Preguntes freqüents

Índex de continguts

Ús dels recursos informàtics....2
Mesures de seguretat....8
Confidencialitat....13
Qualitat de les dades....16
Consentiment....18
Cessió o comunicació de dades....20
Exercici de drets de protecció de dades....25
Accés i conservació d'històries clíniques....30
Organització de la seguretat....36
Dret a la pròpia imatge i enregistraments....37
Altres preguntes....41

Ús dels recursos informàtics

1) Puc accedir a internet des del meu dispositiu mòbil per fer-ne un ús personal fora de l'acompliment de les funcions que són pròpies del meu lloc de feina?

Aquesta pràctica és contrària al Codi de bones pràctiques, que estableix que els recursos informàtics del Servei de Salut han de ser emprats per a les tasques pròpies del personal d'acord amb les funcions que té assignades, tret que tengui autorització.

D'altra banda, d'acord amb el criteri de l'Audiència Nacional, aquest accés a internet no es pot considerar en règim d'autoprestació, atès el caràcter restrictiu de la interpretació que se n'ha de fer de conformitat amb la SAN 3886/2011, de 1r de setembre; per tant, és obligatori complir les mateixes obligacions que la resta dels operadors de xarxes i serveis de comunicacions electròniques; entre d'altres, les següents:

- Obligació d'inscripció registral en el registre d'operadors de la Comissió del Mercat de les Telecomunicacions.
- Garantia del secret de les comunicacions adoptant les mesures necessàries.
- Garantia dels nivells de protecció de les dades de caràcter personal mentre exerceix les seves funcions.
- Deure de conservació de dades relatives a les comunicacions electròniques i a les xarxes públiques de comunicacions.

2) Es poden emprar el correu electrònic i l'agenda corporativa per enviar correus massius, cadenes de missatges, etc.?

El Codi de bones pràctiques estableix que el Servei de Salut posa a la disposició del personal l'accés a determinats recursos informàtics amb la finalitat de facilitar el desenvolupament del seu treball. Així mateix, recorda que els recursos en qualsevol cas són propietat del Servei de Salut i, com a tals, han de ser utilitzats per a les labors pròpies del personal d'acord amb les funcions que té assignades.

D'altra banda, respecte a l'ús del correu electrònic i les agendes, el Codi de bones pràctiques determina que el correu electrònic i l'agenda proporcionats pel Servei de Salut són per fer-ne un ús professional, com a eines de feina que són. És necessari tenir l'autorització corresponent per a qualsevol ús particular, que ha de ser puntual i limitat en freqüència i durada. En cap cas l'ús autoritzat per a finalitats personals pot consistir en una activitat comercial o amb ànim de lucre ni pot ser inadequat o ofensiu.

Igualment, quant a l'ús del correu electrònic i l'agenda, el Codi de bones pràctiques determina expressament que el correu electrònic és un mitjà de comunicació interpersonal, no un mitjà de difusió massiva i indiscriminada d'informació. Per això, cal evitar qualsevol pràctica que pugui posar en risc el funcionament i el bon ús del sistema.

Així mateix, es considera expressament un ús inadequat del servei de correu electrònic i l'agenda el fet que s'emprin com a mitjà per propagar cartes encadenades o participar en esquemes piramidals o activitats similars, o per enviar missatges o informació de manera massiva, la qual cosa consumeix injustificadament recursos tecnològics.

Per tot això, no està permès emprar l'agenda ni el correu corporatius per difondre missatges amb aquestes finalitats.

3) Es poden emprar solucions d'emmagatzematge ofertes per serveis com DropBox, Mega i Google Drive?

Amb caràcter general, el Codi de bones pràctiques estableix que s'ha d'evitar emprar, instal·lar o distribuir programes fora dels estàndards i les recomanacions aprovats pel Servei de Salut, perquè poden comprometre la seguretat dels sistemes d'informació.

En particular, aquest tipus de solucions d'emmagatzematge no permeten aplicar les mesures de seguretat requerides per garantir la protecció de les dades ni complir les obligacions relatives a la comunicació de dades que requereixin el consentiment previ de la persona afectada.

Per això, l'Oficina de Seguretat no autoritza l'ús d'aquests serveis en l'àmbit professional perquè no ofereix garanties suficients de seguretat per al tractament de dades de caràcter personal, en particular les de nivell alt, protegides especialment.

4) Es pot emprar SharePoint com a repositori de documentació clínica?

Segons la LOPDGDD, el Servei de Salut té l'obligació d'implementar les mesures de seguretat establertes en l'ENS. Però SharePoint no té actualment les mesures de seguretat necessàries per garantir el nivell de seguretat requerit per al tractament de documentació clínica, perquè aquesta recull categories especials de dades. Per això, l'Oficina de Seguretat proposa aplicar determinats criteris per determinar si es pot utilitzar SharePoint per a determinades finalitats, en funció del tractament i la categorització de les dades.

S'entén per *categories especials de dades* les relatives a dades personals que revelin l'origen ètnic, les opinions polítiques, les conviccions religioses o filosòfiques, l'afiliació sindical, les dades genètiques i biomètrics dirigides a identificar de manera unívoca una persona física, les dades relatives a la salut i les dades relatives a la vida sexual o l'orientació sexual d'una persona física. Si les dades que s'han de tractar entren en aquesta definició, es recomana no emprar SharePoint per tractar-los.

5) Quines mesures s'han d'assegurar per enviar dades clíniques per mitjà del correu?

Segons la LOPDGDD, el Servei de Salut té l'obligació d'implementar les mesures de seguretat establertes en l'ENS per protegir els actius. Quant a la informació que contenguin tant el cos dels missatges dels correus electrònics com els arxius adjunts, ha d'estar protegida en totes les seves categories, independentment de quina sigui la dimensió de seguretat. Per això, el Codi de bones pràctiques estableix que, amb caràcter general, cal evitar enviar per correu electrònic informació que contengui dades personals de salut i que, si és estrictament necessari, han d'estar xifrades.

Segons el criteri tècnic de la Subdirecció General d'Inspecció de l'AEPD, manifestat en l'Informe 0494/2009, [traducció de l'original] «tant el xifrat que ofereixen els productes que generen arxius PDF o el realitzat per WinZip tenen vulnerabilitats conegudes i es disposa d'eines de lliure distribució que aprofiten aquestes vulnerabilitats. Més concretament, no només es poden obtenir en internet fàcilment utilitats que trenquen les proteccions dels arxius PDF o ZIP, sinó que el mateix algorisme en què descansa la xifra de documents PDF, l'algorisme RC4, és manifestament vulnerable. Tot i que per a l'ús particular es poguessin considerar

adequades, no és així per a l'intercanvi d'informació amb les garanties que es precisen en el Reglament». L'Informe afegeix que [traducció de l'original] «aquesta garantia necessària per preservar la confidencialitat de les comunicacions no només descansa en el sistema de xifrat, sinó també en el sistema de gestió de claus, en particular».

Per aquests motius és preceptiu que l'intercanvi d'informació es dugui a terme fent servir certificats electrònics, de manera que sigui possible protegir la seguretat de la comunicació amb mecanismes de xifrat de clau pública basats en l'ús d'un parell de claus que permetin xifrar el contingut amb una d'aquestes —que queda en poder del propietari— i desxifrar el contingut amb l'altra i només amb aquesta.

6) **Si un organisme (p. ex. un jutjat) sol·licita dades de categories especials d'un usuari del centre (dades de salut, etc.) per un mitjà de comunicació que es pot considerar insegur (fax, correu electrònic sense xifrar), s'ha de cursar-la sol·licitud?**

Des de la perspectiva de la protecció de les dades, no s'ha d'emprar el fax per enviar documentació que contengui dades de categories especials. Per això, cal informar l'organisme sol·licitant que per enviar-la hi ha actualment altres vies, senzilles, igual de ràpides i més segures (correu electrònic xifrat).

7) **Està permès emprar usuaris genèrics per accedir als sistemes d'informació?**

Segons la LOPDGDD, el Servei de Salut té l'obligació d'implementar les mesures de seguretat establertes en l'ENS per protegir l'operació del sistema, una de les quals és el control d'accessos, que cobreix el conjunt d'activitats preparatòries i executives perquè una entitat determinada (usuari o procés) pugui (o no) accedir a un recurs del sistema. Quant a la identificació, s'estableix que cada entitat que accedeixi a un sistema ha de tenir un identificador singular i ha d'estar associada a un identificador únic. En aquest sentit, no s'admet crear usuaris genèrics, doncs cada usuari s'ha d'identificar de manera inequívoca i personalitzada.

8) **En els llocs de guàrdia o en aquells on es facin proves mèdiques, es faci feina per torns o hi hagi equips en funcionament les 24 hores del dia per necessitats del servei, és possible compartir l'usuari del sistema d'informació per evitar sortir i entrar del sistema?**

No es pot compartir l'usuari ni desvetlar la clau d'accés associada a cap empleat, company o una altra persona. Tampoc s'han d'emprar usuaris genèrics compartits. Per tant, cada empleat ha d'iniciar la sessió amb el seu usuari quan comença la seva jornada i tancar-la en acabar.

9) **Es pot instal·lar iTunes, Spotify o qualsevol altre sistema no corporatiu en els equips de feina del Servei de Salut?**

El Codi de bones pràctiques estableix que el Servei de Salut posa a la disposició del personal l'accés a determinats recursos informàtics que faciliten el desenvolupament del seu treball i recorda que aquests recursos són propietat del Servei de Salut; com a tals, han de ser utilitzats per a les labors pròpies del personal d'acord amb les funcions que tingui assignades.

D'altra banda, quant a l'ús dels recursos informàtics determina expressament que ha d'evitar-se usar equips o aplicacions que no estiguin especificats directament com a part del suport lògic o del suport físic estàndard del Servei de Salut, tret que es tingui autorització expressa i per escrit de la gerència.

10) Es pot configurar el compte de correu corporatiu per redirigir els missatges de correu electrònic a comptes personals?

Amb caràcter general, el Codi de bones pràctiques estableix que en cap cas les comunicacions durant les tasques professionals s'han d'enviar des de comptes de correu electrònic personals ofertes per proveïdors d'internet. Tampoc està permès en cap cas redirigir a comptes particulars missatges de correu electrònic de caràcter professional rebuts en el compte proporcionat pel Servei de Salut. Per tant, s'ha de restringir la configuració dels comptes d'usuari per redirigir els missatges de correu electrònic a altres comptes personals (o professionals), però alienes al compte corporatiu proporcionat pel Servei de Salut.

11) Quin protocol ha de seguir cada gerència per a la gestió dels ordinadors dels usuaris quant a l'ús dels recursos informàtics del Servei de Salut?

1. Enviar una nota interna (vegeu una imatge del model després del punt 3) per informar sobre la prohibició d'emmagatzemar arxius d'àudios, vídeo i imatge en les unitats de xarxa per a ús personal i sobre l'advertiment que aquests arxius s'esborraran en una data determinada.
2. Uns dies abans de la data prevista per esborrar-los, s'ha d'enviar un recordatori.
3. En la data en qüestió, s'ha de fer una còpia de seguretat de les dades i posteriorment esborrar tots els arxius excepte aquells que els usuaris hagin demanat expressament que es conservin.

Model de nota interna

CONSELLERIA
SALUT I CONSUM
SERVEI SALUT
ILLES BALEARS

NOTA INTERNA

Assumpte: prohibició d'emmagatzemar vídeos i imatges per a ús personal en les unitats de xarxa

De: Comitè de Seguretat de la Informació A: tots els usuaris de la Gerència

El Codi de bones pràctiques del Servei de Salut en l'ús dels sistemes d'informació i en el tractament de les dades de caràcter personal —recentment se n'ha aprovat una versió nova per mitjà de la Instrucció 4/2022, de 5 de maig, del director general del Servei de Salut de les Illes Balears—, que és de compliment obligat per a tots els professionals, estableix en el punt 7.1.1 que «el Servei de Salut posa a disposició dels usuaris l'accés a determinats recursos informàtics i dispositius de comunicacions, tant fixos com mòbils, que faciliten l'acompliment de la seva feina. Aquests recursos són propietat del Servei de Salut; com a tals, s'han d'emprar per a les tasques pròpies dels usuaris d'acord amb les funcions assignades». D'altra banda, en el punt 7.1.5 determina que està prohibit expressament utilitzar els recursos informàtics per a les finalitats següents:

- Emmagatzemar informació amb continguts de caràcter racista, xenòfob, pornogràfic, sexual, d'apologia del terrorisme o que atempti contra els drets humans, o que actuï en perjudici dels drets a la intimitat, a l'honor i a la imatge pròpia o contra la dignitat de les persones.
- Instal·lar i/o emprar programes o continguts que atemptin contra la legislació en matèria de protecció de la propietat intel·lectual.

Respecte de l'ús de les unitats ofimàtiques (punt 7.3), el Codi de bones pràctiques especifica expressament que «el Servei de Salut pot posar a la disposició dels usuaris unitats ofimàtiques —que consisteixen en espai de disc en xarxa assignat a cada usuari pel personal tècnic del Servei de Salut— per contenir les salvaguardes periòdiques de les seves unitats locals. Aquestes unitats corporatives no s'han d'utilitzar per a finalitats privades, perquè són una eina de treball, tenen una capacitat limitada i són compartides per tots els usuaris, per la qual cosa només s'hi ha de salvaguardar la informació que es consideri estrictament necessària. En particular, cal evitar emmagatzemar en aquestes unitats —fins i tot amb caràcter provisional o temporal— continguts de mida grossa, com ara fitxers multimèdia (àudio, vídeo, imatges...)».

Pel que fa a la gestió de les incidències de seguretat (punt 13), el Codi de bones pràctiques estableix que «l'ús adequat dels recursos informàtics evita que es produeixin incidents que puguin anar en detriment de la seguretat de la informació, alhora que garanteix un rendiment òptim. Per això, quan es detectin incidents que puguin afectar la seguretat de la informació, és responsabilitat del Servei de Salut dur a terme les actuacions que es considerin convenients i proporcionals per prevenir i/o corregir els riscs identificats, per mitjà del monitoratge i l'anàlisi dels recursos afectats per assegurar que s'empren de la manera apropiada i per preservar la seguretat dels sistemes del Servei de Salut».

Per tot això, atesa la necessitat d'optimitzar els recursos el dia XX de xxxx de 20XX s'eliminaran tots els fitxers d'àudio, vídeo i d'imatge que estan allotjats a les unitats de xarxa. Si considerau necessari mantenir-ne algun per necessitats relacionades amb la vostra activitat professional, posau-vos en contacte amb el servei d'informàtica per comunicar quins fitxers necessiteu conservar i per quin motiu, a més de la unitat on estan allotjats.

Localitat, XX de xxxxxxxxx de 20XX

El president | La presidenta del Comitè de Seguretat de la Informació	El secretari | La secretària del comitè i responsable de seguretat de la informació
Nom Llinatge1 Llinatge2	Nom Llinatge1 Llinatge2

12) Es pot modificar la configuració de l'equip d'usuari?

El Codi de bones pràctiques estableix que el Servei de Salut és el responsable de determinar les normes, les condicions i les responsabilitats oportunes per protegir els recursos informàtics.

Per no comprometre les mesures de seguretat establertes pel Servei de Salut, els usuaris han d'evitar emprar equips o aplicacions que no estiguin especificats directament com a part del suport lògic o del suport físic estàndard del Servei de Salut. En cap cas es pot modificar la configuració establerta dels recursos. Per tant, cal evitar emprar, installar o distribuir programes fora de les recomanacions i dels estàndards aprovats pel Servei de Salut, ja que poden comprometre la seguretat dels sistemes d'informació.

