguntes en <u>presència física</u> i actitud a prendre:**

  c) si el pacient es troba ingressat a l'Hospital es pot donar la sala i el llit o urgències, però en cap cas serà facilitada informació d'on es troba el servei de psiquiatria o toxicomanies. Respostes a donar:

  - no es té aquesta dada a recepció
  - que es pregunti a la família

- que acudeixin al SAU en cas d'insistència o situació excepcional (policia, autoritat judicial, etc.).

d) si quan s'observa a la pantalla el malalt per qui es pregunta a estat "exitus":

- no disposem d'aquesta informació i que es posi en contacte amb la família
- derivar-lo al SAU
- en cas excepcional o de forta angoixa, trucar als serveis funeraris del recinte, amb la màxima discreció, per a informar que s'envia a la persona a preguntar.

e) Si l'usuari per qui es pregunta no apareix al registre:

- en cap cas es farà recerca a través de cognoms aproximats, que no suposin el canvi d'una consonant per a una altra amb igual o semblant fonètica.
- que no es té aquesta dada a recepció.

Si la pregunta es realitza a la nit o matinada (en presència física o per telèfon) i no es refereix a urgències, la resposta i orientació a donar és que aquest tipus d'informació es dona a hores diürnes, d'acord amb les hores de visita dels malalts.

XXXXXX, a .....de ..... de 201

Treballador/Col·laborador

(signatura)