

Codi de bones pràctiques en destrucció de documents, dades i suports en centres sanitaris

Comissió Tècnica
en Matèria de
**Documentació
Clínica**



Desembre de 2019



Generalitat de Catalunya
Departament de Salut

S/Sistema de
Salut de Catalunya

Direcció o Coordinació:**Autors o redactors:**

© 2019, Comissió Tècnica en Matèria de Documentació Clínica.

Alguns drets reservats

© 2019, Generalitat de Catalunya. Departament de Salut.



Els continguts d'aquesta obra estan subjectes a una llicència de Reconeixement-NoComercial-SenseObresDerivades 4.0 Internacional.

La llicència es pot consultar a la pàgina web de Creative Commons.

Edita:

Secretaria General.

I edició:

Barcelona, desembre de 2019.

Assessorament lingüístic:

Servei de Planificació Lingüística del Departament de Salut

URL:

https://canalsalut.gencat.cat/ca/professionals/consells_i_comissions/comissio_tecnica_en_materia_de_documentacio_clinica/criteris_i_protocols_de_referencia/

Disseny de plantilla accessible:

Oficina de Comunicació. Identitat Corporativa.

Sumari

1	Objecte i abast.....	4
2	Confidencialitat de la informació.....	4
3	Requeriments	5
3.1	Plantejament.....	5
3.2	Tipus d'empresa	6
3.3	Tipus de suport.....	6
3.4	Dotació de recursos.....	6
3.5	Recursos humans.....	7
3.6	Transport	8
3.7	Centre de destrucció	8

1 Objecte i abast

L'objectiu bàsic d'aquest *Codi de bones pràctiques en destrucció de documents, dades i suports en centres sanitaris* és garantir una gestió adequada del procés d'eliminació atès que la informació sanitària conté dades de caràcter personal o confidencial, mitjançant l'establiment dels requeriments que han d'observar els serveis de conservació, recollida, transport, emmagatzematge, destrucció d'informació amb dades personals i gestió posterior dels residus generats per l'activitat desenvolupada en els centres sanitaris.

S'entén per gestió adequada de la informació de dades de caràcter personal i confidencial dotar de mitjans tècnics i legals per donar compliment al Reglament general de protecció de dades (UE) i a la normativa estatal, la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals.

2 Confidencialitat de la informació

Quan parlem de *confidencialitat*, ens estem referint a la propietat o característica de la informació que fa referència o pertany a una persona física o jurídica, segons la qual no pot posar-se a disposició de persones, entitats o processos no autoritzats ni revelar-se a tercers no autoritzats.

Tant la generació i conservació de la informació com, si escau, la destrucció, han de complir la normativa de gestió documental i arxiu (Llei 10/2001, de 13 de juliol, d'arxius i gestió de documents, i els reglaments que la despleguen), així com les previsions que conté la normativa de protecció de dades (Reglament europeu de protecció de dades de caràcter personal i Llei orgànica de protecció de dades).

En aquest sentit, s'ha de garantir la seguretat i confidencialitat durant tots aquests processos, de manera que si un centre sanitari ha respectat aquestes mesures en les etapes de generació i conservació, i ha de confiar a un tercer la darrera fase de destrucció confidencial, s'ha d'assegurar que aquest últim reuneix les condicions exigides legalment per garantir la seguretat i confidencialitat de la informació.

Així doncs, les exigències de protecció de la informació personal i les necessitats de salvaguardar la reputació corporativa fan que la destrucció documental confidencial representi una part essencial en la vida productiva dels centres sanitaris.

D'altra banda, la conservació de dades més enllà del temps estrictament necessari genera despeses de conservació innecessàries a més d'exposar el centre sanitari a possibles robatoris, ús indegut, divulgació i en suma a sancions per part de les autoritats de protecció de dades (APDCAT i AEPD).

Actualment, la normativa nacional en la matèria, transposada de l'europea, és molt estricta al respecte, i exigeix alts nivells de seguretat en la destrucció de documents no només en suport paper, sinó també de la informació continguda en plàstics, microfibras, formats d'emmagatzematge òptics (CE, CD-RW, DVD d'alta definició, VMD i Blu-ray), cintes de vídeo, memòries USB, discos externs i interns, telèfons mòbils, PDA, etc.

D'acord amb això, la destrucció de dades de caràcter personal en un entorn segur s'ha de convertir en una prioritat en la planificació i integració d'aquestes dades en els processos de gestió diària dels centres sanitaris, i constituir un requisit indispensable per al manteniment dels drets de l'usuari dels serveis assistencials.

3 Requeriments

3.1 Plantejament

Atès que la majoria de centres sanitaris realitzen les destruccions de dades mitjançant la contractació d'una empresa de serveis externa, en primer lloc, s'ha de definir l'objecte del servei:

- Establir els requisits tècnics, organitzatius i logístics que han d'observar els serveis de recollida, transport, emmagatzematge, destrucció de la informació i gestió dels residus generats.