Si és necessari installar programes aliens a l'estàndard establert, cal demanar autorització al responsable del servei, tot i que és necessària la valoració prèvia del servei d'informàtica.

La installació de programes informàtics ha de ser sempre a càrrec del servei d'informàtica corresponent o ha de ser monitorada per aquest a fi d'assegurar que es compleixen les mesures de seguretat requerides i que es compta amb les garanties de suport oportunes.

Amb l'objectiu de mantenir uns nivells adequats de protecció de la informació i dels recursos informàtics, el Servei de Salut ha desenvolupat les pautes necessàries per mantenir les mesures de seguretat que garanteixin que es compleix la normativa vigent en la prestació dels serveis sanitaris.

13) Es pot facilitar una còpia de la bústia de correu i dels documents d'un usuari que està actiu en l'organització?

Sempre que l'usuari estigui actiu i tingui l'autorització de la direcció, es pot facilitar la còpia sollicitada. En canvi, si l'usuari no està actiu s'ha de denegar la petició, ja que el Codi de bones pràctiques estableix que quan un usuari finalitza la relació o vinculació amb el Servei de Salut deixa de tenir accés als seus sistemes d'informació i a les dades que contenen. Així mateix, ha de retornar qualsevol suport que contingui dades a què hagi tingut accés en el marc de la vinculació o relació amb el Servei de Salut.

14) Quines restriccions s'estableixen quant a la navegació i l'ús d'internet?

El Codi de bones pràctiques estableix que, per motius de seguretat i de rendiment de la xarxa del Servei de Salut, els serveis informàtics poden monitorar i limitar l'ús d'internet . A més, el sistema que proporciona el servei de navegació pot disposar filtres d'accés que bloquegin l'accés a webs amb continguts inadequats, programes lúdics de descàrrega massiva o pàgines potencialment insegures o que contenguin virus o codis malignes.

Per aquest motiu, tenint en compte la necessitat d'optimitzar els recursos disponibles, el volum del tràfic de dades i els riscos de seguretat associats a l'ús d'internet, s'han establert certes restriccions en la navegació per internet, per motius de seguretat i de qualitat del servei i per complir en tot moment els requisits que estableix la legislació vigent, i de conformitat amb l'article 23 de l'ENS.

En conseqüència, aquestes restriccions s'han de mantenir, però si es requereix accedir a determinades pàgines web per motius professionals, es pot establir un sistema de peticions per sol·licitar accés a aquestes pàgines per revisar-les des del punt de vista dels riscs de seguretat i, si escau, habilitar-hi l'accés.

15) Es pot enviar per correu electrònic informació que contingui informació sensible o dades de caràcter personal?

L'Oficina de Seguretat recomana que no s'enviïn dades de salut per correu electrònic; en tot cas, seria necessari xifrar els correus; a més, es corre el risc que es guardi informació de categories especials de dades en els correus.

Es recomana enviar per correu una URL en què estiguin allotjades les dades i que el sistema en què s'emmagatzemin no sigui públic i només hi tenguin accés les persones que ho requereixin per exercir les seves funcions.

16) Es pot emprar Whatsapp, Telegram, etc. per enviar informació sensible que contengui dades de caràcter personal?

L'Oficina de Seguretat desaconsella emprar el servei de Whatsapp o altres aplicacions de missatgeria per a usos professionals, perquè no ofereixen garanties de seguretat suficients per al tractament de dades personals, en particular les dades considerades categories especials de dades.

17) Puc emprar una xarxa wifi pública que no sigui del Servei de Salut per fer feina?

L'Oficina de Seguretat ha decidit que de cap manera es pot emprar una xarxa wifi pública per fer feina, perquè qualsevol persona no autoritzada podria capturar informació sensible, atès que no és una xarxa segura.

18) És segur emprar els serveis d'Office 365 per introduir en els formularis els números d'història clínica?

L'entorn d'Office 365 està totalment protegit, però hem de reforçar el missatge que les eines ofimàtiques no són aplicacions de gestió d'històries clíniques, per la qual cosa no s'han d'utilitzar amb aquesta finalitat. Així mateix, hem de recordar que la Llei d'autonomia de pacients estableix que la història clínica ha de ser única, per la qual cosa no pot estar separada en carpetes personals, cosa que dificultaria salvaguardar els drets dels interessats, entre altres aspectes.

Mesures de seguretat

1) Quines mesures de seguretat cal establir per identificar i autenticar pacients per mitjà d'internet?

En el marc de les administracions públiques cal tenir en compte allò que preveu la Llei 39/2015 pel que fa a la identificació i la signatura dels interessats en el procediment administratiu. Es poden identificar electrònicament per aquests mitjans:

a) Sistemes basats en certificats electrònics reconeguts o qualificats de signatura electrònica expedits per prestadors inclosos en la llista de confiança de prestadors de serveis de certificació.

b) Sistemes basats en certificats electrònics reconeguts o qualificats de segell electrònic expedits per prestadors inclosos en la llista de confiança de prestadors de serveis de certificació.

c) Sistemes de clau concertada i qualsevol altre sistema que les administracions públiques considerin vàlid, en els termes i les condicions que s'estableixin.

Els interessats poden signar electrònicament per aquests mitjans:

d) Sistemes de signatura electrònica reconeguda o qualificada i avançada basats en certificats electrònics reconeguts o qualificats de signatura electrònica expedits per prestadors inclosos en la llista de confiança de prestadors de serveis de certificació.

e) Sistemes de segell electrònic reconegut o qualificat i de segell electrònic avançat basats en certificats electrònics reconeguts o qualificats de segell electrònic inclosos en la llista de confiança de prestadors de serveis de certificació.

f) Qualsevol altre sistema que les administracions públiques considerin vàlid, en els termes i les condicions que s'estableixin.

De conformitat amb la LOPDGDD, el Servei de Salut, com a organisme públic, té l'obligació d'implementar les mesures de seguretat establertes en l'ENS. Per això cal adoptar les mesures de seguretat que garanteixin la protecció de les dades en la identificació i autenticació dels usuaris, de conformitat amb el marc normatiu aplicable.

2) Quines previsions cal adoptar per registrar dades d'imatges de pacients?

En primer lloc, cal determinar la finalitat del tractament de les imatges en el moment en que hom faciliti informació al pacient perquè pugui decidir si vol signar el document de consentiment informat:

a) Si la finalitat és assistencial, de diagnòstic o tractament, estaria coberta per la finalitat del tractament «Historia clínica».

b) Si la finalitat del registre d'aquestes imatges és la recerca, estudis, etc., entraria en la finalitat del tractament «Recerca sanitària».

D'altra banda, pel que fa a l'aplicació de mesures de seguretat, d'acord amb la disposició addicional primera de la LOPDGDD, en els tractaments de dades cal implementar les mesures de seguretat establertes en l'ENS.

3) Quines mesures de seguretat cal adoptar per destruir documentació d'una manera segura?

Per garantir que la documentació es destrueix de manera segura cal atendre les instruccions i les mesures establertes en el document *Procedimiento de destrucción de documentos y soportes con datos personales del Servicio de Salud de las Islas Baleares*, en el qual es descriuen les mesures tècniques i organitzatives per garantir la destrucció correcta dels documents i dels suports d'informació.

Així mateix, la legislació que regula la destrucció de documentació en aspectes relacionats amb la seguretat de la informació indica, d'una banda, que la documentació amb dades de caràcter personal s'ha de destruir adoptant mesures dirigides a evitar que es pugui recuperar posteriorment i, d'altra banda, la documentació afectada per l'ENS ha de ser destruïda de manera segura.

D'altra banda, si es contractàs una empresa especialitzada, aquesta tindria la consideració d'*encarregat de tractament*, per la qual cosa caldria complir allò que la

legislació de protecció de dades estipula, igual que altres empreses que tracten dades de caràcter personal per compte del Servei de Salut.

Per establir un procediment de destrucció de documentació cal exigir que la destrucció compleixi la norma espanyola UNE-EN-15713:2010 («Destrucció segura del material confidencial. Codi de bones pràctiques»), que regula tots els aspectes recomanables perquè el procediment es faci de manera segura, entre d'altres, els següents:

- Mesures que han de complir les dependències.
- Mesures que han de complir els empleats.
- Com s'ha de recollir, custodiar i transportar la documentació.
- Què s'ha de fer amb el material resultant una vegada destruïda la documentació.

En relació amb la mida dels residus resultants de la destrucció, cal exigir que la destrucció es faci seguint la normativa DIN/CEN 32757, d'àmbit internacional, que estipula quina ha de ser la mida dels trossos de paper depenent de la confidencialitat de la documentació. Tenint en compte que la documentació pot contenir dades de caràcter personal, cal exigir que es compleixi com a mínim el nivell de seguretat núm. 3, indicat en la normativa esmentada. Finalment, cal certificar la destrucció segura de la documentació.

4) Quines consideracions cal tenir en compte a l'hora de generar llistes temporals amb dades de caràcter personal la finalitat de les quals és de gestió de serveis sanitaris?

Tal com exigeix l'article 30 del RGPD, cada responsable ha de dur un registre de les activitats de tractament efectuades sota responsabilitat seva. Aquest registre ha de contenir les dades següents, com a mínim, per cada tractament: dades de contacte del responsable, finalitats del tractament, descripció de les categories de dades, categoria de destinataris a qui es comuniquen les dades personals, indicació de si es faran transferències internacionals de dades, terminis prevists per suprimir les diferents categories, descripció de les mesures tècniques que cal aplicar segons el risc, etc.

El mateix Reglament no esmenta la necessitat de registrar els tractaments que s'hagin de fer de manera temporal. Per això, el Servei de Salut ha establert els criteris següents per determinar la necessitat que un tractament temporal de dades s'inclogui o no en el registre:

- Valorar el grau de temporalitat del tractament: cal identificar si el tractament de dades temporal serà ocasional o de manera recursiva cada cert període de temps.
- Identificar si es gestionaran a gran escala categories especials de dades o dades relatives a condemnes i infraccions penals.
- Valorar si és probable que el tractament d'aquestes dades pugui suposar un risc alt per als drets i les llibertats de les persones físiques, tenint en compte la naturalesa, el context, l'abast i els objectius del tractament.

Si el tractament de dades ha de ser recursiu en el temps, o sobre categories especials de dades o dades relatives a condemnes i infraccions penals o si pot suposar un risc per als drets i les llibertats de les persones físiques, tenint en compte la naturalesa, el context, l'abast i els objectius del tractament, cal incloure'l en el registre d'activitats de tractament del responsable.

En canvi, si el tractament de dades ha de ser ocasional o no tractarà categories especials de dades ni dades relatives a condemnes i infraccions penals o no suposarà un risc per als drets i les llibertats de les persones físiques, no s'ha de fer constar el tractament en qüestió en el registre d'activitats de tractament de responsable, però sí que s'ha de fer constar en el tractament d'origen respecte del qual depenguin.

D'altra banda, el resultat del risc analitzat determinarà quines mesures de seguretat cal aplicar sobre el tractament de seguretat.

5) Quina és la política sobre l'accés del personal sanitari a aplicacions clíniques des de ca seva?

Amb caràcter general, no es permet que accedeixin a aplicacions clíniques des de fora de les instal·lacions si l'accés no està justificat correctament. Aquesta habilitació ha d'estar condicionada per una necessitat funcional i assistencial que justifiqui l'accés de determinats professionals.

En aquest punt és important ressaltar l'obligació de control d'accés, que estableix que els usuaris tindran accés als recursos que necessitin per acomplir les seves funcions. Pot arribar a ser necessari habilitar l'accés a professionals que facin feina des de fora de les instal·lacions o estiguin de guàrdia, però aquests permisos s'han de revocar o negar sempre que no es doni alguna d'aquestes dues condicions.

Habilitar la possibilitat que els professionals es connectin des de l'exterior de la xarxa del Servei de Salut augmenta els riscs per a la seguretat i per a la confidencialitat i, en conseqüència, incrementa les mesures de seguretat que cal aplicar, que no són només tècniques sinó també organitzatives.

Per això, com a norma general no s'aconsella concedir permisos per accedir a aplicacions clíniques des de l'exterior de la xarxa del Servei de Salut. Així doncs, aquests permisos s'han de donar exclusivament basant-se en necessitats i durant el temps que durin aquestes necessitats.

6) Quines recomanacions cal seguir per comunicar dades per mitjans telemàtics fora de la xarxa del Servei de Salut?

De conformitat amb la LOPDGDD, el Servei de Salut, com a organisme públic, té l'obligació d'implementar les mesures de seguretat establertes en l'ENS, que són les següents quant a la protecció de les comunicacions:

- Emprar xarxes privades virtuals quan la comunicació discorri per xarxes fora del domini de seguretat.
- Emprar algorismes acreditats pel Centre Criptològic Nacional, ja sigui per mitjà del xifrat simètric, protocols d'acord de clau, algorismes asimètrics o funcions resum.

7) Quins són els requisits de confidencialitat i protecció de dades per fer un pilot de nou programari?

L'article 33 de la LOPDGDD estableix que l'accés d'un encarregat de tractament a les dades personals necessàries per prestar un servei al responsable no es considera comunicació de dades.

D'altra banda, l'article 28 de l'RGPD determina que el tractament a càrrec de l'encarregat s'ha de regir per un contracte o acte jurídic que el vinculi al responsable i estableixi l'objecte, la durada, la naturalesa i la finalitat del tractament, el tipus de dades personals i la categories dels interessats, a més de les obligacions i els drets del responsable. Aquest contracte o acte jurídic ha d'estipular particularment els aspectes següents pel que fa a l'encarregat:

- Ha de tractar les dades personals únicament seguint instruccions documentades del responsable i ha d'informar immediatament el responsable si, al seu parer, una instrucció infringeix la normativa de protecció de dades aplicable.
- Ha de garantir que les persones autoritzades per tractar dades s'hagin compromès a servar-ne la confidencialitat.
- Ha d'aplicar les mesures tècniques i organitzatives apropiades per garantir un nivell de seguretat adequat al risc.
- No ha de recórrer a un altre encarregat sense l'autorització prèvia per escrit, específica o general, del responsable. En aquest cas, cal imposar a aquest altre encarregat —per mitjà d'un altre contracte o acte jurídic— les mateixes obligacions de protecció de dades que les estipulades en el contracte o acte jurídic entre el responsable i l'encarregat.
- Ha d'ajudar el responsable tant com sigui possible, i té l'obligació de respondre les sol·licituds que tenguin per objecte l'exercici dels drets dels interessats.
- Ha d'ajudar el responsable a garantir que es compleixi l'RGPD, concretament les obligacions que estableixen els articles 32-36.
- A elecció del responsable, ha de suprimir o tornar totes les dades personals una vegada que acabi la prestació dels serveis de tractament.
- Ha de posar a la disposició del responsable tota la informació necessària per demostrar que es compleixen les obligacions establertes en el contracte.

Per tot això, cal regularitzar aquesta relació establint un contracte d'encarregat del tractament, independentment que es tracti d'una demostració d'un potencial servei o bé de la prestació d'aquest.

8) Quines recomanacions cal seguir per crear una contrasenya segura?