En general, les característiques del servei de destrucció confidencial de documents haurien de preveure:

- a) L'acord de les necessitats.
- b) El subministrament de contenidors per a documents, dades i suports.
- c) La retirada periòdica dels contenidors i/o el contingut segons la periodicitat pactada.
- d) El trasllat de la documentació al centre de destrucció o destrucció in situ.
- e) La destrucció dels documents de manera que no en sigui possible la recuperació posterior.
- f) La garantia i traçabilitat documental d'origen, recorregut i destrucció dels documents dipositats en els contenidors des dels centres sanitaris.
- g) L'emissió del certificat de destrucció corresponent.

Una ajuda molt interessant que cal tenir en compte és la Norma UNE-EN 15713:2010 Destrucció segura de material confidencial. Codi de bones pràctiques, atès que és un bon recull de criteris i recomanacions per a una eliminació segura de documents i dades.

3.2 Tipus d'empresa

Pel que fa a l'empresa que es contracti, s'ha d'establir:

- El contracte de cessió i l'encàrrec de gestió de la informació de caràcter personal mitjançant el qual l'empresa adjudicatària adquireix el compromís contractual com a encarregada del tractament de la informació que contingui dades de caràcter personal (independentment del suport) una vegada retirada. Aquest contracte ha d'assegurar la responsabilitat de l'empresa adjudicatària a l'efecte de la cessió de dades de caràcter personal. El contracte de confidencialitat i privacitat que han de signar totes les persones que prestin serveis per a l'empresa adjudicatària i que intervinguin en algun dels procediments de recollida, gestió o destrucció de la informació del centre sanitari.
- El certificat d'empresa gestora de residus.
- La valoració del compliment i la certificació de la Norma ISO/IEC 27001:2005 -seguretat de la informació.

3.3 Tipus de suport

A continuació, cal considerar els tipus de suport que cal tractar:

- Paper amb dades confidencials.
- Suports electrònics (CD, DVD, cintes, etc.).
- Altres materials informàtics (discs durs, etc.).
- Radiografies (excloses les radiografies obtingudes mitjançant tècniques de revelat a l'aigua, les quals, per la seva condició de residu tòxic i perillós, s'han de gestionar per altres sistemes).

3.4 Dotació de recursos

Pel que fa a la dotació de recursos materials, s'ha de valorar:

- L'especificació de la dotació i instal·lació de contenidors amb tots els requisits de seguretat (tancats i precintats), en els quals s'ha de dipositar tota la documentació susceptible de destruir-se.
- L'especificació dels tipus de contenidors o elements de recollida i emmagatzematge de documentació confidencial:
 - Capacitat expressada en volum de litres.

- Dimensions adients a les necessitats i espais del centre sanitari o àrees. S'ha de valorar la relació volum (capacitat) i superfície ocupada en planta (m²).
- Els contenidors han de ser rígids.
- El tipus de material:
 - Plàstic.
 - Metàl·lic.
 - Altres de similar resistència.
- No s'han d'admetre contenidors o dipòsits de materials fàcilment deformables o perforables (cartró o similars).
- La descripció del tipus de bossa, pany, brida de seguretat, etc.
- El sistema de tancament i precinte ha d'evitar l'accés a la documentació emmagatzemada. En cas de brida de seguretat, cal especificar si és numerada o no.
- El sistema o mecanisme d'introducció de la documentació s'ha dissenyat de manera que no es pugui extreure l'extracció de la documentació.
- Els contenidors han d'estar identificats correctament com a punts de recollida i emmagatzematge de documentació confidencial.
- Quan el contenidor està ple, es realitza o programa la recollida i el transport fins al lloc on s'ha de fer la destrucció completa.
- Depenent del volum de documentació per destruir, es poden recollir altres tipus de mides o suports (palets, caixes en prestatgeries, etc.).

En cas de licitació, és convenient que les empreses licitadores presentin mostres dels contenidors i tots els altres elements que s'utilitzaran en la recollida i el transport de la documentació, informació i dades confidencials.

També s'ha de tenir present que el disseny del procés de gestió no alteri el funcionament normal de l'activitat de l'àrea o servei del centre sanitari.

3.5 Recursos humans

Pel que fa al personal de recollida i transport, els requeriments haurien de ser:

- El personal de recollida i transport s'ha d'identificar en cada servei o àrea abans d'obrir el contenidor o canviar-lo.
- A continuació, s'ha d'obrir el contenidor per treure la documentació confidencial o canviar-lo per un de buit.
- A l'efecte de garantir en tot moment el control i la traçabilitat de la documentació retirada, el transport dins del centre sanitari s'ha de fer de forma separada i individualitzada, de manera que, en tot moment, es pugui identificar la procedència exacta dels documents.
- En qualsevol cas, els contenidors de recollida i/o transport han de disposar d'un sistema de tancament segur que permeti detectar fàcilment qualsevol intent d'accés o manipulació.