En el procés de generar i gestionar contrasenyes, cal tenir en consideració les regles següents:

- Han de tenir una longitud de vuit caràcters o més.
- Han de consistir en una combinació de caràcters alfanumèrics (lletres majúscules i minúscules, dígits numèrics i signes especials).
- No convé que tenguin caràcters idèntics consecutius.
- Idealment, la contrasenya no ha de ser igual a cap de les tres darreres contrasenyes emprades.
- La contrasenya s'ha de canviar periòdicament, cada tres mesos.
- No han d'estar basades en dades que algú altre pugui endevinar o obtenir fàcilment.
- Han de ser fàcils de recordar. Per tant, cal trobar una solució de compromís entre la robustesa de la contrasenya i la facilitat de recordar-la.

- Cal evitar comunicar les contrasenyes per escrit.
- És especialment important mantenir el caràcter secret de la contrasenya.
- És recomanable emprar sistemes de gestió de contrasenyes.

9) Es fan còpies de seguretat de la informació de caràcter personal emmagatzemada en l'equip local o en dispositius personals?

Amb caràcter general, la informació emmagatzemada de manera local en els ordinadors i equips informàtics dels usuaris no és objecte de salvaguarda per mitjà de cap procediment corporatiu de còpia de seguretat.

No obstant això, en el cas que es tracti d'informació de pacients especialment protegida, cal complir totes les mesures de seguretat de nivell alt exigides per l'RGPD, per la qual cosa no podem recomanar que es mantenguin aquestes dades en fitxers ofimàtics, atès que no garanteixen les mesures de seguretat (xifratge de la informació, autenticació d'usuaris, registre d'accessos, etc.).

10) Es pot extreure informació del registre d'accessos per incorporar-la a un informe intern per tal d'obrir algun tipus d'expedient (disciplinari, per exemple)?

Els sistemes d'informació que gestionen dades de caràcter personal han de generar un registre d'accessos, a fi de supervisar i controlar el tractament i l'ús que se'n fa.

Per això, si es detecten incidents que puguin afectar la seguretat de la informació (per exemple, la sospita d'accessos indeguts), és responsabilitat del Servei de Salut dur a terme les actuacions convenients i proporcionals per prevenir i/o corregir els riscs identificats monitorant i analitzant els recursos afectats per comprovar si s'empren apropiadament i per preservar la seguretat dels sistemes del Servei de Salut.

En aquest sentit, el Codi de bones pràctiques habilita que l'anàlisi i el monitoratge d'accessos es facin per un requeriment legal o una investigació sobre un ús il·legítim o il·legal, per vigilar i controlar si es compleixen les obligacions, per controlar els mitjans informàtics, per coordinar la continuïtat laboral, per protegir el sistema informàtic, i per prevenir responsabilitats davant terceres persones.

En qualsevol d'aquests supòsits, no hi hauria inconvenient per obtenir aquesta informació del registre d'accessos per incorporar-la a un informe intern. No obstant això, convindria cursar una sol·licitud formal en la qual s'especificàs la finalitat per a la qual es requereix la informació (un expedient disciplinari, per exemple), i d'aquesta manera tenir documentada la sol·licitud.

Confidencialitat

1) Què és el deure de confidencialitat?

És un dels principis de la LOPDGDD, per mitjà del qual s'estableix que totes les persones que intervenguin en qualsevol fase del tractament de dades personals estan subjectes a tractar-los de tal manera que en garanteixin la seguretat adequada —inclosa la protecció contra el tractament no autoritzat o il·lícit i contra la pèrdua, la destrucció o el dany accidental— aplicant-hi mesures tècniques o organitzatives apropiades. Aquesta obligació és complementària dels deures de secret professional, de conformitat amb la normativa aplicable.

2) Què passa si es vulnera el deure de secret?

L'incompliment del deure de confidencialitat és una infracció considerada molt greu segons l'article 72 de la LOPDGDD. A més, si una infracció és imputable a una autoritat o un directiu i s'acredita que hi havia recomanacions perquè el tractament hagués estat atès degudament, en la resolució cal incloure una amonestació al càrrec responsable i se n'ha d'ordenar la publicació en el *Butlletí Oficial de l'Estat* o en el diària oficial autonòmic que correspongui.

3) En quins casos es pot revelar informació?

Les lleis permeten als professionals sanitaris revelar dades dels pacients sense que puguin ser sancionats per això en els tres casos següents: *a)* quan el pacient ho autoritzi, *b)* quan la llei exigeixi col·laborar amb la justícia i *c)* quan hi hagi un risc per a terceres persones.

4) Es pot facilitar informació per telèfon a un pacient sobre el seu estat de salut o el resultat de proves?

Segons ha disposat l'AEPD en la seva *Guía para pacientes y usuarios de la sanidad*, «en principi, hi hauria el risc d'estar facilitant informació a un tercer i, per tant, per motius de seguretat s'hauria d'evitar. Es podria fer si hi ha un protocol d'identificació del sol·licitant de la informació, mitjançant la sol·licitud de nom i llinatges, número de DNI, número de telèfon des del qual telefona que coincideixi amb el que va facilitar al professional, adreça electrònica, número de targeta sanitària, etc. Caldria tenir la seguretat que qui sol·licita la informació n'és el titular» [traducció de l'original].

Per això, de conformitat amb el *Protocolo de actuación en los casos de solicitudes de información sobre ubicación de pacientes del Servicio de Salud*, com a norma general no es pot facilitar per telèfon informació sobre la ubicació de pacients. En aquest cas, cal indicar al sol·licitant —incloses les forces i els cossos de seguretat de l'Estat— que ha d'acudir en persona a la gerència per fer la consulta.

5) Si durant una telefonada al 061 revel informació de salut d'un pacient identificat que necessita assistència i posteriorment, com a titular de les dades, exercesc el dret d'accés a la transcripció d'aquesta telefonada, ¿s'incompliria la normativa de protecció de dades si s'inclouen les dades del pacient sense el seu consentiment?

Sí, en concret s'incompliria el principi d'integritat i confidencialitat de les dades previst en l'article 5.1.*f)* de l'RGPD, per permetre un accés no autoritzat a dades personals d'altres interessats.

Segons estableix el RGPD (articles 15-22), els interessats tenen dret a exercir els drets d'accés, rectificació, supressió, limitació, oposició i/o portabilitat respecte de les dades personals «que els concerneixin». En aquest sentit, quan es rebi una sol·licitud per exercir aquests drets cal respondre-hi limitant-se exclusivament a les dades que concerneixin l'interessat.

Per tant, si es rep una sol·licitud d'accés a la transcripció d'una telefonada cal facilitar exclusivament les dades que concerneixin l'interessat i anonimitzar o suprimir la informació que afecti terceres persones, tal com estableix el procediment de gestió dels drets dels interessats del Servei de Salut.

En aquest sentit, si es rep una sol·licitud per exercir el dret d'accés a una telefonada relativa a l'assistència d'una tercera persona, s'ha de limitar a les dades que es refereixin a la seva persona, sempre que no entri en col·lisió amb els drets del pacient en qüestió.

Així mateix, la informació facilitada s'ha d'integrar en la història clínica del pacient identificat, perquè —segons estableix l'AEPD, en la seva *Guía para pacientes y usuarios de la sanidad*— «tot pacient o usuari té dret que quedi constància, per escrit o en el suport tècnic més adequat, de la informació obtinguda en tots els seus processos assistencials, fets pel servei de salut tant en l'àmbit de l'atenció primària com en el de l'atenció especialitzada» [traducció de l'original].

A més, de conformitat amb l'article 14 de l'RGPD, quan les dades personals s'obtinguin d'una tercera persona —p. ex., per mitjà d'una telefonada al 061— cal facilitar al titular de les dades la informació relativa al tractament que es dona a les seves dades al més aviat possible (a tot estirar, en el termini d'un mes). En particular, cal proporcionar-li tota la informació que preveu l'article 13 del RGPD i sobre l'origen de les seves dades.

Això no obstant, no cal revelar qui va fer la telefonada, perquè cal tenir en compte que el dret a l'accés del pacient a la documentació de la història clínica no es pot exercir en perjudici del dret de terceres persones a la confidencialitat de les dades que hi consten, recollides en interès terapèutic del pacient, ni en perjudici del dret dels professionals participants en l'elaboració, els quals poden oposar-se al dret d'accés la reserva de les anotacions subjectives.

6) Quan les forces de seguretat ho sol·liciten, ¿és obligatori facilitar-los les dades personals dels usuaris del centre?

Els tractaments de dades que facin les forces i els cossos de seguretat no entren en l'àmbit d'aplicació de l'RGPD ni de la LOPDGDD, sinó de l'article 22 de la Llei orgànica 15/1999, que estipula que la recollida de dades de caràcter personal a càrrec de les forces i els cossos de seguretat de l'Estat sense el consentiment de les persones afectades es limita als supòsits i a les categories de dades que siguin necessàries per prevenir un perill real per a la seguretat pública o per reprimir infraccions penals.

En el cas concret de les dades de salut, es poden recollir exclusivament en els supòsits en què sigui absolutament necessari per a les finalitats d'una investigació concreta, i d'acord amb el *Protocolo de comunicación de datos a cuerpos y fuerzas de seguridad del Estado*. En els casos en què un professional, en ocasió de l'assistència sanitària que hagi prestat, tengui l'evidència que el pacient pateix lesions que hagin pogut ser causades per un tercer i n'hagi assabentat l'autoritat judicial per mitjà del corresponent comunicat judicial de lesions, les forces de seguretat actuants, en la funció de policia judicial, no podran accedir a les dades de salut del pacient diferents de les relatives a la lesió que consta en el comunicat judicial esmentat sense un mandat judicial o una sol·licitud del Ministeri Fiscal.

Addicionalment, qualsevol accés a la història clínica associat a les dades d'identificació personal dels pacients amb finalitats judicials està subjecte al que disposin els tribunals en cada cas concret, de manera que no és lícit accedir-hi sense el mandat judicial corresponent, d'acord amb l'article 16.3 de la LAP.

Qualitat de les dades

1) Quina regulació és aplicable al tractament que els treballadors socials donen a les dades de caràcter personal?

Amb caràcter general, la Llei 4/2009, d'11 de juny, de serveis socials de les Illes Balears, regula les prestacions del sistema públic de serveis socials establint tres tipus de prestacions: prestacions tècniques, econòmiques i tecnològiques, d'acord amb la classificació següent:

- Prestacions tècniques: informació sobre els recursos socials més adequats disponibles i sobre com accedir-hi; orientació sobre els mitjans més adequats per respondre a les necessitats plantejades; assessorament i suport a les persones i als grups que necessitin l'actuació social; valoració singularitzada i diagnòstic social de les situacions personals, de convivència i familiars, i de les demandes socials; intervenció professional i tractament social orientats a complir les finalitats dels serveis socials; protecció jurídica i social dels menors d'edat en situació de risc i desemparament; protecció jurídica i social de les persones amb capacitat limitada; atenció residencial substitutiva de la llar; atenció diürna/nocturna/domiciliària.
- Prestacions econòmiques: aportacions dineràries que tenen per finalitat atendre determinades situacions de necessitat de les persones que no disposen de prou recursos econòmics per afrontar-les i que no estan en condicions d'aconseguir-ne o de rebre'n d'altres fonts.
- Prestacions tecnològiques: les que atenen les necessitats socials de les persones per mitjà d'un producte, com ara la teleassistència domiciliària i les ajudes instrumentals destinades a mantenir o millorar l'autonomia personal o afavorir la inserció social.

Així mateix, aquesta Llei reconeix el dret a la confidencialitat respecte de la informació que coneguin els serveis socials, d'acord amb la legislació de protecció de dades de caràcter personal, i en tipifica l'incompliment com una infracció greu.

En conseqüència, aplicant el principi de qualitat de les dades, els treballadors socials han de recollir únicament i exclusivament les dades que siguin estrictament necessàries per gestionar la prestació social corresponent, és a dir, només les que siguin pertinents i apropiades a la finalitat que es persegueix i, a més, realment necessàries, no excessives.

2) Quina regulació és aplicable al tractament de dades per prevenir la mutilació genital femenina?

Respecte de la regulació de la prevenció de la mutilació genital femenina, cal remarcar el següent:

- L'article 149.2 del Codi penal la tipifica com un delicte de lesions en els termes següents: «El que causi a un altre una mutilació genital en qualsevol de les seves manifestacions es castiga amb la pena de presó de sis a 12 anys».
- Per una altra banda, l'article 23.4 de la Llei orgànica 6/1985, d'1 de juliol, del poder judicial, estableix la competència de la jurisdicció espanyola per conèixer d'aquests fets comesos per espanyols o estrangers fora del territori estatal, sempre que els responsables siguin a Espanya; és a dir, habilita la persecució del delicte tot i que s'hagi comès fora del territori espanyol. D'aquesta manera s'intenta impedir la

mutilació genital femenina aprofitant que la família de la possible víctima d'aquest delicte se'n va de vacances al seu país d'origen.

Si bé altres comunitats autònomes tenen regulació específica, en el nostre cas cal regir-se per la Llei orgànica 1/2004, de 28 de desembre, de mesures de protecció integral contra la violència de gènere, i la Llei 11/2016, de 28 de juliol, d'igualtat de dones i homes, i actuar seguint el *Protocol d'actuació sanitària davant la violència masclista a les Illes Balears*, i entendre la mutilació genital femenina com una expressió més de violència de gènere.

En aquest sentit, l'article 78 de la Llei 11/2016, relatiu a identificació de les situacions de violència masclista, estableix com a mitjà de prova per identificar la situació de violència de gènere l'informe mèdic, infermer o psicològic d'un professional col·legiat en el qual consti que la víctima ha estat atesa en algun centre sanitari a conseqüència de la violència masclista.

En el cas de la mutilació genital femenina, amb la possibilitat d'anotar en la història clínica de la pacient la recomanació d'impedir-la explicant les conseqüències físiques i psicològiques que provoca i les conseqüències legals trobaríem prou habilitació en la normativa esmentada, perquè aquesta informació resultaria necessària per a la prevenció i el diagnòstic mèdics, la prestació d'assistència sanitària o tractaments mèdics o la gestió de serveis sanitaris sempre que aquest tractament de dades el faci un professional sanitari subjecte al secret professional o una altra persona subjecta així mateix a una obligació equivalent de secret.

3) Es pot proporcionar una llista d'altes de pacients, amb informació del servei i motiu de l'alta, al servei de centraleta telefònica (*call center*) per atendre telefonades?

En primer lloc, cal destacar que la mera relació de pacients ingressats es considera informació que fa referència a dades de salut del pacient o que pot revelar-les, i respecte d'això la LOPDGDD i l'RGPD són especialment rigorosos, atès que estableixen com a regla general la prohibició de tractar aquesta categoria de dades llevat que hi concorri alguna base de legitimació de les descrites en l'article 9.2 de l'RGPD.

D'altra banda, els usuaris haurien de tenir accés únicament i exclusivament als recursos que requereixin per acomplir les seves funcions. En aquest sentit, es considera que la indicació del servei i el motiu de l'alta podrien excedir aquestes funcions.

En línia amb el que s'ha exposat, pel que fa a la identificació de l'interessat en telefonades el *Procedimiento de actuación en la atención de comunicaciones telefónicas respecto al RGPD* estableix la premissa de no facilitar cap mena d'informació de caràcter personal i confidencial dels pacients si no és possible acreditar la identitat de l'interlocutor telefònic com a titular de les dades per mitjà d'algun dels mecanismes proposats.

Per tot això, recomanam que s'eviti facilitar aquestes dades (servei i motiu de l'alta) al personal d'atenció de les telefonades, que es garanteixi l'aplicació de mesures de seguretat de nivell alt en l'accés a aquestes llistes i que s'extremi la precaució sobre la informació dels pacients que es faciliti per telèfon, de conformitat amb el *Procedimiento de actuación en la atención de comunicaciones telefónicas respecto al RGPD*.

4) Hi ha cap norma que obligui a incloure en la transcripció d'una telefonada entre el 061 i un usuari el nom del teleoperador que l'ha atès?

Sí. De conformitat amb l'article 14 de la Llei 41/2002, en la història clínica ha de constar, entre altres informacions, la identificació dels metges i d'altres professionals que hagin intervingut en les telefonades per tal d'assolir la màxima integració possible de la documentació clínica de cada pacient, almenys, en l'àmbit de cada centre. En aquest sentit, cal registrar qui ha atès un usuari, tant presencialment com en una telefonada al 061.

Consentiment

1) Quins requisits han de complir els documents de consentiment per fer estudis de recerca o docència?

D'acord amb el *Protocolo de protección de datos en el ámbito de la investigación y docencia* i basant-se en la disposició addicional dissetena de la LOPDGDD, el tractament de dades en la recerca en matèria de salut és lícit sempre que l'interessat —o el seu representant legal— atorgui explícitament el consentiment.

Tal com estableix el punt 32 de l'RGPD, el consentiment s'ha de fer efectiu per mitjà d'un acte afirmatiu clar que reflecteixi una manifestació de voluntat lliure, específica, informada i inequívoca del pacient d'acceptar el tractament de dades de caràcter personal en qüestió, és a dir, una declaració per escrit —fins i tot per mitjans electrònics— o verbal. I, d'acord amb el punt 7, si el tractament es basa en el consentiment del pacient, el responsable ha de ser capaç de demostrar que aquell ha consentit que es tractin les seves dades personals. En aquest sentit, atès que la capacitat de demostrar el consentiment atorgat verbalment és molt limitada, l'Oficina de Seguretat recomana, com a regla general, que l'acte de consentiment informat es dugui a terme per escrit.

2) Quin és el termini de conservació del consentiment atorgat per a la comunicació de dades de caràcter personal?

Cal prendre en consideració els aspectes següents per determinar el termini:

- Si el tractament es basa en el consentiment del pacient, el responsable ha de ser capaç de demostrar que aquell ha consentit el tractament de les seves dades personals (article 7.1 de l'RGPD).
- Tractar dades de caràcter personal sense el consentiment de les persones afectades està catalogat com a infracció molt greu (article 72 de la LOPDGDD).
- Les infraccions molt greus prescriuen al cap de tres anys (article 47.1 de la Llei orgànica 15/1999).

Per tot això, el termini mínim durant el qual cal conservar aquest consentiment és de tres anys, a fi de garantir l'atenció de possibles responsabilitats derivades del tractament. No s'ha de confondre aquest consentiment amb el termini de conservació del consentiment informat o de la documentació clínica que figura en la història clínica del pacient, per als quals el termini de conservació és superior. En aquest sentit, es recomana consultar la política de conservació del Servei de Salut, en la qual s'indiquen els terminis màxims de conservació de les dades personals segons les diferents activitats de tractament de les dades que fa el Servei de Salut.

3) Cal demanar consentiment a un usuari per verificar les seves dades a fi d'evitar que hagi d'aportar la documentació que les acredita?

Amb caràcter general, no cal demanar aquest consentiment si les dades de caràcter personal es recullen per acomplir les funcions pròpies de les administracions públiques en l'àmbit de les seves competències.

Això no obstant, per emprar els serveis de verificació i consulta de dades, per mitjà de plataformes d'intermediació, l'article 6.2.*b)* de la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics, reconeix el dret «a no aportar les dades i documents que estiguin en poder de les administracions públiques, les quals han d'utilitzar mitjans electrònics per obtenir la informació esmentada sempre que, en el cas de dades de caràcter personal, tinguin el consentiment dels interessats en els termes que estableix la Llei orgànica 15/1999, de protecció de dades de caràcter personal, o una norma amb rang de Llei ho determini, llevat que hi hagi restriccions d'acord amb la normativa aplicable a les dades i documents recollits. El consentiment es pot emetre i acceptar per mitjans electrònics».

D'altra banda, l'article 3 del Decret 6/2013, de 8 de febrer, de mesures de simplificació documental dels procediments administratius, que desplega els drets reconeguts en la Llei 4/2001, de 31 de març, de la bona administració i del bon govern de les Illes Balears, estableix igualment que «és necessari que la persona interessada consenti que les seves dades o documents puguin ser consultats i comprovats per l'òrgan instructor, fent constar aquest consentiment, expressament, en la sol·licitud d'iniciació del procediment o en qualsevol altra comunicació posterior. [3] Quan la persona interessada no atorgui el seu consentiment exprés per fer les consultes oportunes, estarà obligada a aportar la documentació que contengui les seves dades. Si no l'aporta, l'Administració li ha de requerir la documentació [...].»

4) És necessari que el metge o el centre sanitari demani el consentiment al pacient o usuari per recollir i emprar les seves dades personals?

No és necessari si s'han d'emprar per a finalitats de medicina preventiva o laboral, d'avaluació de la capacitat laboral del treballador, de diagnòstic mèdic, de prestació d'assistència o tractament de tipus sanitari o social o de gestió dels sistemes i serveis d'assistència sanitària i social. La base de legitimació per a aquest tractament de dades està establerta en l'article 6.1.*b)* de l'RGPD per a les entitats asseguradores de salut privades i en l'article 6.1.*c)* del mateix Reglament per a la sanitat pública.

Tampoc és necessari si es tracten les dades per raons d'interès públic en l'àmbit de la salut pública, com ara la protecció davant amenaces transfrontereres greus per a la salut o per garantir alts nivells de qualitat i de seguretat de l'assistència sanitària i dels medicaments o productes sanitaris o la inspecció de reclamacions dels usuaris. La base de legitimació està establerta en l'article 6.1.*e)* de l'RGPD.

També es poden tractar les dades de salut sense demanar consentiment si el tractament és necessari per protegir interessos vitals del pacient o usuari —o d'una altra persona física si aquell no està capacitat físicament o jurídicament per donar consentiment— o quan ho demani un òrgan judicial. La base de legitimació està establerta en l'article 6.1.*d)* de l'RGPD.

5) **En els casos de persones sense incapacitar legalment, però que, per exemple, estan en una fase avançada de deterioració cognitiva i es neguen a rebre atenció social, ¿es poden tractar les seves dades sense que hi doni consentiment?**

Sí, és possible, perquè la base jurídica del tractament de les seves dades personals no és el consentiment, sinó una obligació legal aplicable al responsable del tractament, o el compliment d'una missió que es du a terme en interès públic o en l'exercici de poders públics. Depenent dels casos i les circumstàncies també pot ser-hi aplicable que el tractament sigui necessari per protegir els interessos vitals de l'interessat.

A més d'aquestes bases, pot ser aplicable alguna de les excepcions de l'article 9.2 de l'RGPD o una conjunció d'aquestes.

Cessió o comunicació de dades

1) **Es poden facilitar les dades de contacte d'un pacient a una oficina de farmàcia perquè es posi en contacte amb aquest per comunicar-li incidències en relació amb la dispensació de medicaments?**

D'acord amb el registre del tractament «Gestió de la prestació farmacèutica», aquest té la finalitat de gestionar i controlar la prescripció de medicaments, visats i despesa farmacèutica de les Illes Balears, en la qual no es preveu recollir entre les dades de caràcter identificador les de contacte del pacient (adreça, telèfon, etc.). Així mateix, tampoc s'hi preveu cedir o comunicar aquestes dades més enllà de les previsions legals.

En aquest sentit, no hi ha habilitació per comunicar aquestes dades a les oficines de farmàcia amb la finalitat que es pretén, perquè l'article 33 de la Llei 16/2003, de 28 de maig, de cohesió i qualitat del Sistema Nacional de Salut, remet a la normativa vigent en matèria de protecció de dades pel que fa a la definició de les dades bàsiques per a la gestió per mitjans informàtics de la informació necessària per a la dispensació individualitzada de medicaments.

Per a això, sempre que es tractin dades amb una finalitat diferent a l'establerta cal demanar explícitament el consentiment del pacient. Com a alternativa, es proposa invertir el circuit i que sigui la Direcció General de Farmàcia qui comuniqui al pacient la incidència notificada per l'oficina de farmàcia, perquè acudeixi a aquesta oficina corresponent o s'hi posi en contacte, sense perjudici de les possibles implicacions de fer comunicacions telefòniques. Així doncs, abans de facilitar qualsevol informació cal comprovar la identitat de l'interlocutor telefònic per mitjà d'un mecanisme segur, és a dir, fent-li preguntes de validació per garantir que és el titular de les dades.

Cal tenir una consideració especial quan es telefoni a un domicili i l'interessat no hi sigui, o quan s'activi un contestador. En aquests casos, en què no es pot autenticar la identitat del titular de les dades, cal complir la premissa bàsica de no facilitar informació de caràcter personal i confidencial dels pacients.

2) **Es poden facilitar al Col·legi Notarial de les Illes Balears les dades d'ingrés d'un pacient?**

Aquesta informació es considera una dada de caràcter personal relacionada amb la salut, per la qual cosa cal complir totes les obligacions previstes per la LOPDGDD i l'RGPD.

La comunicació al Col·legi Notarial de les Illes Balears s'ha de considerar una comunicació de dades a tercers, per la qual cosa cal tenir el consentiment de l'interessat, llevat que el tractament es faci per una obligació legal, per interès públic o en l'exercici de poders públics.

Actualment no es té el consentiment dels pacients per cedir aquestes dades al Col·legi Notarial ni s'ha pogut constatar que comunicar-les-hi amb la finalitat de l'ordenació de l'exercici de professió notarial i de fer complir els col·legiats les lleis generals i especials estigui emparat per alguna de les excepcions previstes per la LOPDGDD i l'RGPD. La comunicació d'aquestes dades sense consentiment podria suposar una infracció tipificada com a molt greu per la LOPDGDD, perquè són dades de caràcter personal relacionades amb la salut. Per tant, no es poden comunicar.

En aquest sentit, en la seva *Guía para pacientes y usuarios de la sanidad*, l'AEPD ha afirmat que es poden cedir les dades de salut a altres entitats diferents de les que les han recollides i tractades si hi ha legitimació, com ara quan es visita un metge de la sanitat privada —amb la targeta de la companyia asseguradora— i aquest facilita a l'entitat la informació mínima necessària perquè aboni la prestació sanitària.

3) Es pot informar l'ocupador sobre les dades de salut dels seus empleats quan acudeixen a una revisió de prevenció dels riscs laborals?

No. La informació que es facilita a l'ocupador és si el treballador és apte o no apte per a la feina, o si és apte i necessita alguna adaptació, però no se'l pot informar dels resultats de les proves mèdiques dels treballadors.

4) Quina informació han de contenir els comunicats mèdics de baixa? Es poden facilitar a l'ocupador?

El facultatiu que segueix el procés d'incapacitat del treballador expedeix dues còpies del comunicat mèdic de baixa: una per al treballador i l'altra per entregar-la a l'empresa on fa feina.

Aquest document ha de contenir les dades personals del treballador, la data de la baixa, la contingència que la causa, el codi de diagnòstic, el codi estatal d'ocupació del treballador i la durada estimada del procés de recuperació de la salut i, si escau, l'anotació de si es tracta de la recaiguda d'un problema de salut anterior. Així mateix, hi ha de constar la data en què es farà el pròxim reconeixement mèdic.

5) Quines recomanacions cal tenir en compte per expedir justificants d'hospitalització als familiars d'un pacient?

L'Oficina de Seguretat ha elaborat el *Procediment de sol·licitud i emissió de justificants d'assistència sanitària i hospitalització del Servei de Salut de les Illes Balears*, en l'apartat 3.2 del qual s'explica com s'ha d'actuar quan es rep la sol·licitud d'un acompanyant d'un pacient perquè li expedeixin un justificant de l'hospitalització.

6) Es poden facilitar a un ajuntament dades d'assistència sanitària d'un pacient que ha interposat una reclamació per responsabilitat patrimonial?

Cal tenir en compte que, en la tramitació d'un expedient de responsabilitat patrimonial, l'accés de l'òrgan instructor a la documentació sanitària o a la història clínica de l'interessat és una comunicació o cessió de dades.

L'AEPD s'ha pronunciat respecte de les cessions o comunicacions de dades mantenint la validesa de la comunicació de dades personals entre administracions públiques. No obstant això, perquè es pugui dur a terme, s'hauria de fonamentar en alguna de les bases jurídiques previstes en l'article 6 de l'RGPD:

a) Ha de tenir el consentiment de l'interessat per al tractament de les seves dades personals.

b) El tractament ha de ser necessari per executar un contracte en el qual l'interessat sigui part.

c) El tractament ha de ser necessari per complir una obligació legal, per protegir interessos vitals, per complir una missió realitzada en interès públic o en l'exercici de poders públics conferits al responsable de tractament, i per satisfer interessos legítims perseguits pel responsable del tractament.

Per tot això, es recomana no cedir dades personals a tercers encara que es tengui el consentiment exprés a aquest efecte, atès que en ocasions la mateixa AEPD ha determinat que aquest consentiment no es considera un fonament jurídic vàlid perquè una administració pública tracti dades personals.

7) Es poden facilitar dades d'usuaris d'un centre sanitari als diputats autonòmics que ho sol·licitin?

Els diputats autonòmics, dins les seves funcions de control, poden obtenir informació personal de la qual és responsable el Govern de les Illes Balears. Les sol·licituds d'informació dels diputats s'han de tractar en els termes i amb les limitacions establertes en els reglaments del Parlament de les Illes Balears com a norma especial aplicable de manera prevalent.

Les sol·licituds d'informació dels diputats no s'han d'adreçar als centres sanitaris, sinó a la Conselleria de Salut i Consum, la qual, tenint en compte la sensibilitat de la informació, pot comunicar fonamentadament els motius que poden evitar o restringir la informació que s'ha de facilitar als diputats. Els centres sanitaris, si escau, poden manifestar aquestes limitacions a la Conselleria.

8) Hi ha una directriu comuna per expedir justificants per als pacients i els acompanyants?

Sí. L'Oficina de Seguretat ha elaborat el *Procediment de sol·licitud i emissió de justificants d'assistència sanitària i hospitalització del Servei de Salut*, en el qual s'estableixen els passos i les instruccions que cada òrgan del Servei de Salut ha de seguir per expedir justificants d'assistència sanitària i d'hospitalització pera als pacients i els acompanyants, i s'hi presenten els tipus de justificant que es poden expedir.

Sobre aquesta matèria, l'AEPD estableix en la *Guía para pacientes y usuarios de la sanidad*, que «l'acompanyant té un interès legítim per a aquest tractament i ha d'acreditar la vinculació amb el pacient. El contingut del justificant ha de complir el principi de minimització de dades i ha d'incloure el nom i els llinatges del pacient, la data i l'hora de l'ingrés i el nombre aproximat de dies d'estada. No ha d'especificar la malaltia ni la unitat on està ingressat el pacient ni el tipus de cirurgia» [traducció de l'original].

9) Pot un centre hospitalari informar de l'ingrés d'un pacient i d'un està allotjat?

Segons la *Guía para pacientes y usuarios de la sanidad*, no és possible, sinó que ha de demanar consentiment al pacient o als seus familiars (si aquell no està capacitat) perquè es pugui facilitar aquesta informació. A més, per evitar situacions conflictives és molt important que es faciliti aquesta informació de manera destacada i fent entendre al pacient les conseqüències pràctiques.