- El personal de recollida i transport ha d'estendre un justificant (albarà o similar) amb el contingut dels contenidors retirats indicant:
 - El servei o àrea, i si s'escau, edifici i planta.
 - El nombre de contenidors retirats especificant els tipus.
 - La signatura del responsable o segell del servei/àrea.
 - La conformitat del responsable de recollida.
- El personal de recollida i transport ha de traslladar els contenidors i altres elements fins al vehicle de transport, sense abandonar-los ni deixar-los sense vigilància.
- Pel que fa al vehicle, aquest ha de romandre tancat al llarg de l'estaca al centre sanitari.

3.6 Transport

Pel que fa als vehicles destinats al transport:

- Els vehicles destinats al transport fins a les instal·lacions de destrucció han de presentar característiques que donin garanties d'un emmagatzemament i transport tancats i sense possibilitat de sostracció o pèrdua de documents.
- La relació de vehicles ha d'incloure les característiques dels vehicles relatius a la seguretat de la informació en la fase de transport (sistemes de seguiment, coordinació i sistemes de comunicació amb la planta de destinació, sistemes d'alarma, d'immobilització, etc.).
- Per tant, la recollida dels contenidors s'hauria de fer mitjançant vehicles rígids, tancats i geolocalitzables al llarg de tot el trajecte.

Altres qüestions que cal valorar al llarg del procediment de treball:

- La freqüència o periodicitat de les visites als punts de recollida de documents, dades i suports.
- Els tipus de comprovacions per fer en cada visita.
- La metodologia per a la mobilització i reposició dels contenidors.
- Les rutes internes de mobilització dels contenidors.
- Els processos de comunicació amb els responsables o coordinadors dels centres o serveis.
- La documentació de seguiment. L'informe detallat i mostra de: albarà de retirada, transport, certificat de destrucció, traçabilitat de les accions, sistema de control de pesos, sistema de control de signatures, etc.

3.7 Centre de destrucció

Pel que fa al centre de destrucció, s'haurien de tenir presents les recomanacions següents:

- L'especificitat de les instal·lacions on s'han de rebre els contenidors amb

la documentació i on s'ha de destruir.

- El detall del procés de destrucció: ubicació de l'espai, si està protegit o no; si la destrucció és amb demora temporal o sense; si la documentació es barreja o no amb els d'altres companyies, si hi ha classificació prèvia o no per qualitat del residu.
- L'especificació de les mesures de seguretat existent en el centre de destrucció: personal de vigilància, contracte amb companyia de seguretat, etc.
- La valoració d'un pla de contingència que doni garanties addicionals de continuïtat del servei en cas de paralització de les instal·lacions de tractament i destrucció de les dades de caràcter personal objecte del contracte.
- La valoració d'una assegurança específica de protecció de dades amb cobertura pel pagament de sancions per incompliment del contracte i de la normativa en matèria de protecció de dades de caràcter personal.
- L'empresa adjudicatària ha d'elaborar un informe mensual, semestral o anual amb el resum del servei, incidències ocorregudes, nombre de retirades, volum, etc.
- S'ha de valorar que aquesta informació sigui facilitada per una plataforma informàtica via web o mitjançant un altre sistema de comunicació i consulta que permeti el seguiment del contracte amb les dades següents:
 - El nombre de contenidors fixos (amb especificació del tipus) distribuïts per cada centre, edifici o servei.
 - El nombre de freqüència de retirada de la documentació.
 - El pes del material retirat per cada centre, edifici o servei per setmana, mes, semestre o any.
 - Altres informacions rellevants.
- L'eina ha de disposar dels sistemes i mecanismes adients de control d'accés i ús (sistema codificat d'accés del personal).
- El compromís de facilitar còpia de la documentació o informes resultants de les auditories internes i externes que l'adjudicatari ha de fer d'acord amb la normativa aplicable.
- La destrucció efectiva en la planta de l'empresa mitjançant el nivell corresponent (de l'1 al 7).
- L'emissió del certificat de destrucció que ha d'incloure les dades del client, volum de destrucció i nivell del tall de destrucció utilitzat.
- La possibilitat de preveure la destrucció de la documentació (en directe, mitjançant presència o enregistrament)
- La garantia de confidencialitat durant tot el procés.

D'altra banda, s'ha de valorar la possibilitat d'auditar i visitar les instal·lacions dels centres de destrucció, amb l'objectiu de comprovar el procés i les mesures de seguretat establertes.