En aquesta línia, el *Protocolo de actuación frente a solicitudes de información sobre ubicación de pacientes del Servicio de Salud de las Islas Baleares* disposa que, sempre que el pacient estigui en condicions i plenament capacitat, cal demanar-li consentiment perquè la gerència corresponent pugui facilitar la informació sobre on està allotjat; a més, en l'acte de consentiment ha de determinar quines persones hi estan autoritzades a saber aquesta informació. El formulari de consentiment s'ha de conservar digitalitzat en la història clínica del pacient i en paper en l'arxiu de la gerència.

També regula com cal actuar per atendre aquesta sol·licitud depenent de l'estat del pacient i d'on estigui allotjat:

a) Hospitalitzacions urgents derivades d'un procés assistencial al servei d'urgències: només es pot facilitar la informació sobre on està allotjat el pacient a les persones que hagin comparegut al servei d'admissió i estiguin vinculades amb el pacient per raons familiars o de fet (mare/pare, filla/fill, germana/germà, dona/marit o parella de fet). Per comprovar el vincle, el sol·licitant ha d'aportar informació addicional (document d'identitat, llibre de família...).

b) Hospitalitzacions programades: si el pacient està plenament capacitat, en el moment que ingressi a l'hospital cal demanar-li consentiment per informar sobre on estarà allotjat a les persones que ho sol·licitin compareixent al servei d'admissió. Si no hi ha evidència clara sobre si l'estat del pacient li permet donar-hi, aleshores només es podrà facilitar la informació a les persones que hi estiguin vinculades per raons familiars o de fet.

Excepcionalment i per a ambdós casos, si les forces o els cossos de seguretat de l'Estat demanen on està allotjat un pacient per motius de seguretat pública, cal facilitar-los la informació d'acord amb el *Protocolo de cesión de datos a las fuerzas y cuerpos de seguridad*.

10) En els casos de persones tutelades per agències de tutela d'adults, ¿poden els centres sociosanitaris facilitar als seus familiars dades sobre l'estat de salut o dades socials d'aquells?

En principi, no. Quan una persona està tutelada, la comunicació de qualsevol dada seva —sociosanitària o d'una altra naturalesa— s'ha de fer sempre al tutor legal o mitjançant aquest. Només es podrien facilitar dades als familiars si en la sentència d'incapacitació es determinàs aquesta possibilitat específicament o com a conseqüència del seu abast.

11) Si es rep una telefonada des de l'estranger per sol·licitar informació sobre on està allotjat un pacient, es pot facilitar?

El *Procedimiento de actuación en la atención de comunicaciones telefónicas respecto al RGPD* recomana donar només informació de si està allotjat en aquest centre concret, però sense detallar el lloc exacte ni el diagnòstic, perquè és difícil comprovar la identitat de la persona que telefona i quin vincle té amb el pacient.

12) Es pot deixar informació d'una cita en el contestador d'un telèfon?

No, mai s'ha de deixar aquesta informació en un contestador. Si el pacient no respon a la telefonada, s'ha d'intentar contactar-hi en un altre moment.

13) Es poden enviar citacions per correu postal ordinari?

Sí, sempre que a l'exterior del sobre no s'inclogui informació que pugui revelar-ne o evidenciar-ne el contingut. La confidencialitat de les comunicacions està legislada.

14) S'ha tingut en compte d'alguna manera l'atenció telefònica a persones sordes?

En l'article 4 del capítol II («Condicions bàsiques d'accessibilitat i no discriminació en matèria de telecomunicacions») del Reglament sobre les condicions bàsiques per a l'accés de les persones amb discapacitat a les tecnologies, els productes i els serveis relacionats amb la societat de la informació i els mitjans de comunicació social (aprovat pel Reial decret 1494/2007, de 12 de novembre) s'estableix que «el Ministeri de Treball i Afers Socials, a través del Centre Estatal d'Autonomia Personal i Ajudes Tècniques, ha de promoure l'existència d'una oferta suficient i tecnològicament actualitzada de terminals de telefonia mòbil especials, adaptats als diferents tipus de discapacitats».

15) Si un pacient no autoritza que s'expedeixi un justificant per a un acompanyant, ¿no hi ha risc de col·lisió amb els drets de l'acompanyant sobre la possibilitat de sol·licitar el permís corresponent a la seva empresa?

Sense el consentiment del pacient o del tutor legal no es pot expedir el justificant: el dret fonamental a la privadesa i la protecció de dades personals preval sobre el dret dels treballadors de gaudir d'un permís retribuït, recollit en la Llei de l'estatut bàsic de l'empleat públic i en la Llei de l'estatut dels treballadors.

16) Hi ha una locució informativa corporativa?

L'Oficina de Seguretat ha fet una proposta, inclosa en el procediment, que es pot utilitzar a aquest efecte:

> De conformitat amb el Reglament general de protecció de dades, us informam que [indicau la unitat organitzativa] serà el responsable de les dades que faciliteu amb la finalitat de [indicau la finalitat] i sobre la base del [incloure base legitimadora]. Les vostres dades es podran comunicar a tercers quan sigui necessari per complir les finalitats descrites. Teniu dret a accedir, rectificar i suprimir les dades que ens faciliteu, a oposar-vos i a limitar-ne el tractament i a la portabilitat d'aquestes dades. Així mateix, en [indicau on es troba la segona capa d'informació] podreu consultar la informació addicional i detallada sobre protecció de dades.
>
> Si acceptau aquest avís legal i voleu continuar, pitjau [X]. Si voleu tornar a escoltar l'avís legal pitjau [X].

17) Si una empresa o concessionària s'encarrega de la videovigilància, ¿també és responsable del tractament de les imatges?

El responsable del tractament de les imatges sempre és la gerència corresponent. Si són visionades per personal extern o emmagatzemades en sistemes o aplicacions d'un tercer, cal subscriure unes clàusules d'«encarregat del tractament per al tractament de les imatges per compte de tercers», de conformitat amb l'article 28 de l'RGPD; d'aquesta manera aquestes entitats adquireixen la condició d'encarregat del tractament de les imatges. L'Oficina de Seguretat ha elaborat un model de clàusules d'encarregat de tractament que han de subscriure amb els proveïdors dels serveis de videovigilància.

Exercici de drets de protecció de dades

1) Es pot facilitar informació sobre el registre d'accessos des dels sistemes d'informació per tal de satisfer el dret d'accés d'un pacient a la seva història clínica?

A petició del Departament Juridicoadministratiu del Servei de Salut, el 27 de maig de 2007 l'AEPD va emetre un informe sobre si és procedent facilitar aquesta informació, en el qual fa referència a la Resolució de 15 de juny de la mateixa AEPD sobre un supòsit en què la persona afectada va exercir el dret d'accés a les seves dades personals especificant que volia que li facilitassin una llista de les persones que hi havien accedit durant un període determinat. Per mitjà d'aquesta Resolució, l'AEPD va desestimar la sol·licitud al·legant que «no s'ha de confondre l'accés als documents i a les dades que figuren en l'expedient administratiu —que es regeix per la Llei de règim jurídic i del procediment administratiu comú— amb l'accés a dades personals, disponibilitat que va a compte de l'interessat, entre les facultats del qual no hi ha l'accés a les dades de les persones que hagin tramitat l'expedient corresponent, perquè no són dades objecte de tractament» [traducció de l'original]. En aquest sentit, l'Advocacia de l'Estat —adscrita a l'AEPD— entén que l'interessat únicament tindria dret a saber qui ha estat cessionari de les seves dades, però no els accessos des de l'organització del responsable de tractament.

Tot i que l'article 15 de la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal, hagi estat derogat per l'article 15 de l'RGPD i per l'article 13 de la LOPDGDD, l'abast del dret d'accés dels interessats és el mateix, per la qual cosa s'interpreta que es manté allò que estableix la Resolució de 15 de juny de 2007 de l'AEPD.

En aquest sentit s'ha pronunciat recentment l'AEPD en la *Guía para pacientes y usuarios de la sanidad* establint que, llevat que una llei ho permeti expressament, el dret d'accés no inclou la identificació dels professionals sanitaris que accedeixen a una història clínica.

2) Es poden facilitar les dades de un presumpte agressor registrats en la història clínica d'una víctima de violència de gènere?

Segons la tipologia de la informació tractada, s'ha identificat un supòsit de recollida de dades que podria resultar excessiva o no pertinent si aquesta informació es conservarà juntament amb la història clínica de la víctima o una simple còpia per arxivar-la al centre sanitari.

D'acord amb el *Protocolo común para la actuación sanitaria ante la violencia de género*, l'anotació en la història clínica d'una confirmació diagnòstica de violència de gènere no equival a una qualificació legal del cas, que és competència de l'àmbit judicial. És a dir, no s'està acusant ni jutjant el presumpte agressor, sinó avaluant clínicament la víctima.

Tanmateix, la incorporació d'aquesta informació podria excedir el judici de proporcionalitat i necessitat que exigeix el principi de qualitat de les dades, no tant en relació amb la finalitat judicial perseguida amb la notificació del comunicat mèdic de lesions, sinó per la possible incorporació o conservació d'aquest juntament amb la història clínica de la víctima.

En aquest sentit, atès que és un document medicolegal i no sanitari, la finalitat del qual és exclusivament judicial i no assistencial, convindria eliminar de la còpia conservada al centre la informació relativa al presumpte agressor, perquè no respon a la finalitat de les dades recollides amb una finalitat medicoassistencial.

Així mateix, per extensió al supòsit plantejat, es recomana retirar aquesta informació de la còpia de la història clínica que s'entregui a la víctima, perquè facilitar-la-hi podria vulnerar el dret a la confidencialitat de les dades referents a terceres persones.

3) En els casos d'ordres d'allunyament relacionades amb un usuari del centre sanitari, ja sigui per maltractaments, assetjament, violència de gènere, etc., ¿és possible informar-ne tots els empleats, inclosos els que no tenen accés a dades de caràcter personal (com ara el personal de neteja)?

La informació s'ha de traslladar a tot el personal que tengui la funció d'identificar els visitants i prendre decisions sobre l'accés al centre. En aquest sentit, cal tenir en compte que tot el personal —tant el que té accés a dades personals com el que no en té— ha d'haver subscrit un compromís de confidencialitat.

D'aquesta manera, de conformitat amb les accions mínimes que cal dur a terme en el sistema sanitari —definides en el *Protocol d'actuació sanitària davant la violència masclista a les Illes Balears*—, cal mantenir la privadesa i la confidencialitat de la informació obtinguda i establir una coordinació amb altres professionals i institucions. Així mateix, si es detecta un cas de violència de gènere cal seguir les recomanacions d'actuació descrites en aquest protocol.

4) S'ha d'atendre una sol·licitud de supressió del contingut complet de la història clínica d'un pacient?

Segons l'article 17 de l'RGPD, l'interessat té dret a obtenir sense dilació indeguda del responsable del tractament la supressió de les dades personals que li concerneixen. Quan el tractament de les dades sigui necessari per complir una obligació legal que requereixi el tractament de dades imposat pel dret de la Unió Europa que s'apliqui al responsable de tractament o per formular, exercir o defensar una reclamació, el responsable de tractament no està obligat a suprimir les dades personals per una simple sol·licitud de l'interessat.

L'article 6 de la Llei 14/1986, de 25 d'abril, general de sanitat, disposa que les actuacions de les administracions públiques sanitàries han d'estar orientades a garantir l'assistència sanitària en tots els casos de pèrdua de la salut.

D'altra banda, l'article 15 de la LAP assenyala que la història clínica ha d'incorporar la informació que es consideri transcendental per al coneixement veraç i actualitzat de l'estat de salut del pacient i que la finalitat principal d'aquesta és facilitar l'assistència sanitària, deixant constància de totes les dades que, sota criteri mèdic, permetin saber de manera veraç i actualitzada l'estat de salut. L'article 17 estableix l'obligació de conservar la documentació clínica per a l'assistència adient al pacient durant el temps adequat a cada cas, que ha de ser de cinc anys, com a mínim. No obstant això, l'apartat 2 del mateix article afegeix a l'obligació de conservació que la documentació clínica també s'ha de conservar a efectes judicials de conformitat amb la legislació vigent.

En aquest mateix sentit, l'article 32 de la LOPDGDD estableix que el responsable del tractament està obligat a blocar les dades quan les rectifiqui o les suprimeixi. En l'apartat 2 del mateix article es defineix com a *blocatge de dades* la identificació i la reserva de les dades rectificades o suprimides adoptant les mesures tècniques i organitzatives per impedir-ne el tractament —inclosa la visualització—, excepte per posar les dades a la disposició dels tribunals, el Ministeri Fiscal o les administracions públiques competents —en particular les autoritats de protecció de dades— per exigir possibles responsabilitats derivades del tractament i només pel termini de prescripció d'aquestes. Una vegada transcorregut aquest termini cal destruir les dades.

En aquest aspecte cal tenir en consideració el termini de prescripció de cinc anys de conservació de la informació establert per l'article 1964 del Codi civil perquè, si es presenta una reclamació contra un professional sanitari per una suposada responsabilitat contractual, la història clínica serveix com a mitjà de prova en els processos de prova sobre responsabilitat civil.

De tot això es desprèn que el dret a l'assistència sanitària no es podria garantir si determinats professionals no poguessin tenir accés al conjunt d'informació inclosa en una història clínica. Per això, el dret de rectificació i/o el de supressió de dades d'una història clínica pot estar limitat, perquè segons la *Guía para pacientes y usuarios de la sanidad*, si es tracta de dades mèdiques ha de ser el facultatiu o l'administració sanitària qui decideixi si es rectifiquen o cancel·len. Per a això cal analitzar rigorosament cada cas seguint el procediment següent:

1. Un metge funcional ha de valorar si la informació assistencial que es vol suprimir en la història clínica del pacient és necessària i essencial per garantir una assistència sanitària correcta.
2. En relació amb la valoració anterior:
   - Si es considera que la informació clínica assistencial que es vol eliminar és necessària i essencial per garantir una assistència sanitària correcta, s'ha de desestimar la sol·licitud de l'exercici del dret de supressió.
   - Si el metge funcional estima que la informació assistencial que se sol·licita suprimir no és necessària ni essencial per garantir una assistència sanitària correcta s'ha de consultar la data del procés assistencial corresponent a la informació que es vol eliminar. Si aquesta data és inferior o igual a cinc anys des de la data actual (termini mínim de conservació de les dades en la història clínica del pacient segons l'article 17 de la LAP), la informació no es pot suprimir de la història clínica del pacient ni es pot blocar fins que no venci el termini de prescripció; una vegada superat, la informació s'ha de suprimir totalment. En aquest sentit, és recomanable consular la *Política de conservación del Servicio de Salud de las Islas Baleares*, en la qual figura una

taula que indica els terminis màxims de conservació de les dades personals en funció de les diferents activitats de tractament que es desenvolupen en el Servei de Salut.

5) En un centre sociosanitari, ¿és possible cancel·lar/suprimir determinades dades d'un usuari si ho sol·licita?

Posem com a exemple el cas d'un usuari que no vol que constin algunes dades de tipus social —per exemple, que els fills no el visiten—, considerades imprescindibles per prestar la deguda atenció atès que reflecteixen els suports familiars.

En aquest cas no és possible suprimir les dades. Com que el consentiment no és la base jurídica del tractament, no és possible revocar el consentiment ni oposar-se al tractament de les dades sense ponderar aquest dret amb la base jurídica que avala el tractament. Amb caràcter general, la base jurídica es trobarà en el compliment d'una obligació legal aplicable al responsable del tractament, perquè cal mantenir l'autenticitat de la història sociosanitària.

La sol·licitud s'ha de contestar motivant les raons per les quals no es cancel·len les dades, d'acord amb allò que preveu el *Protocolo de actuación en el ejercicio de derechos de los interesados*.

Una cautela apropiada podria ser marcar aquestes dades com a confidencials i establir mecanismes perquè només siguin consultades quan sigui estrictament necessari i, en cadascun dels accessos, advertir del seu caràcter especialment sensible per mitjà d'un missatge al professional que hi accedeix.

6) Si els pares d'un pacient menor d'edat estan separats, ¿poden exercir el dret d'accés a la història clínica del seu fill o filla?

Cal tenir en consideració diferents criteris d'edat:

a) Segons la LAP, els menors d'edat emancipats o que tenguin setze anys complerts poden prestar consentiment informat sense necessitat de representant.

b) Els menors que tenguin catorze anys complerts poden exercir els drets de protecció de dades sense necessitat de representant.

c) Els menors que tenguin dotze anys complerts tenen dret a ser escoltats amb relació a les actuacions que puguin afectar-los la salut, tot i que el consentiment l'ha de prestar un representant legal.

Per respondre la pregunta plantejada, si el menor està emancipat o té catorze anys complerts, l'exercici del dret d'accés a la història clínica no s'exerceix mitjançant un representant legal, sinó que cal que el menor doni consentiment o que sigui representat per una persona que hagi designat.

En canvi, si el menor té catorze anys, cadascun dels pares pot exercir el dret d'accés a la informació assistencial de la seva història clínica sempre que tots dos tenguin la potestat parental; però si els pares estan separats, cal acreditar la potestat parental presentant un document judicial (sentència o interlocutòria que aprovin el conveni regulador) que faci referència a aquesta condició.

No obstant això, cal tenir en compte allò que estableix la *Guía para pacientes y usuarios de la sanidad* sobre l'accés dels pares a la història clínica dels fills menors

que tenguin entre catorze i divuit: «El Codi civil estableix que la pàtria potestat s'exerceix en benefici dels fills menors d'edat; així mateix, els pares han de vetlar per aquests, alimentar-los i educar-los. L'accés a la informació sanitària és fonamental per vetlar pels menors. Està limitat el dret a les persones que tenen la pàtria potestat, no a altres familiars» [traducció de l'original].

7) Què cal fer si la sol·licitud d'exercici de drets es cursa per un mitjà diferent de l'establert pel Servei de Salut?

Tal com estableix l'article 12.2 de la LOPDGDD, «el responsable del tractament està obligat a informar l'afectat sobre els mitjans a la seva disposició per exercir els drets que li corresponen. Els mitjans han de ser fàcilment accessibles per a l'afectat. L'exercici del dret no es pot denegar pel sol motiu que l'afectat opti per un altre mitjà».

Actualment, el Servei de Salut posa a la disposició dels interessats la possibilitat de sol·licitar l'exercici d'aquests drets per mitjà dels serveis responsables de cada gerència, per a la qual cosa ha dissenyat formularis en els quals es concreta la informació que l'interessat ha d'aportar per cursar la sol·licitud.

Si l'interessat opta per contactar-hi per altres mitjans (per correu electrònic, per telèfon...), cada gerència del Servei de Salut estarà obligada a atendre la sol·licitud indicant tota la informació que l'interessat ha d'aportar per cursar la sol·licitud.

8) Quina diferència hi ha entre una sol·licitud de revisió d'accessos a la història clínica i una sol·licitud de l'exercici de dret d'accés a la història clínica?

La sol·licitud d'accés a la història clínica és un dret de protecció de dades establert i regulat per l'RGPD i la LOPDGDD. L'interessat té dret a obtenir del Servei de Salut l'accés a les dades personals que li concerneixen i a la informació següent sobre aquestes dades: finalitats del tractament; categories de les dades; destinataris de les dades; termini previst de conservació; possibilitat de sol·licitar al responsable que rectifiqui o suprimeixi les dades personals o que en limiti el tractament; possibilitat d'oposar-se al tractament; dret de presentar una reclamació davant una autoritat de control; informació sobre l'origen de les dades, i informació sobre possibles transferències internacionals.

Les sol·licituds per exercir el dret d'accés es reben a cada gerència i és responsabilitat de cadascuna tramitar-les i resoldre-les, per a això les gerències tenen un termini d'un mes des del moment en què les reben. No obstant això, aquest termini es pot prorrogar dos mesos per motiu de la complexitat o el nombre de sol·licituds rebudes.

En canvi, una sol·licitud de revisió d'accessos a la història clínica es refereix a la llista de tots els professionals que hagin accedit a la història clínica d'un pacient. Aquestes sol·licituds es presenten en cada gerència, però aquestes les envien a l'Oficina de Seguretat perquè les revisi. L'Oficina de Seguretat proporciona els accessos i emet els informes corresponents juntament amb el model de resposta que cal donar a l'interessat. Tota aquesta informació es remet a la gerència corresponent perquè investigui els possibles accessos indeguts i perquè el seu departament d'atenció a l'usuari contacti amb l'interessat per donar-li la resposta a la sol·licitud. En aquest cas no hi ha cap norma que estableixi un termini de resposta.

9) Què cal tenir en compte quan un pacient sol·licita exercir el dret de no ser informat?

De conformitat amb l'article 4 de la LAP i l'article 11 de la Llei 5/2003, de 4 d'abril, de salut de les Illes Balears, el pacient té dret a no ser informat dels processos assistencials sempre que manifesti aquesta voluntat per escrit especificant els processos dels quals no vol ser informat. És important destacar que la sol·licitud l'ha de cursar el pacient mateix, sempre que no estigui incapacitat.

10) En el cas d'un menor que tengui catorze anys complerts, ¿és necessari que autoritzi els seus tutors legals perquè puguin exercir els drets del menor en representació d'aquest?

L'article 154 del Codi civil habilita l'accés dels pares a la informació sanitària dels fills sobre els que tenguin la potestat parental a fi de vetlar adequadament per la salut d'aquests, en compliment de les obligacions que els imposa precisament la potestat parental. L'habilitació per accedir a l'historial clínic es refereix només als titulars de la potestat parental, no a qualsevol familiar del menor.

Pel seu costat, el menor d'edat pot exercir el dret d'accés a la seva història clínica a partir dels catorze anys, però no es pot entendre com una limitació del dret dels titulars de la potestat parental del menor no emancipat d'accedir a la seva història clínica.

Les reclamacions en els casos de negativa d'entregar les històries clíniques dels menors als progenitors que tenguin la potestat parental s'han d'adreçar a les autoritats sanitàries o judicials corresponents.

Accés i conservació d'històries clíniques

1) Quins requisits cal comprovar abans d'habilitar els psicòlegs per accedir a la història clínica amb funcions d'inspecció?

Amb caràcter general, la LAP habilita l'accés a les històries clíniques al personal sanitari acreditat degudament que tengui funcions d'inspecció, avaluació, acreditació i planificació, per comprovar la qualitat de l'assistència, si es respecten els drets dels pacients/usuaris i si es compleix tota obligació del centre amb aquests o amb la mateixa administració sanitària.

En aquest sentit, la normativa estableix que els psicòlegs que facin feina a centres, establiments o serveis del Sistema Nacional de Salut (SNS) —o a centres concertats amb aquest— per oferir les prestacions sanitàries derivades de la cartera de serveis comuns del SNS que els pertoquin han de tenir el títol oficial de psicòleg/psicòloga especialista en psicologia clínica. Però si no fan feina en el marc de la cartera de serveis comuns del SNS, per tenir la consideració de professionals sanitaris han de tenir també el títol oficial de màster en Psicologia General Sanitària.

2) Què s'entén per *anotació subjectiva*?

Una *anotació subjectiva* són les impressions o valoracions personals que un professional sanitari fa constar en una història clínica que no estan basades directament en dades objectives ni en proves complementàries sinó exclusivament en la percepció pròpia, però que són d'interès per atendre un pacient, tot i que no poden tenir la consideració de *diagnòstic*. Cal d'abstenir-se d'incloure-hi expressions, comentaris o dades que no tenguin relació amb l'assistència sanitària del pacient o que

no tenguin transcendència per saber de manera veraç i actualitzada l'estat de salut del pacient.

Sobre aquest tema, la *Guía para pacientes y usuarios de la sanidad* estableix que els professionals sanitaris que elaborin la documentació d'una història clínica poden oposar la reserva de les seves anotacions subjectives al dret d'accés a aquesta documentació.

3) Qui ha de revisar el contingut de la història clínica abans de facilitar-ne una còpia al pacient?

D'acord amb l'article 18.3 de la LAP, cal tenir en compte dues limitacions importants per recopilar la informació que s'entregarà lliurarà al pacient:

- Anotacions subjectives: es reconeix el dret a eliminar les anotacions subjectives de la documentació que s'entregarà.
- Dades relatives a terceres persones implicades en el diagnòstic o coneixement del pacient: no es poden facilitar dades de terceres persones que es puguin incloure en la història d'un pacient per interès terapèutic. Cal ocultar o eliminar aquesta informació abans d'entregar la documentació al pacient.

Per això es considera que el més adequat és que la direcció mèdica o el coordinador del centre revisi la documentació que s'entregarà lliurarà i retiri aquestes dades i anotacions.

4) Es pot facilitar al pacient la informació relativa als processos assistencials de psiquiatria o psicologia?

Atès que el pacient té el dret d'accedir a la documentació de la seva història clínica, això inclou la informació relativa als processos assistencials de psiquiatria o psicologia. Per tant, es reconeix el dret d'accés al contingut d'aquesta informació encara que estigui en un suport separat de la resta del contingut de la història clínica o en històries clíniques separades.

No obstant això, en aquests casos cal prestar una atenció especial a les limitacions al dret d'accés, perquè s'ha de separar la informació relativa a terceres persones implicades en el diagnòstic o el reconeixement del pacient, de manera que no se'n facilitin dades que constin en la història clínica del pacient. És a dir, aquestes dades no pertanyen al pacient i no és possible facilitar-les-hi, i per això cal ocultar-les o eliminar-les abans d'entregar-li la documentació.

5) Són possibles els tractaments amb finalitats dea recerca mèdica en un centre sociosanitari?

Sí, de conformitat amb l'article 9.2.*j)* del RGPD, és permès el tractament de categories especials de dades per a finalitats de recerca científica, sobre la base del dret de la Unió Europea o dels estats membres, sempre que es compleixin aquestes condicions:

- El tractament ha de ser proporcional a l'objectiu establert.
- Cal respectar la protecció de dades en allò que és essencial.
- Cal establir mesures adequades i específiques per protegir els interessos i els drets fonamentals de l'interessat.

- Els tractaments s'han de supeditar a les garanties adequades, a la normativa sectorial sanitària, a la LAP i, en particular, a la disposició addicional dissetena de la LOPDGDD disposant mesures tècniques i organitzatives adequades, sobretot per garantir la minimització de les dades.

6) És necessari que la documentació de la història clínica es conservi en paper per fer assaigs clínics?

En l'article 58 del text refós de la Llei de garanties i ús racional dels medicaments i productes sanitaris —aprovat pel Reial decret legislatiu 1/2015, de 24 de juliol— s'estableix que tots els assaigs clínics, inclosos els estudis de biodisponibilitat i bioequivalència, s'han de dissenyar, dur a terme i comunicar d'acord amb les normes de bona pràctica clínica i respectant els drets, la seguretat i el benestar dels subjectes de l'assaig, que prevalen sobre els interessos de la ciència i la societat.

Pel que fa a les garanties de la recerca dels medicaments d'ús humà, en l'article 62 (relatiu a les garanties de transparència) s'estableix que tota la informació sobre l'assaig clínic s'ha de registrar, tractar i conservar de mode que es pugui comunicar, interpretar i comprovar de manera precisa i alhora protegint el caràcter confidencial dels registres dels subjectes de l'assaig.

Per una altra banda, el Reial decret 1090/2015, de 4 de desembre, pel qual es regulen els assajos clínics amb medicaments, els comitès d'ètica de la recerca amb medicaments i el Registre Espanyol d'Estudis Clínics, estableix el següent en l'article 38, relatiu a les normes de bona pràctica clínica:

- El promotor d'un assaig clínic i l'investigador han de garantir que l'assaig clínic es du a terme de conformitat amb el protocol i els principis de la bona pràctica clínica.
- Sense perjudici d'altres disposicions, el promotor i l'investigador, en elaborar el protocol i aplicar aquest Reial decret i el protocol, han de tenir degudament en compte les normes de qualitat i les directrius de la Conferència Internacional d'Harmonització sobre bona pràctica clínica.
- En el cas d'assaigs clínics amb medicaments de teràpia avançada cal seguir addicionalment les normes de bona pràctica clínica específiques per a medicaments de teràpia avançada.
- L'Agència Espanyola de Medicaments i Productes Sanitaris ha de fer accessibles públicament les directrius sobre bona pràctica clínica previstes en aquest article.

L'arxiu mestre de l'assaig clínic ha de complir allò que estableixen els articles 57 i 58 del Reglament sobre assaigs clínics de medicaments d'ús humà, que disposen el següent:

- El promotor i l'investigador han de dur un arxiu mestre de l'assaig clínic, que ha de contenir en tot moment els documents essencials relacionats amb aquest assaig clínic que permetin verificar la qualitat de les dades obtingudes tenint en compte totes les característiques de l'assaig, en particular si es tracta d'un assaig clínic de nivell baix d'intervenció. Aquest arxiu ha d'estar fàcilment disponible per als estats de la Unió Europea, que han de poder accedir-hi directament quan ho sol·licitin.
- Els suports emprats per conservar el contingut de l'arxiu mestre han de permetre mantenir-lo complet i llegible durant vint-i-cinc anys.

En conseqüència, no sembla que sigui necessari conservar la documentació de la història clínica en paper per fer aquests assaigs.

7) Durant quant de temps cal conservar la documentació i les mostres d'anatomia patològica?

Segons les conclusions de conservació de mostres i documents en anatomia patològica del Llibre blanc de la Societat Espanyola d'Anatomia Patològica, amb caràcter general es recomanen els terminis de conservació següents:

- Informes: deu anys des del diagnòstic, com a mínim.
- Blocs de parafina: deu anys, com a mínim.
- Peticions: fins al diagnòstic, com a mínim.

D'altra banda, l'article 17 de l'RGPD estableix que el pacient té dret que el responsable del tractament de les seves dades les suprimeixi sense dilació indeguda quan ja no siguin necessàries per a les finalitats per a les quals es van recollir. En aquest mateix sentit, l'article 32 de la LOPDGDD determina que el responsable del tractament està obligat a blocar les dades quan sigui procedent rectificar-les o suprimir-les. (Vegeu la definició de *blocatge de dades* en el punt 4 del capítol «Exercici de drets de protecció de dades»). Passat aquest termini cal destruir les dades, de conformitat amb les instruccions definits en el *Procedimiento de destrucción de documentos y soportes con datos personales del Servicio de Salud de las Islas Baleares*.

Respecte de les peticions, no hi ha regulació específica sobre aquest tema. Seguint la recomanació de la Societat Espanyola d'Anatomia Patològica, sembla adequat conservar-les fins al diagnòstic, com a mínim.

8) Què cal prendre principalment en consideració en habilitar l'accés a la història clínica amb finalitats de recerca i/o docència?

D'acord amb *el Protocolo de protección de datos en proyectos de investigación y docencia*, cal tractar les dades en un entorn amb dades dissociades. D'acord amb la LAP, l'accés a la història clínica amb finalitats de recerca o docència es regeix per la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (actualment derogada gairebé totalment per la LOPDGDD), i la Llei 14/1986, de 25 d'abril, general de sanitat, i la resta de normes aplicables en cada cas. L'accés a la història clínica amb aquestes finalitats obliga a preservar les dades d'identificació personal del pacient separades de les de caràcter clinicoassistencial, de manera que, com a regla general, quedi assegurat l'anonimat, llevat que el pacient hagi donat consentiment per no separar-les.

Per això cal tractar les dades de manera dissociada, per tal que no sigui possible identificar l'interessat, és a dir, que no sigui possible establir per mitjans raonables el nexe entre una dada i una persona identificada o identificable gràcies al fet d'haver destruït el nexe amb tota informació que identifiqui l'interessat o que l'associació exigeixi un esforç (termini de temps o despesa) desproporcionat.

Addicionalment, en el protocol esmentat s'estableix el procediment d'autorització i registre d'accessos a la història clínica a fi de controlar els que tenguin la finalitat descrita, però el tractament dissociat de les dades és essencial si no es pot aconseguir el consentiment del pacient.

9) Es pot facilitar l'accés a la història clínica d'un pacient que hagi mort?

D'acord amb l'article 3 de la LOPDGDD, els centres sanitaris i els facultatius d'exercici individual només poden facilitar l'accés a la història clínica d'un pacient que hagi mort a les persones vinculades a aquest per raons familiars o de fet, i als hereus d'aquell, llevat que el pacient mort ho hagués prohibit expressament o una llei ho estableixi així.

Sobre aquest tema, l'AEPD ha manifestat en la *Guía para pacientes y usuarios de la sanidad*, que «els centres sanitaris i els facultatius d'exercici individual només poden facilitar l'accés a la història clínica d'un pacient que hagin mort a les persones vinculades a aquest per raons familiars o de fet, tret que el pacient ho hagués prohibit expressament i així s'acrediti. En qualsevol cas, l'accés d'una tercera persona a la història clínica motivat per un risc per a la seva salut s'ha de limitar a les dades pertinents. No es pot facilitar informació que afecti la intimitat del mort ni les anotacions subjectives dels professionals, ni que perjudiqui terceres persones. Llevat que una llei ho permeti expressament, el dret d'accés no inclou la identificació dels professionals sanitaris que accedeixen a la història clínica» [traducció de l'original].

10) Puc accedir a la història clínica d'un amic o d'un familiar seu si aquell m'ho demana per informar-lo del seu estat de salut?

No, només podeu accedir a la informació que necessiteu per acomplir les vostres funcions. Si un amic us demana aquesta informació, indicau-li que no hi estau autoritzat i que pot sol·licitar-la formalment al seu facultatiu.

En aquest sentit s'ha expressat l'AEPD en la *Guía para pacientes y usuarios de la sanidad* [traducció de l'original]:

> Quan un professional sanitari accedeix a una història clínica ho ha de fer perquè és necessari per fer la seva feina. No és lícit que hi accedeixi per curiositat, per facilitar informació d'un pacient a un conegut, un veïnat...
>
> L'Agència Espanyola de Protecció de Dades ha sancionat en nombroses ocasions els serveis de salut de diferents comunitats autònomes on feia feina un professional que va accedir indegudament a la història clínica d'un usuari en entendre que, com a responsable del tractament, no havia establert les mesures de seguretat adequades per evitar-ho.
>
> [...] A més, cal assenyalar que el professional sanitari que accedeix il·lícitament a dades de salut pot incórrer en un delicte de descobriment i revelació de secrets, previst i penat en el Codi penal. Una sentència del Tribunal Suprem (n'hi ha diverses) va ratificar la condemna a un metge que va accedir a les històries de pacients dels seus col·legues del centre de salut sense que fossin pacients seus.

11) És factible facilitar dades de salut d'un pacient i dels seus fills a la Comissió de Tutela del Menor?

Sí, sempre que ho hagi autoritzat el responsable del tractament, perquè hi ha habilitació legal.

12) Han de constar els comunicats mèdics de lesions dins la història clínica d'un pacient?

Tal com la defineix la LAP en l'article 3, la història clínica és «el conjunt de documents que contenen les dades, valoracions i informacions de qualsevol índole sobre la situació i l'evolució clínica d'un pacient al llarg del procés assistencial». I en l'article 15 estableix que ha d'incorporar la informació que es consideri transcendental per al coneixement veraç i actualitzat de l'estat de salut del pacient, i que té la finalitat

principal de facilitar l'assistència sanitària deixant constància de totes les dades que, sota criteri mèdic, permetin el coneixement veraç i actualitzat de l'estat de salut.

Atès que el comunicat mèdic de lesions és un document de valoració física que aporta informació transcendental per al coneixement veraç de l'estat de salut del pacient, ha de formar part de la història clínica.

13) Si un usuari sol·licita el registre d'accessos anteriors als dos darrers anys, ¿què li han de contestar?

El Servei de Salut estableix un període de retenció dels registres d'accés als sistemes d'història clínica de dos anys, en virtut del requeriment establert pel derogat Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desplegament de la Llei orgànica 15/1999.

Tal com s'especifica en el *Procedimiento de solicitudes de información de registros de acceso*, l'interessat pot especificar en el formulari habilitat a aquest efecte el registre d'accessos a les seves dades personals en un període determinat, però mai més enllà de dos anys des de la data actual. Per tant, cal respondre-li que no es disposa de la informació relacionada amb el registre d'accessos anteriors a aquest termini.

14) Per a les sol·licituds telemàtiques, ¿té la mateixa validesa presentar una fotocòpia del document d'identitat com comparèixer de manera presencial?

Sí, està regulat per la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques, i la Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic.

15) Quin és el període de conservació i retenció de la documentació clínica?

Termini de conservació d'històries clíniques actives

La normativa aplicable és la LAP, l'article 17.1 de la qual determina l'obligació de conservar la documentació clínica durant el temps adequat a cada cas i, com a mínim, cinc anys des de la data de l'alta de cada procés assistencial. En aquest sentit, si el pacient no sol·licita que se suprimeixi certa informació de la seva història clínica, aquesta s'ha de conservar fins que deixi de ser necessària per a processos assistencials futurs.

Així doncs, si a criteri del facultatiu es considera que la informació de la història clínica és rellevant a efectes preventius, assistencials o epidemiològics es pot conservar durant el temps que es consideri oportú, que podria ser tota la vida del pacient.

Termini de conservació d'històries clíniques de pacients que han mort

Després de la defunció del pacient, la informació que conté la història clínica deixa de ser necessària per a la finalitat de prestar-li una assistència sanitària adequada; per tant, s'ha de suprimir una vegada passats cinc anys des de la data de la defunció.

No obstant això, de conformitat amb l'article 17.2 de la LAP hi ha certes excepcions que poden justificar prolongar el termini de conservació quan calgui:

1. A efectes judicials:
   - De conformitat amb la normativa aplicable en matèria de protecció de dades en aquests supòsits, les dades s'han de mantenir degudament blocades durant el termini de prescripció aplicable o fins que acabi el procés judicial o el procediment administratiu corresponents.
   - Amb relació al termini de prescripció en processos judicials sobre responsabilitat civil, és de cinc anys des que es pugui exigir el compliment de l'obligació (article 1964 del Codi civil). No obstant això, si es pren en consideració que les històries clíniques poden ser considerades com a element probatori d'un delicte, també cal tenir en compte la via penal, i llavors s'ha de conservar la documentació clínica com a mínim fins que el delicte hagi prescrit, un termini que pot arribar fins als vint anys, com a màxim (article 131 del Codi penal).
2. Per raons epidemiològiques, de recerca o d'organització i funcionament del Sistema Nacional de Salut: en relació amb aquest supòsit cal tenir en compte que l'article 17.2 de la LAP exigeix que el tractament es faci de manera que s'eviti tant com sigui possible identificar les persones afectades. En aquests casos, la *Guía para pacientes y usuarios de la sanidad* preveu que les dades personals puguin pseudonimitzar-se, és a dir, separar les dades identificatives del pacient de les de salut, encara que es puguin tornar a associar si cal.

Per tot això les històries clíniques dels pacients morts es poden conservar durant més temps. Segons la Comissió Central de Deontologia, tot i que el Codi d'Ètica i Deontologia Mèdica de l'Organització Mèdica Col·legial d'Espanya, igual que altres codis deontològics europeus, no estableix l'extensió temporal del deure dels metges de conservar les històries clíniques dels pacients, aquestes s'han de conservar almenys vint anys des de la defunció del pacient.

Organització de la seguretat

En l'àmbit de l'organització de la seguretat, ¿quines funcions cal atribuir al responsable de seguretat física?

Li correspon impla ntar les mesures de seguretat que siguin competència seva entre les determinades pel responsable de la seguretat de la informació, en concret les següents:

- Informar el responsable de seguretat de la informació sobre el grau d'implantació, l'eficàcia i els incidents relacionats amb les mesures de seguretat físiques.
- Coordinar i controlar les mesures de seguretat física aplicables a les dades de caràcter personal.
- Validar la normativa de seguretat i els procediments de seguretat física.
- Comprovar que les mesures de seguretat físiques establertes siguin adequades per protegir la informació gestionada i els serveis prestats.
- Controlar directament els mecanismes que permeten el control d'accés a les instal·lacions o zones d'accés restringides i impedir que siguin desactivats.
- Donar suport i supervisar la investigació dels incidents relacionats amb la seguretat física des que es notifiquin fins que s'hagin resolt.

Dret a la pròpia imatge i enregistraments

1) Està permès que un usuari faci fotografies d'empleats dins de les instal·lacions d'un centre sanitari per denunciar o presentar una queixa per l'atenció o servei rebuts?

El dret d'imatge que resultaria afectat per la captació de les fotografies està regulat per la Llei orgànica del dret a l'honor, a la intimitat personal i familiar i a la pròpia imatge. Prendre fotografies es considera una intromissió il·legítima en aquest dret —en particular dels empleats que fan feina al centre, extensible també, per exemple, a usuaris, familiars de pacients, etc.— quan el titular del dret (és a dir, l'empleat fotografiat) no hagi donat consentiment expressament per fer-li fotografies, llevat de les excepcions previstes per la Llei:

a) Persones que ocupin un càrrec públic o una professió de notorietat o projecció pública, sempre que la imatge es capti durant un acte públic o a llocs oberts al públic.

b) En els casos d'informació gràfica sobre un succés o esdeveniment públic, si la imatge d'una persona determinada hi apareix com a merament accessòria.

Com que *a priori* no es pot saber si es tracta d'un dels dos supòsits excepcionals, prendre aquestes fotografies és una intromissió il·legítima en el dret a la pròpia imatge de la persona afectada, i per això està prohibit.

Així mateix, l'AEPD manifesta que «sembla difícil entendre que la captació d'imatges o vídeos per particulars dels empleats públics es faci en l'àmbit de l'esfera íntima d'aquells particulars, en les relacions familiars o d'amistat. Només el fet que els enregistraments es facin en l'àmbit laboral, al lloc on els empleats públics presten servei, i sense cap relació amb ells que excedeixi la purament professional, sembla portar-nos a la conclusió que en el supòsit plantejat no és aplicable l'excepció domèstica. En definitiva, si les imatges captades o gravades per particulars no es refereixen a la seva esfera més íntima, seran aplicable les normes sobre protecció de dades personals, tant per obtenir la imatge com per difondre-la o publicar-la posteriorment» [traducció de l'original]. Si les imatges s'utilitzen per a finalitats concretes —per presentar denúncies en expedients disciplinaris o fins i tot penals contra determinats empleats públics, o per difondre-les per internet, per exemple— cal actuar de la manera següent:

- Complir el principi de transparència i informació, de conformitat amb l'article 11 de la LOPDGDD, informant l'interessat sobre el tractament que s'aplicarà a les dades que li concerneixin (finalitat del tractament i altres aspectes indicats en l'apartat 2 de l'article citat).
- Complir el principi de minimització de les dades establert en l'article 5.1.*c)* de l'RGPD, que determina que les dades personals han de ser adequades, pertinents i limitades a allò necessari amb relació a les finalitats per a les quals són tractades; per tant, la finalitat de la captació ha d'existir i ha de ser legítima; en cas contrari, no es pot dur a terme el tractament.
- Tractar les dades lícitament, de conformitat amb l'article 6 de l'RGPD, sol·licitant el consentiment per a finalitats específiques.

2) Està permès enregistrar converses amb el personal del centre sanitari?

De conformitat amb la jurisprudència, cal distingir dos supòsits: d'una banda, l'enregistrament d'una conversa d'altres persones i, d'una altra, l'enregistrament d'una conversa mantinguda amb altres persones. En el segon cas no s'infringeix el secret de les comunicacions. En concret, segons han exposat diverses sentències, «l'enregistrament d'una conversa privada per un interlocutor que hi participa no es pot considerar obtinguda il·lícitament perquè no poden vulnerar el dret del secret de les comunicacions aquest que són destinataris d'aquelles» (Sentència del Tribunal Suprem 652/2016) [traducció de l'original].

Això no obstant, encara que sigui legal que algun dels interlocutors d'una conversa l'enregistri sense el consentiment dels altres, difondre-la sense el consentiment d'aquests sí que és una conducta delictiva. En aquest sentit s'ha pronunciat el Tribunal Suprem (STS 652/2016): «L'acte de l'enregistrament per un dels interlocutors de la conversa no conculca cap secret imposat per l'article 18.3 i tan sols, per ventura, es podria concebre com a conducta preparatòria per a la ulterior difusió del que ha enregistrat. Quant a l'última dimensió del comportament considerat, és també clar que la contravenció constitucional només es podria entendre materialitzada pel fet mateix de la difusió (article 18.1 CE)» [traducció de l'original].

Així doncs, per difondre enregistraments fets a professionals dels centres sanitaris del Servei de Salut se'n necessita prèviament el consentiment; en cas contrari seria una vulneració del dret a l'honor i a la intimitat. D'aquesta manera, els professionals sanitaris no es poden negar que els seus pacients gravin les converses que mantenen amb ells, però sí es poden negar que aquestes es difonguin.

No obstant això, cal tenir en compte que aquests enregistraments —en els quals la persona que grava és part de l'enregistrament— es poden utilitzar com a mitjà probatori en un procediment judicial.

En tots dos supòsits, el personal sanitari no es pot negar a prestar l'assistència mèdica.

3) Es poden publicar en un blog d'internet fotografies de pacients o usuaris preses dins les instal·lacions d'un centre sanitari?

El dret d'imatge que resultaria afectat per la captació de les fotografies està regulat per la Llei orgànica del dret a l'honor, a la intimitat personal i familiar i a la pròpia imatge, de manera que el supòsit plantejat seria una intromissió il·legítima en aquest dret si el titular del dret (en aquest cas, el pacient afectat o qualsevol altra persona que aparegui en la fotografia) no hagi donat consentiment expressament perquè es prengui i es publiqui. Fins i tot si la fotografia està presa durant una activitat que formi part d'un programa o una iniciativa del centre —en aquest cas seria el centre qui incorreria en responsabilitat per la intromissió— és necessari el consentiment exprés de les persones que apareixen en la fotografia. No obstant això, donar aquest consentiment és revocable; per tant, també cal retirar les fotografies de les persones que, fins i to havent consentit que es publiquin, expressin oposició a mantenir-les publicades.

D'altra banda, si es tracta d'activitats o iniciatives privades —que es desenvolupen en l'àmbit exclusivament personal o domèstic d'un grup de persones— convé advertir de la conveniència de retirar les fotografies publicades sense el consentiment exprés de les persones que hi apareguin, sobretot en els casos en què alguna hagi manifestat oposició a publicar-les.

4) Es poden instal·lar càmeres de videovigilància en un centre sanitari?

Solen ser als llocs d'accés, als passadissos i a les sales, però no dins les consultes.

Les càmeres de videovigilància tenen la finalitat de garantir la seguretat de les persones i de les instal·lacions; per tant, es poden instal·lar sempre que se n'informi (habitualment amb un cartell). Es pot sol·licitar informació de les finalitats de les càmeres, durant quant de temps es conserven els enregistraments, sobre la possibilitat d'exercir els drets corresponents i sobre el responsable de la instal·lació.

5) Es pot instal·lar una càmera web per observar una sala de pacients psiquiàtrics per valorar-ne el nivell d'agressivitat?

D'acord amb el *Procedimiento de adecuación del tratamiento de sistemas de videovigilancia del Servicio de Salud*, per instal·lar càmeres de videovigilància cal examinar de manera crítica si és adequat per assolir l'objectiu i si és necessari en relació amb aquest objectiu.

En aquest sentit, instal·lar una càmera web en una sala de pacients psiquiàtrics per evitar agressions s'emmarca en la finalitat de preservar la seguretat de les persones i dels béns i les instal·lacions. Per tant, en principi s'hi pot instal·lar una càmera web.

Per considerar si la videovigilància és una mesura apropiada, necessària i proporcional cal comprovar si es compleixen els requisits següents:

- Si la mesura és susceptible d'aconseguir l'objectiu proposat (judici d'idoneïtat).
- Si, a més, és necessària, en el sentit que no hi hagi una altra mesura més moderada per aconseguir l'objectiu amb la mateixa eficàcia (judici de necessitat).
- Si és ponderada o equilibrada pel fet de derivar-se'n més beneficis o avantatges per a l'interès general que perjudicis sobre altres béns o valors en conflicte (judici de proporcionalitat en sentit estricte).

El dubte és si és possible observar els pacients psiquiàtrics per altres mitjans, com ara a través d'un vidre-mirall des d'una sala contigua. Si es pot instal·lar aquest sistema o un altre de similar, es recomana vigilar la sala d'aquesta manera, perquè no suposa un tractament de dades de caràcter personal. Si no és possible, l'alternativa seria la càmera web tenint en compte que, tant si es visualitzen les imatges en temps real com si es graven, suposa un tractament de dades personals, del qual cal informar per mitjà dels cartells oportuns: exposats en llocs visibles i notificant el tractament, la identitat del responsable i la possibilitat d'exercir els drets de protecció de dades.

6) Es pot accedir a enregistraments captats per càmeres de videovigilància quan es tenguin sospites d'algun incident (p. ex., trencament d'una porta)?

Segons el *Procedimiento de adecuación del tratamiento de videovigilancia del Servicio de Salud*, el responsable de tractament pot accedir als enregistraments en vídeo sempre que estigui legítimament justificat i que la finalitat sigui la mateixa per la qual es van recollir les dades. Es pot considerar l'exemple plantejat en l'enunciat de la pregunta com a legítim i amb la mateixa finalitat (preservar la seguretat de les persones, els béns i les instal·lacions).

7) Pot l'interessat sol·licitar l'accés als enregistraments de càmeres de videovigilància en els quals aparegui? En cas afirmatiu, en quines condicions?

D'acord amb el *Procedimiento de adecuación del tratamiento de videovigilancia del Servicio de Salud.* si un interessat —com a particular— sol·licita una còpia de les dades, el responsable del tractament ha de tenir en compte que en alguns casos pot suposar la vulneració dels drets d'altres persones que també apareguin en els enregistraments. Per això, en aquest cas cal prendre les mesures oportunes per entregar únicament enregistraments en els quals no es pugui identificar altres persones físiques o bé emmascarar-ne la cara perquè no siguin identificables.

Si cal saber la identitat d'una altra persona per poder dur a terme determinades accions judicials i/o contractuals, l'accés a les imatges està legitimat sempre que la finalitat de la comunicació de les dades sigui compatible amb la finalitat per a la qual es van recollir. Per exemple, si el sistema de videovigilància està instal·lat amb finalitats de seguretat, es poden cedir imatges si l'interès legítim invocat pel sol·licitant es refereix a l'exercici del dret fonamental a la tutela judicial efectiva, en la mesura que les imatges s'utilitzaran per obtenir proves per formular una denúncia per delicte o una reclamació per responsabilitat contractual o extracontractual a una companyia d'assegurances, perquè seria compatible amb la finalitat inicial.

8) Què es pot fer si, en un acte al centre sanitari amb públic, un usuari és gravat per algun assistent però aquell (o el seu tutor) no ha donat consentiment per al tractament de les imatges?

Es recomana que, en aquests actes, el centre sanitari informi sobre la possibilitat que els assistents prenguin imatges per a ús domèstic, cosa que està fora de l'àmbit d'aplicació de l'RGPD segons el seu article 2.2.*c)*, que estableix la inaplicabilitat d'aquesta norma al tractament de dades personals recollides per una persona física en l'exercici d'activitats exclusivament personals o domèstiques. Igualment és una bona pràctica informar abans de començar l'acte (per exemple, amb cartells) que l'enregistrament només es pot reproduir en l'àmbit domèstic (activitats privades, familiars i d'amistat) i no públicament.

Addicionalment, si es tracta d'activitats o iniciatives privades —en el sentit que es facin en l'àmbit exclusivament personal o domèstic d'un grup de persones—, cal advertir-los que convé retirar les imatges publicades sense el consentiment exprés de les persones que hi apareixen, especialment si alguna ha manifestat oposició a publicar-les.

9) Si, en un acte al centre sanitari amb públic, el personal del centre capta imatges dels assistents, ¿es poden publicar en un blog d'internet?

Sempre cal informar els assistents (o els seus representants legals o tutors en cas d'incapacitació legal d'aquells) sobre la finalitat de la captació de les imatges i de la difusió que se'n pretén fer, és a dir, si es publicaran a internet (web, xarxes socials...) o en qualsevol altre mitjà de publicació, i demanar-lo el consentiment inequívoc i explícit.

El dret d'imatge que seria afectat si es publiquen aquestes imatges està regulat en la Llei orgànica del dret a l'honor, a la intimitat personal i familiar i a la pròpia imatge. Captar i difondre imatges es considerarà una intromissió il·legítima en aquest dret si el titular del dret (en aquest cas, qualsevol persona que aparegui en les imatges) no ha donat consentiment exprés per prendre-les i publicar-les. En aquest sentit, si l'acte forma part d'un programa o iniciativa del centre —en aquest cas, seria el centre qui

incorreria en responsabilitat per la intromissió— cal tenir el consentiment exprés de les persones que apareguin en les imatges. No obstant això, el consentiment és revocable; per tant, també cal retirar les imatges de les persones que, fins i tot havent-ne consentit la publicació, expressin oposició a mantenir-les publicades.

Si no s'obté el consentiment o es denega, d'acord amb el *Plan de inspección de oficio de la atención sociosanitaria*, de l'AEPD, cal publicar les imatges de manera que no sigui possible identificar les persones que hi apareixen (per exemple, pixelant-les).

10) Es poden instal·lar càmeres de videovigilància dins les ambulàncies?

Si s'hi instal·len amb la finalitat de vigilància i seguretat de persones, béns i instal·lacions, és el mateix tractament de la videovigilància, per la qual cosa es poden instal·lar a aquest efecte, tal com recull el *Procedimiento de adecuación del tratamiento de videovigilancia del Servicio de Salud*.

Si es requereix videovigilància amb una altra finalitat, cal valorar la necessitat de la instal·lació i la base legal per al tractament. Per això recomanam contactar amb l'Oficina de Seguretat (*seguretat@ibsalut.es*).

11) Quina és la finalitat del tractament de dades personals recollides per càmeres tèrmiques?

En la presa de la temperatura per mitjà de càmeres tèrmiques no es registren ni emmagatzemen en cap sistema dades sobre la temperatura corporal. Si es detecta que una persona té una temperatura elevada i aquesta acudeix al centre sanitari com a pacient, les dades relacionades amb la seva temperatura corporal seran registrades en la seva història clínica per garantir una assistència sanitària correcta.

Altres preguntes

1) Com es pot classificar la documentació confidencial a l'efecte de destruir-la i/o reciclar-la?

Amb caràcter general, es pot diferenciar entre *informació pública* (informació publicada a la disposició del públic) i *informació confidencial*, classificada en tres nivells: ús intern, ús restringit i ús altament restringit. Tan sols en el cas de la informació pública no s'estableixen restriccions pel que fa al tractament, les còpies o el reciclatge. Per a la resta de la informació, sí que cal seguir allò que estipula el *Procedimiento de destrucción de documentos y soportes con datos personales del Servicio de Salud de las Islas Baleares*.

2) Quines dades es poden publicar en el cens d'electors en unes eleccions sindicals?

L'article 44 de l'Estatut bàsic de l'empleat públic regula el procediment per a l'elecció de les juntes de personal i delegats de personal i estableix els criteris generals següents:

- Són electors i elegibles els funcionaris que estiguin en la situació de servei actiu. No tenen la consideració d'electors ni elegibles els funcionaris que ocupin llocs el nomenament dels quals s'efectuï per mitjà de reial decret o per decret dels consells de govern de les comunitats autònomes i de les ciutats de Ceuta i Melilla.
- Poden presentar candidatures les organitzacions sindicals legalment constituïdes o les coalicions d'aquestes, i els grups d'electors d'una mateixa unitat electoral, sempre que el nombre sigui equivalent, almenys, al triple dels membres que s'hagin d'elegir.

- Les juntes de personal són elegides per mitjà de llistes tancades, per mitjà d'un sistema proporcional corregit; i els delegats de personal són elegits per mitjà de llistes obertes i sistema majoritari.

  Així mateix, l'article 43 —relatiu a la promoció d'eleccions a delegats i juntes de personal— estableix que «els legitimats per promoure eleccions tenen dret, a aquest efecte, que l'Administració pública corresponent els subministri el cens de personal de les unitats electorals afectades, distribuït per organismes o centres de treball».

  En aquesta normativa no es regula el contingut de la llista del cens electoral. No obstant això, l'article 6 del Reglament d'eleccions a òrgans de representació dels treballadors en l'empresa estableix el contingut del cens laboral, en el qual han de constar, de tots els treballadors, el nom i els llinatges, el sexe, la data de naixement, el número del document d'identitat, la categoria o el grup professional i l'antiguitat a l'empresa.

  Així mateix, tenint en compte que en l'article 1.2 de la Llei orgànica 11/1985, de 2 d'agost, de llibertat sindical, es considera que són *treballadors* tant els que siguin subjectes d'una relació laboral com els que ho siguin d'una relació de caràcter administratiu o estatutari al servei de les administracions públiques, s'hi podria comparar el contingut mínim exigit en els censos laborals d'eleccions a òrgans de representació dels treballadors en empreses els que facin feina en el sector públic.

  En aquest sentit, l'AEPD determina que aquest cens laboral s'ha d'ajustar al modelo núm. 2 de l'annex del Reglament d'eleccions a òrgans de representació dels treballadors en l'empresa —publicat per mitjà del Reial decret 1844/1994, de 9 de setembre—, en el qual es detallen les dades personals pertinents per a aquesta finalitat (Resolució R/00485/2009, de 16 de març, en el procediment de declaració d'infracció d'administracions públiques AP/00059/2008, instruït a l'entitat Gerència d'Atenció Primària 061 Illes Balears).

  Així mateix, cal tenir en compte el principi de minimització de les dades, descrit en l'article 5 de l'RGPD, en el qual s'assenyala que les dades han de ser adequades, pertinents i limitades a allò necessari en relació amb les finalitats per a les quals són tractades.

3) És legítim que comerços, centres de treball i altres establiments prenguin la temperatura corporal dels seus clients o usuaris?

Prendre la temperatura corporal és un tractament de dades personals, i per això es regeix pels principis establerts en el RGPD:

- Licitud, lleialtat i transparència: el tractament s'ha de basar en una causa legitimadora de les previstes en la normativa de protecció de dades per a les categories especials de dades (articles 6.1 i 9.2 de l'RGPD). Aquesta base jurídica s'ha d'analitzar en cada cas i pot ser diferent en cada àmbit, però així i tot mai es pot basar en el consentiment de l'interessat, perquè les persones no es poden negar que se'ls prengui la temperatura corporal sense perdre per això la possibilitat d'entrar en un centre de treball, en altres establiments o en mitjans de transport.

- Limitació de la finalitat i minimització de les dades: les dades sobre la temperatura corporal només es poden obtenir amb la finalitat específica de detectar possibles persones contagiades i evitar que accedeixin a un lloc determinat i hi contactin amb altres persones. Aquestes dades han de ser adequades, pertinents i limitades a allò necessari en relació amb les finalitats per a les quals són tractades, i no es poden utilitzar per a cap altra finalitat. Això és especialment aplicable en els casos en què la temperatura corporal es prengui amb algun dispositiu que puguin gravar i conservar les dades (com ara les càmeres tèrmiques) o tractar informació addicional (en particular, informació biomètrica).
- Exactitud: els equips de mesurament de la temperatura corporal han de ser adequats per registrar amb fiabilitat els intervals de temperatura que es considerin rellevants.
- Limitació del termini de conservació: és important establir terminis i criteris de conservació de les dades en els casos registrats. Segons l'AEPD, no s'han de conservar llevat que es pugui justificar suficientment per la necessitat de respondre a eventuals accions legals derivades de la decisió de denegar l'accés a una persona per haver-se negat que li prenguin la temperatura corporal.

  Així mateix, cal tenir en compte les mesures relatives a la informació als treballadors, clients o usuaris sobre aquests tractaments, en particular si s'enregistrarà i es conservarà la informació, i altres mesures per permetre que les persones en les quals s'hagi detectat una temperatura superior a la normal puguin reaccionar a la decisió d'impedir-los accedir a un recinte (per exemple, justificant que la seva temperatura elevada és deguda a una altra raó).

4) Es poden posar cartells amb el nom i els llinatges dels usuaris d'un centre sanitari a la porta de les habitacions perquè no s'extraviïn o entrin per error dins una altra habitació i per facilitar les visites? Es poden posar cartells a les taules del menjador amb la identificació (nom i llinatges o fotografia) dels usuaris i informació sobre les al·lèrgies que pateixen o sobre si tenen disfàgia o altres característiques especialment rellevants per a les menjades?

Cal valorar la necessitat d'identificar els pacients o exposar les dades referides en els diferents moments de la prestació del servei, sempre considerant altres mesures menys intrusives per a la privadesa i que ofereixin garanties de seguretat equivalents. Per exemple, es podria valorar l'alternativa de posar el número de l'habitació en una fitxa o un distintiu que l'usuari dugui damunt.

Sobre la informació que es pot mostrar al menjador a què es refereix la pregunta, ha de ser la mínima necessària per permetre administrar de manera segura aliments o medicaments, però cal valorar les alternatives que permetin que la informació estigui exclusivament a la disposició dels treballadors del menjador.

5) Es pot comprovar la col·legiació dels treballadors d'un centre consultant el seu col·legi professional?

Sí, sempre que la col·legiació sigui obligatòria per acomplir l'activitat laboral. Aquest tractament està emparat per la Llei 2/1974, de 13 de febrer, de col·legis professionals.

6) Es poden considerar segurs els mitjans electrònics?

Sí, perquè estan regulats per la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques, i la Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic.