Títol del Projecte Fi de Carrera:

Estudi de la Seguretat i Privadesa dels Historials Mèdics en Format Electrònic

Diego Manuel Moreno Giraldos

Enginyeria en Informàtica

Jordi Castellà Roca

Consultor

Data de Lliurament

5 de Juny de 2011

©Diego Manuel Moreno Giraldos

Reservats tots els drets. Està prohibit la reproducció total o parcial d'aquesta obra per qualsevol mitjà o procediment, compresos la impressió, la reprografia, el microfilm, el tractament informàtic o qualsevol altre sistema, així com la distribució d'exemplars mitjançant lloguer i préstec, sense l'autorització escrita de l'autor o dels límits que autoritzi la Llei de Propietat Intel·lectual.

Dedicatòria i agraïments

Aquesta memòria representa el resultat d'un esforç continuat de molts anys.

Primer amb els estudis d'Enginyeria Tècnica en Informàtica de Gestió i després amb el segon cicle de l'Enginyeria Informàtica.

Durant aquest temps he tingut relació amb molts companys i consultors al llarg de totes les assignatures que he cursat. Aprofito aquest moment per a agrair-los la seva col·laboració.

Vull agrair al consultor Jordi Castellà Roca l'atenció i el suport durant aquests mesos.

També vull agrair a la Universitat Oberta de Catalunya l'oportunitat que ens ofereix d'ampliar la formació acadèmica.

Finalment, vull dedicar el projecte a la meva família, especialment a la meva esposa Isabel i al meu fill Sergio, per la seva paciència i comprensió des que vaig començar els estudis a la UOC.

Resum

El PFC s'emmarca dins de l'àrea de seguretat informàtica.

D'acord amb la legislació, la informació de caràcter personal ha de ser protegida ja que es tracta d'informació molt sensible.

Cal aplicar mesures que garanteixin la seguretat i privadesa de la informació.

En el cas específic de la informació relativa a les dades de salut de les persones, el nivell de protecció ha de ser encara més elevat.

A més, en el cas dels historials mèdics electrònics la informació es transmet per xarxes de comunicacions per la qual cosa cal aplicar mesures addicionals de seguretat per tal de garantir la seguretat i privadesa de la informació.

L'objectiu d'aquest PFC és estudiar la legislació actual i extreure els requeriments de seguretat i privadesa exigits, per tal de determinar el grau de compliment d'aquests requeriments per part de les implementacions existents.

Paraules Clau

Autenticitat

Certificat

Confidencialitat

Control d'accés

Criptografia

HIPAA

Historial Mèdic Electrònic

Integritat

LOPD

PKI

Privadesa

Seguretat

Targeta intel·ligent

Nom de l'àrea de PFC

Seguretat informàtica

Índex de continguts.

Índex de figures.

Índex de taules.

Capítol 1. Introducció.

Societat de la informació.

La progressiva incorporació dels ordinadors a les diferents activitats productives, de creació i lleure, així com l'expansió de les xarxes de comunicacions a tots els àmbits de la vida ciutadana, constitueixen dos fenòmens que visualitzen els canvis que està experimentant la nostra societat.

Aquest conjunt de tecnologies basades en la microelectrònica, la informàtica i les xarxes de comunicacions, és a dir, les tecnologies de la informació i la comunicació (TIC), constitueixen avui un factor de transformació similar al que en el seu moment van tenir la impremta o la màquina de vapor.

Les TIC es materialitzen en nombrosos dispositius i programes que van dels ordinadors personals als telèfons mòbils passant per Internet.

Màquines, xarxes, programes i serveis faciliten la comunicació entre persones i l'accés a ingents quantitats d'informació en format digital.

Si durant la revolució industrial les fàbriques eren el principal motor de creació de riquesa, a l'emergent societat de la informació aquest rol el tenen les xarxes de comunicacions i la capacitat intel·lectual dels ciutadans per transformar la informació en coneixement.

Les xarxes de comunicació ens permeten realitzar algunes activitats amb independència del moment i del lloc on ens trobem. La Universitat Oberta de Catalunya n'és un exemple.

Aquesta alta disponibilitat horària i geogràfica ha ampliat el camp d'aplicació de les noves tecnologies a sectors com l'educació, defensa, sanitat, transport, assegurances, banca, etc.

Un dels camps específics que resulta beneficiat per aquesta situació és el camp de l'assistència mèdica on-line conegut com eSalut. [1]

Internet és una plataforma de comunicacions i d'informació que ha fet accessibles tot tipus de serveis a pràcticament qualsevol punt del planeta i són cada vegada més les línies de negoci a la xarxa que aprofiten els avantatges que ofereix aquest sistema de comunicació:

- Alta disponibilitat horària i geogràfica.
- Resposta immediata.
- Baix cost.
- Interactivitat.

Pas del paper als continguts electrònics.

La societat de la informació afavoreix l'ús de nous suports d'informació com a alternativa al paper. Bàsicament, el terme "oficina sense papers" descriu el procés de transferir arxius del paper a format digital. Això permet incrementar la productivitat i estalviar temps i diners.

Una oficina sense papers evita la pèrdua d'informació en cas de trasllat de documents o en cas d'accidents com incendis, inundacions i altres. Per a això, caldrà portar una bona gestió de les còpies de seguretat i dels procediments de recuperació de dades.

La seguretat també augmenta en una oficina sense papers ja que es pot controlar qui té accés als documents i establir sistemes de jerarquies mitjançant permisos d'accés. Per exemple, és possible fer que un empleat pugui veure i modificar el contingut d'un document, mentre que un altre empleat només pugui veure'l, però no modificar-lo. També és possible adjudicar permisos per veure només una part de la informació, per exemple, dades generals però no dades sensibles.

Un altre avantatge és la reducció dels costós d'impressió, mailing i emmagatzematge de documents en paper. Així, les empreses que adoptin l'oficina sense papers podran millorar els seus serveis ja que es facilita la gestió dels documents.

A més, s'elimina la informació redundant ja que no cal que múltiples departaments o empleats tinguin còpies impreses del mateix document.

També elimina la necessitat de distribuir versions actualitzades ja que, quan s'actualitza un document, la nova versió està immediatament disponible per a qualsevol persona autoritzada.

Cas concret dels historials mèdics.

Fins fa uns anys els hospitals i centres mèdics emmagatzemaven els historials mèdics exclusivament en paper.

Aquesta situació presentava alguns inconvenients: el centre mèdic no podia compartir informació, els pacients no podien accedir als seus historials, moltes vegades s'extraviaven expedients amb la conseqüent pèrdua d'informació. Un altre problema era que els expedients normalment passaven per moltes mans de manera que persones que no eren el metge del pacient podien arribar a veure la informació de l'expedient [2].

La quantitat d'informació que pot acumular un pacient al llarg d'un tractament per una malaltia és molt gran i a més s'ha de tenir tota en compte per a futurs diagnòstics o futures malalties. Un dels grans reptes que s'han plantejat els centres de salut és l'eliminació parcial o completa del paper en les històries clíniques.

Història Clínica Electrònica.

La Història Clínica Electrònica (HCE), també anomenada història mèdica electrònica (HME) o història clínica informatitzada (HCI), és el registre digital de les dades socials, mèdiques i preventives d'un pacient, obtingudes de manera directa o indirecta i actualitzades constantment. En anglès té diverses denominacions: Electronic health record (EHR), Electronic medical record (EMR), Electronic patient record (EPR) o Computerised patient record (CPR) [3] [4].

La història clínica electrònica suposa incorporar les Tecnologies de la Informació i la Comunicació (TIC) en el nucli de l'activitat sanitària. Això porta com a conseqüència que la història deixi de ser un registre de la informació generada en la relació entre un pacient i un professional o un centre sanitari, per formar part d'un sistema integrat d'informació clínica.

La història clínica electrònica és el registre unificat i personal, multimèdia, en què s'arxiva en suport electrònic tota la informació referent al pacient i a la seva atenció. És accessible, amb les limitacions apropiades, en tots els casos en què es precisa assistència clínica (urgències, atenció primària, especialitats, ingressos hospitalaris i altres).

Les dues figures següents mostren dos exemples d'històries clíniques electròniques.

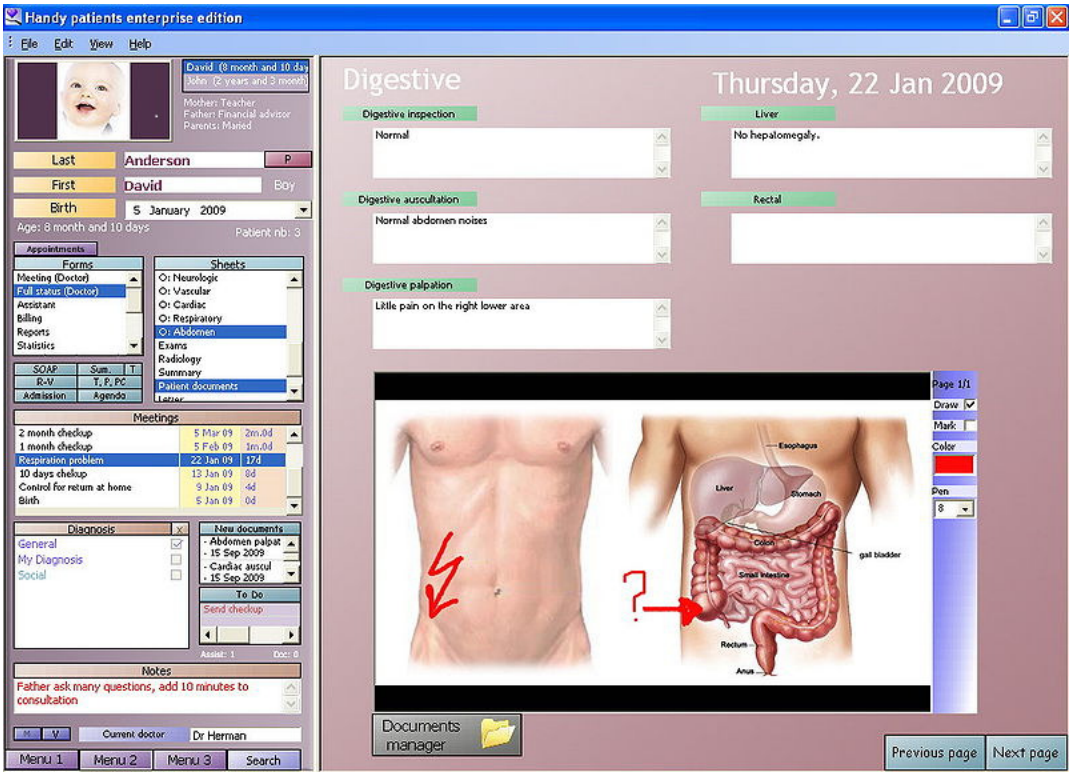

Figura 1. Primer exemple d'història clínica electrònica.

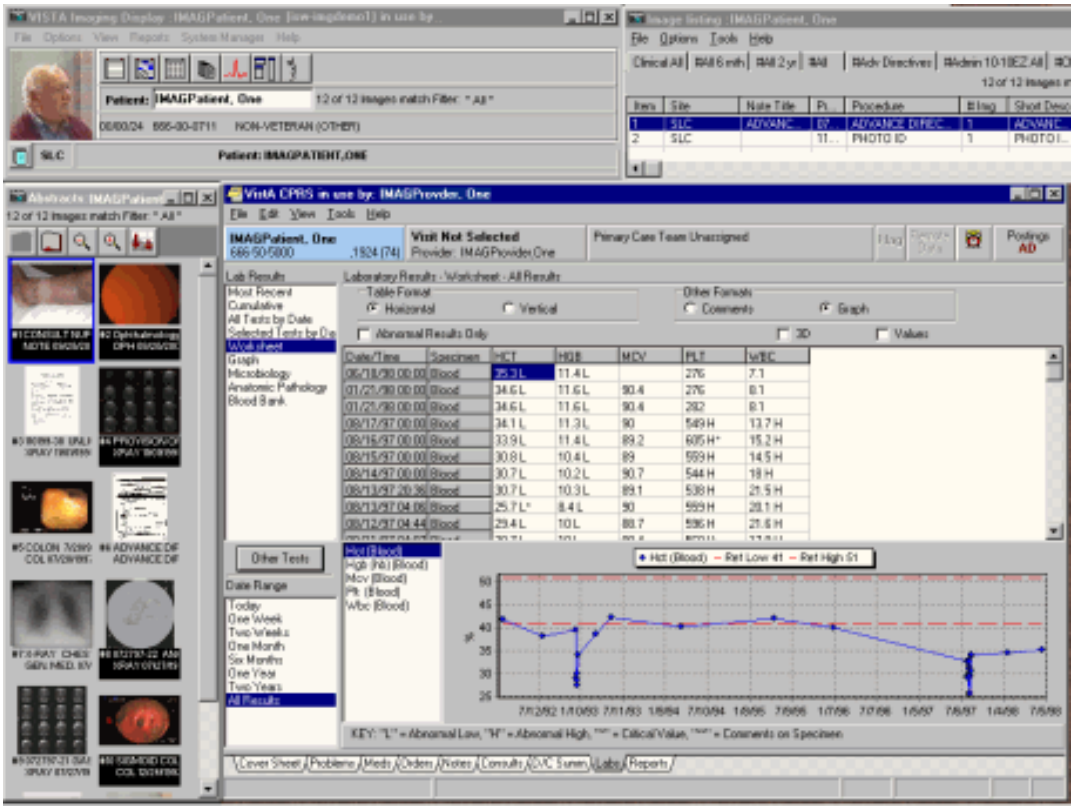

Figura 2. Segon exemple d'història clínica electrònica.

Encara que molts creuen que la creació i l'ús de registres mèdics és molt moderna i que està associada a l'ús de l'ordinador, algunes fonts indiquen que la història clínica es va desenvolupar per primera vegada per Hipòcrates en el segle V aC per a dos objectius: per reflectir amb precisió el curs de la malaltia i per a indicar la causa probable de la malaltia.

Aquests objectius continuen sent adequats, però els sistemes de registres electrònics de salut també poden proporcionar funcionalitat addicional que no es pot fer amb els sistemes basats en paper, com ara la personalització, la conservació i emmagatzematge a llarg termini dels registres, les alertes interactives per als metges, etc.

A causa d'aquests avantatges, a partir de finals de 1960 moltes universitats als Estats Units van començar el desenvolupament de programari per ajudar a la captura i el manteniment de l'HCE.

Per exemple, en la dècada de 1960, el Dr. Lawrence Weed proposa un tipus de sistema de registres mèdics electrònics que va anomenar història clínica orientada als problemes. La seva idea era integrar la informació mèdica dels pacients dels diferents metges per oferir una millor atenció de salut.

A mitjans de la dècada de 1980, l'Institute of Medicine va iniciar un estudi que es va dur a terme per millorar la prestació d'assistència sanitària a causa de la insatisfacció amb el registre mèdic en paper. L'any 1991 es va publicar l'estudi titulat "The computer-based Patient Record:

An essential Technology for Health Care" [5]. Aquest estudi va tenir un efecte fonamental sobre l'avançament de l'HCE.

Posteriorment, l'Institute of Medicine va dur a terme més estudis. El 1999, es va publicar una obra anomenada "To Err is Human: Building a Safer Health System" [6]. Aquest estudi va posar de relleu que moltes persones moren a causa d'errors mèdics. Algunes d'aquestes morts van ocórrer a causa de l'escriptura il·legible del metge, cosa que es podria evitar fàcilment mitjançant l'ús de l'HCE.

Avantatges de tenir els historials en format digital.

La gestió dels historials en format electrònic presenta una sèrie d'avantatges:

- Permet millorar l'eficiència organitzativa, reduir despeses i estalviar temps.
- Permet a un metge consultar l'historial d'un pacient de manera ràpida, en qualsevol moment i des d'una ubicació física diferent on pot estar emmagatzemada la informació. Això pot ajudar al metge a emetre un ràpid diagnòstic i prendre una decisió adequada.
- Incrementa la disponibilitat de la informació, la qual cosa millora la presa de decisió. Això és molt important en el cas d'un servei d'urgències ja que no es pot perdre temps en conèixer informació vital.
- Si l'expedient mèdic està emmagatzemat en un únic lloc i en format electrònic, és més senzilla la seva gestió.
- Permet augmentar la seva seguretat (redundància, còpies de seguretat, etc.), a més dels avantatges respecte a disposar d'aquestes mateixes dades en paper (volum, vulnerabilitat a incendis, inundacions, etc.).
- Un altre avantatge és la centralització de la informació de manera que qualsevol professional pugui consultar tota la informació sense necessitat de demanar-la prèviament.
- Permet aconseguir que la informació que forma part de l'historial de cada pacient no quedi dispersa pels centres mèdics de manera que qualsevol metge, des de qualsevol punt del món on hi hagi una connexió a Internet, pugui consultar l'historial mèdic del pacient que està tractant en aquell moment de forma automàtica i instantània.
- Es pot evitar la pèrdua o duplicació d'informació, i així reduir els errors administratius.
- L'accés a un historial mèdic electrònic és molt útil quan es rep assistència sanitària fora de la residència habitual, en cas de viatge o a l'estranger.
- Si no tenim l'historial mèdic electrònic a l'abast haurem d'explicar personalment els antecedents amb el risc que això suposa d'imprecisions, informació inexacta, etc.

Exemples.

La gestió d'historials mèdics des de la xarxa permet als pacients consultar el seu expedient mèdic des de casa, rebre els resultats de les proves i analítiques, i l'assignació de visites. Aquest fet obre noves portes a la consultoria mèdica i permet un millor servei a domicili. Qualsevol pacient pot ser atès de manera ràpida i precisa sense necessitat de cues.

S'obren noves possibilitats en el camp de la telemedicina, amb la possibilitat de realitzar diagnòstics de forma remota. Podem esmentar alguns exemples:

• un laboratori pot introduir els resultats d'una analítica.

• un radiòleg pot mostrar una radiografia.

• els centres sanitaris poden compartir els historials clínics.

La connexió a Internet amb dispositius mòbils (portàtils, PDAs...), permet tenir la informació de l'expedient mèdic d'una persona per donar servei a un pacient fora de les instal·lacions habituals (a casa del pacient, en cas d'un accident de tràfic, etc.), i augmentar la mobilitat del metge dins de l'entorn habitual de treball sense la necessitat de tenir un ordinador.

Sensibilitat de la informació.

Degut al tipus d'informació i a les repercussions de les accions a prendre pels facultatius, les dades mèdiques tenen un gran valor. Això implica un especial interès per protegir la integritat i l'autenticitat de les mateixes.

La legislació obliga a garantir la confidencialitat, autenticitat, integritat i no repudi de les dades personals emmagatzemades en medis electrònics.

• Confidencialitat: Només el personal autoritzat pot accedir als historials. Ningú a part del pacient o un metge ha de poder veure les dades d'un l'historial.

• Autenticitat. S'ha de garantir la identitat del metge que ha inserit les dades. Ningú ha de poder suplantar la identitat en el nostre sistema, fent-se passar per una altra persona.

• Integritat: Les dades no poden ser modificades sense autorització. En el cas que un usuari maliciós pogués accedir a la base de dades, s'ha de garantir que aquest no podrà modificar la informació o, si més no, detectar que s'ha efectuat una modificació no permesa.

• No-repudi: Les dades inserides per un metge no poden ser repudiades. Cap professional no es podrà desdir del que ha anotat anteriorment en un historial mèdic.

Una manera eficaç de protegir la privadesa de la informació és utilitzar el procediment de dissociació de dades consistent en tractar les dades personals de manera que la informació que s'obtingui no pugui ser associada amb una persona identificada o identificable.

Perills que comportaria una protecció/gestió incorrecta d'aquesta informació.

No obstant això, aquesta informació és molt sensible i es podrien donar les situacions següents:

Es podria fer pública la malaltia d'una persona en detriment de la seva imatge (pèrdua de la confidencialitat).

La pèrdua de confidencialitat pot donar lloc a abusos per terceres parts.

Per exemple, un laboratori deshonest podria fer una campanya de màrqueting d'un producte a persones amb predisposició a patir una malaltia.

Les companyes d'assegurances podrien aprofitar el coneixement de la predisposició d'una persona a patir una malaltia per exigir-li una prima més elevada.

Un metge podria modificar l'historial mèdic amb informació inexacta i després negar haver-ho fet (pèrdua de la integritat i no repudi).

Fins i tot podria fer una diagnosi incorrecta o prescriure un medicament inadequat i després evitar les conseqüències legals de la seva acció (pèrdua de la integritat i no repudi).

D'altra banda, una gestió incorrecta pot donar lloc a la pèrdua o duplicació d'informació i a errors administratius en detriment de la salut del pacient.

1.1. Justificació del PFC i context en el qual es desenvolupa.

Els hospitals, les empreses, els bancs i en general la resta d'institucions tenen una gran necessitat de protegir la informació que gestionen, però en el cas concret de les dades de caràcter personal contingudes en un historial mèdic la garantia d'aquesta protecció esdevé prioritària ja que la informació continguda és molt sensible.

La legislació actual reconeix el dret a la protecció de la informació de caràcter personal.

En el cas de les dades relatives a la salut, donada la sensibilitat d'aquesta informació, cada país ha creat una legislació per protegir-la. Per tant, és necessari recollir i analitzar la legislació existent.

A partir de l'estudi de la legislació es poden extreure les mesures de seguretat o requisits que s'han de complir.

Els sistemes de gestió d'historials mèdics han de complir aquests requisits. Cal estudiar si els sistemes proposats compleixen aquests requisits i si la seva seguretat és suficient.

Per tant, l'objectiu d'aquest PFC és analitzar els articles científics i els treballs pràctics relatius a historials mèdics i determinar fins a quin punt compleixen la legislació actual en matèria de seguretat informàtica.

1.2. Objectius del PFC.

Els objectius principals d'aquest PFC són els següents:

1) Fer un recull de la legislació actual sobre protecció de dades de caràcter personal a nivell internacional, estatal i autonòmic, tant amb caràcter general com de forma més específica sobre la protecció de les dades dels historials mèdics en format electrònic.

2) Analitzar la legislació recollida i extreure els requisits de seguretat i privadesa que es demanen.

3) Cercar articles o implementacions relatives a històries mèdiques.

4) Avaluar si les mesures proposades compleixen realment amb els requisits fixats.

Estudiarem cadascun d'aquests objectius en un capítol diferent del PFC.

1.3. Enfocament i mètode seguit.

A partir de la legislació recollida sobre protecció de dades de caràcter personal es realitza una anàlisi de la informació per tal d'extreure els requeriments de seguretat i privadesa exigits per la legislació.

D'altra banda es fa una recerca sobre la literatura científica existent sobre la protecció de dades de caràcter personal contingudes en els historials mèdics dels pacients.

També s'investiga sobre implementacions reals realitzades amb la finalitat de protegir la seguretat i privadesa dels historials mèdics.

Finalment s'analitzen les mesures proposades i s'avalua el grau de conformitat d'aquests estudis i implementacions amb els requeriments exigits per la legislació descrita anteriorment.

1.4. Planificació del projecte.

- **2 al 13 de març**

Recull de legislació.

- ✓ Legislació general sobre protecció de dades personals.
- ✓ Legislació específica sobre historials mèdics electrònics.

- **14 al 27 de març**

Anàlisi de la legislació.

- ✓ Anàlisi de la legislació.
- ✓ Extracció dels requeriments de seguretat i privadesa exigits per la legislació.

- **28 de març a l'1 de maig**

Literatura científica i projectes.

- ✓ Literatura científica.
- ✓ Projectes.

- **2 de maig al 29 de maig**

Avaluació dels treballs.

- ✓ Grau d'acompliment dels requeriments fixats.
- ✓ Conclusions.

- **30 de maig al 5 de juny**

Redacció de la documentació final: memòria i presentació.

- **6 de maig al 12 de juny**

Presentació de la defensa del PFC.

	Nombre de tarea	Duración	Comienzo	Fin
1	Recullll de legislació	8 días?	mié 02/03/11	dom 13/03/11
2	Anàlisi de la legislació	10 días?	lun 14/03/11	dom 27/03/11
3	Literatura científica i projectes	25 días?	lun 28/03/11	dom 01/05/11
4	Avaluació dels treballs	20 días?	lun 02/05/11	dom 29/05/11
5	Redacció de la documentació final	5 días?	lun 30/05/11	dom 05/06/11
6	Defensa del PFC	5 días?	lun 06/06/11	dom 12/06/11

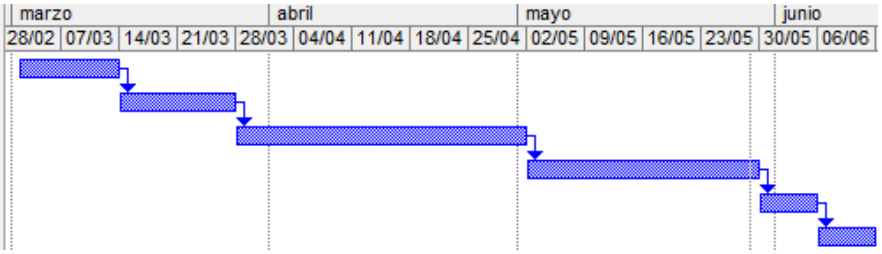

Figura 3. Planificació temporal del PFC.

1.5. Descripció dels altres capítols de la memòria.

- **Capítol 2: Recull de legislació sobre protecció de dades de caràcter personal.**

En aquest capítol es recull la legislació relativa a la protecció de dades de caràcter personal a nivell internacional, estatal i autonòmic parant especial atenció a la legislació relativa a les dades de caràcter personal en format electrònic i a les dades de caràcter personal contingudes en els historials mèdics electrònics.

- **Capítol 3: Requeriments de seguretat i privadesa exigits per la legislació.**

A partir de la legislació recollida en el capítol anterior, es fa una anàlisi i s'extreuen els requeriments de seguretat i privadesa exigits per la legislació.

- **Capítol 4: Literatura científica.**

En aquest capítol es fa una recerca en la literatura científica sobre historials mèdics en format electrònic. Es fa una avaluació del grau de compliment dels treballs seleccionats pel que fa als requeriments de seguretat i privadesa exigits per la legislació i es presenten les conclusions d'aquest estudi.

- **Capítol 5: Projectes.**

En aquest capítol es fa un estudi dels projectes més importants existents actualment i es descriuen les seves característiques principals.

- **Capítol 6: Conclusions i treball futur.**

En aquest capítol es presenten unes breus conclusions generals i es fan uns comentaris sobre possibles millores i ampliacions al treball realitzat.

- **Glossari.**

- **Bibliografia.**

- **Annexos.**

Capítol 2. Recull de legislació sobre protecció de dades de caràcter personal.

La legislació sobre protecció de dades de caràcter personal és un conjunt de normes que cal aplicar pel que fa al registre, gestió, tractament i eliminació de les dades personals.

La normativa relativa a la protecció de dades personals és molt extensa i està en constant desenvolupament ja que la seva relació amb l'avenç de les noves tecnologies és directa.

L'ús correcte de les dades personals és un dret fonamental que cal protegir. Així, l'article 12 de la **Declaració Universal dels Drets Humans** de 10 de desembre 1948, adoptada per l'Assemblea General de Nacions Unides, estableix que el dret a la vida privada és un dret fonamental [7] :

"Ningú no serà objecte d'intromissions arbitràries en la seva vida privada, la seva família, el seu domicili o la seva correspondència, ni d'atacs al seu honor i reputació. Tothom té dret a la protecció de la llei contra tals intromissions o atacs".

Aquesta protecció ha de ser més rigorosa quan més sensible sigui la dada, ja que no tenen la mateixa naturalesa les dades personals d'un establiment comercial que les d'un centre mèdic, per posar dos exemples. En ambdós casos tindrem fitxers de dades personals que caldrà protegir si bé el nivell de protecció serà diferent en un cas o un altre.

Malauradament, la protecció de les dades personals encara està molt lluny del nivell desitjable i és habitual trobar-se avui dia amb casos de dades personals registrades, tractades, comunicades, cedides i eliminades sense cap mena de control.

Estem parlant, doncs, d'una assignatura pendent, la de garantir els drets de les personals de manera efectiva davant les possibles irregularitats en el tractament de les seves dades.

Així ho manifesta l'Agència Espanyola de Protecció de Dades en la seva memòria anual 2009 [8].

D'altra banda, diverses normes legals d'àmbit internacional, nacional i autonòmic reconeixen el dret a la protecció de la informació personal.

2.1. Marc normatiu a la Unió Europea.

L'article 8 del **Conveni Europeu per a la protecció dels drets humans i les llibertats fonamentals** de 4 de novembre de 1950 estableix el dret al respecte a la vida privada i familiar [9] :

"Tota persona té dret al respecte de la seva vida privada i familiar, del seu domicili i de la seva correspondència.
No podrà haver ingerència de l'autoritat pública en l'exercici d'aquest dret, sinó en la mesura que aquesta ingerència estigui prevista per la llei i constitueixi una mesura que, en una societat democràtica, sigui necessària per a la seguretat nacional, la seguretat pública, el benestar econòmic del país, la defensa de l'ordre i la prevenció del delicte, la protecció de la salut o de la moral, o la protecció dels drets i les llibertats dels altres".

La **Carta dels drets Fonamentals de la Unió Europea** estableix el dret a la vida privada i familiar, i el dret a la protecció de dades de caràcter personal [10] :

"Article 7. Dret a la vida privada i familiar.

Tota persona té dret al respecte de la seva vida privada i familiar, del seu domicili i de les seves comunicacions.

Article 8. Protecció de dades de caràcter personal.

1. Tota persona té dret a la protecció de les dades de caràcter personal que li pertoquen.

2. Aquestes dades s'han de tractar de manera lleial, per a finalitats concretes i sobre la base del consentiment de la persona afectada o en virtut d'altres fonaments legítims previstos per la llei. Tota persona té dret a accedir a les dades recollides que li pertoquen i a la seva rectificació.

3. El respecte d'aquestes normes queda subjecte al control d'una autoritat independent".

Un altre text rellevant és el **Conveni 108/1981 del Consell d'Europa** per a la protecció de les persones envers el tractament automatitzat de dades de caràcter personal [11] .

Les previsions d'aquest conveni formen la base de les legislacions nacionals dels diferents estats a nivell comunitari.

D'altra banda, la **Directiva 95/46/CE del Parlament Europeu i del Consell**, de 24 d'octubre de 1995, relativa a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades és el text de referència, a escala europea, en matèria de protecció de dades personals [12] .

Crea un marc regulador destinat a establir un equilibri entre un nivell elevat de protecció de la vida privada de les persones i la lliure circulació de dades personals dins de la Unió Europea.

Amb aquest objectiu, la Directiva fixa límits estrictes per a la recollida i utilització de les dades personals i demana la creació, en cada Estat membre, d'un organisme nacional independent encarregat de la protecció de les esmentades dades.

Aquesta Directiva s'aplica a les dades tractades per mitjans automatitzats (per exemple una base de dades informàtica de clients), així com a les dades contingudes en un fitxer no automatitzat (fitxers en paper tradicionals).

La Directiva té com a objectiu protegir els drets i les llibertats de les persones pel que fa al tractament de dades personals, establint principis d'orientació per a determinar la licitud d'aquest tractament. Aquests principis es refereixen a:

- La qualitat de les dades.
- La legitimació del tractament.
- Les categories especials de tractament (per exemple, dades relatives a la salut).
- La informació als afectats per aquest tractament.
- El dret d'accés de l'interessat a les dades.
- Les excepcions i limitacions.
- El dret de l'interessat a oposar-se al tractament.
- La confidencialitat i la seguretat del tractament.
- La notificació del tractament a l'autoritat de control.

La Directiva anterior és complementada per la **Directiva 2002/58/CE del Parlament Europeu i del Consell**, de 12 de juliol de 2002, relativa al tractament de les dades personals i a la protecció de la intimitat en el sector de les comunicacions electròniques [13] .

2.2. Marc normatiu a l'estat espanyol.

L'article 18 de la **Constitució Espanyola de 1978** estableix el dret a la intimitat com un dret fonamental [14] :

"Article 18.

1. Es garanteix el dret a l'honor, a la intimitat personal i familiar i a la pròpia imatge.

2. El domicili és inviolable. No s'hi podrà entrar ni fer-hi cap escorcoll sense el consentiment del titular o sense resolució judicial, llevat del cas de delicte flagrant.

3. Es garanteix el secret de les comunicacions i, especialment, de les postals, telegràfiques i telefòniques, excepte en cas de resolució judicial.

4. La llei limitarà l'ús de la informàtica per tal de garantir l'honor i la intimitat personal i familiar dels ciutadans i el ple exercici dels seus drets".

El mandat constitucional es va fer efectiu amb la promulgació de la Llei Orgànica 5/1992, de 29 d'octubre, de Regulació del Tractament Automatitzat de Dades de caràcter personal (LORTAD).

En la sentència 254/1993 del Tribunal Constitucional, de 20 de juliol. es reconeix per primera vegada: "el dret a la llibertat enfront de les potencials agressions a la dignitat i a la llibertat de la persona provinents d'un ús il·legítim del tractament automatitzat de dades".

D'altra banda, en el moment d'aprovar la LORTAD s'estava tramitant a la UE la Directiva de Protecció de Dades, Directiva 95/46/CE del Parlament Europeu i del Consell, de 24 d'octubre de 1995, relativa a la Protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades.

Així, la LORTAD coincidia en els mateixos principis i objectius que la Directiva, ja que ambdues tenen el seu origen comú en el Conveni 108, per exemple, coincidia en temes com ara el consentiment de l'afectat i el dret d'informació.

La Directiva homogeneïtza les legislacions de la UE i estableix un termini de tres anys per a la seva transposició en els estats membres, la qual cosa va donar lloc a l'aprovació de la vigent **Llei Orgànica 15/1999 de Protecció de Dades de caràcter personal** (LOPD), de 13 de desembre, que va derogar la LORTAD [15] .

La Llei Orgànica estableix uns principis de protecció de dades:

- Qualitat de les dades: Les dades de caràcter personal només es poden recollir per ser tractades, així com sotmetre-les a aquest tractament, quan siguin adequades, pertinents i no excessives en relació amb l'àmbit i les finalitats determinades, explícites i legítimes per a les quals s'han obtingut.

- Dret d'informació en la recollida de dades: Els interessats als quals se sol·licitin dades personals han de ser prèviament informats de manera expressa, precisa i inequívoca:

a) De l'existència d'un fitxer o un tractament de dades de caràcter personal, de la finalitat de la recollida de les dades i dels destinataris de la informació.

b) Del caràcter obligatori o facultatiu de la resposta a les preguntes que els siguin plantejades.

c) De les conseqüències de l'obtenció de les dades o de la negativa a subministrar-les.

d) De la possibilitat d'exercir els drets d'accés, rectificació, cancel·lació i oposició.

e) De la identitat i la direcció del responsable del tractament o, si s'escau, del seu representant.

- Consentiment de l'afectat: El tractament de les dades de caràcter personal requereix el consentiment inequívoc de l'afectat, llevat que la llei disposi altra cosa.

- Dades especialment protegides: Només amb el consentiment exprés i per escrit de l'afectat poden ser objecte de tractament les dades de caràcter personal que revelin la ideologia, l'afiliació sindical, la religió i les creences. Les dades de caràcter personal que facin referència a l'origen racial, a la salut i a la vida sexual només poden ser recollides, tractades i cedides quan, per raons d'interès general, així ho disposi una llei o l'afectat hi consenti expressament.

- Dades relatives a la salut: Les institucions i els centres sanitaris públics i privats i els professionals corresponents poden procedir al tractament de les dades de caràcter personal relatives a la salut de les persones que hi acudeixin o hi hagin de ser tractades, d'acord amb el que disposa la legislació estatal o autonòmica sobre sanitat.

- Seguretat de les dades: El responsable del fitxer i, si s'escau, l'encarregat del tractament han d'adoptar les mesures de caràcter tècnic i organitzatives necessàries que garanteixin la seguretat de les dades de caràcter personal i n'evitin l'alteració, la pèrdua, el tractament o l'accés no autoritzat.

- Deure de secret: El responsable del fitxer i els qui intervinguin en qualsevol fase del tractament de les dades de caràcter personal estan obligats al secret professional pel que fa a les dades i al deure de guardar-les, obligacions que subsisteixen fins i tot després de finalitzar les seves relacions amb el titular del fitxer o, si s'escau, amb el seu responsable.

- Comunicació de dades: Les dades de caràcter personal objecte del tractament només poden ser comunicades a un tercer per al compliment de finalitats directament relacionades amb les funcions legítimes del cedent i del cessionari amb el consentiment previ de l'interessat.

- Accés a les dades per compte de tercers: La realització de tractaments per compte de tercers ha d'estar regulada en un contracte.

Articles més rellevants de la Llei Orgànica 15/1999 relatius a la protecció de dades personals mèdiques.

Article 7. Dades especialment protegides.

1. D'acord amb el que estableix l'apartat 2 de l'article 16 de la Constitució, ningú no pot ser obligat a declarar sobre la seva ideologia, religió o creences.

Quan en relació amb aquestes dades es procedeixi a recollir el consentiment a què es refereix l'apartat següent, s'ha d'advertir l'interessat respecte al seu dret a no donar-lo.

2. Només amb el consentiment exprés i per escrit de l'afectat poden ser objecte de tractament les dades de caràcter personal que revelin la ideologia, l'afiliació sindical, la religió i les creences. S'exceptuen els fitxers mantinguts pels partits polítics, els sindicats, les esglésies, les confessions o les comunitats religioses i associacions, les fundacions i altres entitats sense ànim de lucre, amb finalitat política, filosòfica, religiosa o sindical, quant a les dades relatives als seus associats o els seus membres, sens perjudici que la cessió d'aquestes dades requereix sempre el consentiment previ de l'afectat.

3. Les dades de caràcter personal que facin referència a l'origen racial, a la salut i a la vida sexual només poden ser recollides, tractades i cedides quan, per raons d'interès general, així ho disposi una llei o l'afectat hi consenti expressament.

4. Queden prohibits els fitxers creats amb la finalitat exclusiva d'emmagatzemar dades de caràcter personal que revelin la ideologia, l'afiliació sindical, la religió, les creences, l'origen racial o ètnic, o la vida sexual.

5. Les dades de caràcter personal relatives a la comissió d'infraccions penals o administratives només poden ser incloses en fitxers de les administracions públiques competents en els casos que preveuen les normes reguladores respectives.

6. No obstant el que disposen els apartats anteriors, poden ser objecte de tractament les dades de caràcter personal a què es refereixen els apartats 2 i 3 d'aquest article quan aquest tractament sigui necessari per a la prevenció o per al diagnòstic mèdic, la prestació d'assistència sanitària o de tractaments mèdics o la gestió de serveis sanitaris, sempre que el tractament de dades, l'efectuï un professional sanitari subjecte al secret professional o una altra persona subjecta a una obligació equivalent de secret.

També poden ser objecte de tractament les dades a què es refereix el paràgraf anterior quan el tractament sigui necessari per salvaguardar l'interès vital de l'afectat o d'una altra persona, en cas que l'afectat estigui físicament o jurídicament incapacitat per donar-ne el consentiment.

Article 8. Dades relatives a la salut.

Sens perjudici del que disposa l'article 11 pel que fa a la cessió, les institucions i els centres sanitaris públics i privats i els professionals corresponents poden procedir al tractament de les dades de caràcter personal relatives a la salut de les persones que hi acudeixin o hi hagin de ser tractades, d'acord amb el que disposa la legislació estatal o autonòmica sobre sanitat.

Article 9. Seguretat de les dades.

1. El responsable del fitxer i, si s'escau, l'encarregat del tractament han d'adoptar les mesures de caràcter tècnic i organitzatiu necessàries que garanteixin la seguretat de les dades de caràcter personal i n'evitin l'alteració, la pèrdua, el tractament o l'accés no autoritzat, tenint en compte l'estat de la tecnologia, la naturalesa de les dades emmagatzemades i els riscos a què estan exposats, tant si provenen de l'acció humana o del medi físic o natural.

2. No s'han de registrar dades de caràcter personal en fitxers que no compleixin les condicions que es determinin per via reglamentària en relació amb la seva integritat i seguretat i a les dels centres de tractament, locals, equips, sistemes i programes.

3. S'han d'establir per reglament els requisits i les condicions que han de complir els fitxers i les persones que intervinguin en el tractament de les dades a què es refereix l'article 7 d'aquesta Llei.

Article 11. Comunicació de dades.

1. Les dades de caràcter personal objecte del tractament només poden ser comunicades a un tercer per al compliment de finalitats directament relacionades amb les funcions legítimes del cedent i del cessionari amb el consentiment previ de l'interessat.

2. El consentiment que exigeix l'apartat anterior no és necessari:

f) Quan la cessió de dades de caràcter personal relatives a la salut sigui necessària per solucionar una urgència que requereixi accedir a un fitxer o per fer els estudis epidemiològics en els termes que estableix la legislació sobre sanitat estatal o autonòmica.

Article 34. Excepcions.

El que disposa l'article anterior sobre moviment internacional de dades no és aplicable:

c) Quan la transferència sigui necessària per a la prevenció o per al diagnòstic mèdic, la prestació d'assistència sanitària o tractament mèdic o la gestió de serveis sanitaris.

Matèries protegides en funció del nivell de seguretat.

La LOPD suposa un gran avenç normatiu amb efectes a tot el territori nacional en matèria de regulació de tractament de dades personals. Tot i això la Llei orgànica per si mateixa és una declaració d'intencions i de normativa general en la matèria i calia, per tant, esperar el seu desenvolupament normatiu. El Reglament de desenvolupament de la LOPD va ser aprovat pel **Reial Decret 1720/2007**, de 21 de desembre [16] .

El Reial Decret classifica les matèries protegides per a cada nivell de seguretat, com es pot veure en les taules següents.

MATÈRIES PROTEGIDES EN FUNCIÓ DEL NIVELL DE SEGURETAT (arts. 80 i 81 RD 1720/2007)	
NIVELL	**MATÈRIES PROTEGIDES**
BAIX	81.1 Tots els fitxers o tractaments de dades de caràcter personal. 81.5. En el cas de fitxers o tractaments de dades d'ideologia, afiliació sindical, religió, creences, origen racial, **salut** o vida sexual només s'han d'implantar les mesures de seguretat de nivell bàsic quan: a) Les dades s'utilitzin amb l'única finalitat de realitzar una transferència dinerària a les entitats de què els afectats siguin associats o membres. b) Es tracti de fitxers o tractaments no automatitzats on de forma incidental o accessòria s'incloguin les dades sense tenir relació amb la seva finalitat. 81.6. També es poden implantar les mesures de seguretat de nivell bàsic en els fitxers o tractaments que continguin dades relatives a la **salut**, referents exclusivament al grau de discapacitat o la simple declaració de la condició de discapacitat o invalidesa de l'afectat, amb motiu del compliment de deures públics.

Tabla 1. Matèries protegides en el nivell de seguretat baix.

MATÈRIES PROTEGIDES EN FUNCIÓ DEL NIVELL DE SEGURETAT (arts. 80 i 81 RD 1720/2007)	
NIVELL	**MATÈRIES PROTEGIDES**
MITJÀ	81.2 a) Els relatius a la comissió d'infraccions administratives o penals. b) Aquells el funcionament dels quals es regeixi per l'article 29 de la Llei orgànica 15/1999, de 13 de desembre. c) Aquells els responsables dels quals siguin administracions tributàries i es relacionin amb l'exercici de les seves potestats tributàries. d) Aquells els responsables dels quals siguin les entitats financeres per a finalitats relacionades amb la prestació de serveis financers. e) Aquells els responsables dels quals siguin les entitats gestores i serveis comuns de la Seguretat Social i es relacionin amb l'exercici de les seves competències. De la mateixa manera, aquells els responsables dels quals siguin les mútues d'accidents de treball i malalties professionals de la Seguretat Social. f) Els que continguin un conjunt de dades de caràcter personal que ofereixin una definició de les característiques o de la personalitat dels ciutadans i que permetin avaluar determinats aspectes de la seva personalitat o comportament.

Tabla 2. Matèries protegides en el nivell de seguretat mitjà.

MATÈRIES PROTEGIDES EN FUNCIÓ DEL NIVELL DE SEGURETAT (arts. 80 i 81 RD 1720/2007)	
NIVELL	**MATÈRIES PROTEGIDES**
ALT	81.3 a) Els que es refereixin a dades d'ideologia, afiliació sindical, religió, creences, origen racial, **salut** o vida sexual. b) Els que continguin o es refereixin a dades obtingudes per a fins policials sense consentiment de les persones afectades. c) Els que continguin dades derivades d'actes de violència de gènere. 81.4. Als fitxers els responsables dels quals siguin els operadors que prestin serveis de comunicacions electròniques disponibles al públic o explotin xarxes públiques de comunicacions electròniques respecte a les dades de tràfic i a les dades de localització, s'hi han d'aplicar, a més de les mesures de seguretat de nivell bàsic i mitjà, la mesura de seguretat de nivell alt que conté l'art. 103 d'aquest Reglament (Registre d'accessos).

Tabla 3. Matèries protegides en el nivell de seguretat alt.

Mesures de seguretat en funció del nivell de seguretat.

El Reglament estableix un conjunt de mesures de seguretat en funció del nivell de seguretat.

MESURES DE SEGURETAT EN FUNCIÓ DEL NIVELL DE SEGURETAT (RD 1720/2007)	
DOCUMENT DE SEGURETAT **(art. 88)**	**NIVELL BÀSIC** Àmbit d'aplicació. Mesures, normes, procediments d'actuació, regles i estàndards de seguretat. Funcions i obligacions del personal. Estructura dels fitxers amb dades de caràcter personal i descripció dels sistemes d'informació que els tracten. Procediment de notificació, gestió i resposta davant les incidències. Els procediments de realització de còpies de seguretat i de recuperació de les dades en els fitxers o tractaments automatitzats. Transport de suports i documents, destrucció i reutilització de documents. **NIVELL MITJÀ** Identificació del responsable de seguretat. Els controls periòdics que s'han de realitzar per verificar el compliment del que disposa el document.
PERSONAL **(art. 89)**	**NIVELL BÀSIC** Funcions i obligacions clarament definides i documentades. Difusió entre el personal de les normes que els afectin i de les conseqüències del seu incompliment.
INCIDÈNCIES **(art. 90,100)**	**NIVELL BÀSIC** Registrar les incidències. **NIVELL MITJÀ** Registrar els procediments de recuperació de les dades, la persona que va executar el procés, les dades restaurades i gravades manualment. Autorització del responsable del fitxer per a la recuperació de les dades.

Tabla 4. Mesures de seguretat (I).

MESURES DE SEGURETAT EN FUNCIÓ DEL NIVELL DE SEGURETAT (RD 1720/2007)	
IDENTIFICACIÓ I AUTENTICACIÓ **(art. 91,93,98)**	**NIVELL BÀSIC** Relació actualitzada d'usuaris i perfils d'usuaris, i els accessos autoritzats. Procediments d'identificació i autenticació. Control d'accés. Procediment d'assignació, distribució i emmagatzematge de contrasenyes que garanteixi la confidencialitat i integritat. Política de control d'accés (per exemple, la periodicitat del canvi de contrasenyes). **NIVELL MITJÀ** Mecanisme de control d'accés (per exemple, l'establiment d'un nombre màxim d'intents d'accés).
CONTROL D'ACCÉS **(art. 91)**	**NIVELL BÀSIC** Assignació de rols als usuaris per a limitar l'accés a la informació d'acord amb el principi de necessitat de saber i establir mecanismes per al seu control. Concessió de permisos d'accés només per personal autoritzat. **NIVELL MITJÀ** Exclusivament el personal autoritzat en el document de seguretat pot tenir accés als llocs on estiguin instal·lats els equips físics que donin suport als sistemes d'informació.

Tabla 5. Mesures de seguretat (II).

MESURES DE SEGURETAT EN FUNCIÓ DEL NIVELL DE SEGURETAT (RD 1720/2007)	
GESTIÓ I DISTRIBUCIÓ DE SUPORTS **(art. 92, 97,101)**	**NIVELL BÀSIC** Identificar el tipus d'informació que contenen. Fer un inventari. Emmagatzematge amb accés restringit. Sortida de suports autoritzada pel responsable del fitxer. **NIVELL MITJÀ** Registre d'entrada i sortida de suports. Mesures per evitar la recuperació de la informació d'un suport que hagi de ser rebutjada o reutilitzada. Mesures per evitar la recuperació de la informació emmagatzemada que hagi de sortir. **NIVELL ALT** Xifrat de dades en la distribució de suports.
CÒPIES DE SEGURETAT I RECUPERACIÓ **(art. 94, 102)**	**NIVELL BÀSIC** Verificar l'aplicació dels procediments de còpies de seguretat i recuperació. Garantir la reconstrucció de les dades a l'estat en què es trobaven en el moment de produir-se la pèrdua o destrucció. Còpia de seguretat, al menys setmanal. **NIVELL ALT** Còpia de seguretat i de procediments de recuperació en un lloc diferent d'aquell en què estiguin els equips.
RESPONSABLE **(art. 95)**	**NIVELL MITJÀ** En el document de seguretat s'han d'assignar un o més responsables de seguretat encarregats de coordinar i controlar les mesures. No suposa una exoneració de la responsabilitat que correspon al responsable del fitxer o a l'encarregat del tractament.

Tabla 6. Mesures de seguretat (III).

MESURES DE SEGURETAT EN FUNCIÓ DEL NIVELL DE SEGURETAT (RD 1720/2007)	
PROVES **(art. 94)**	**NIVELL MITJÀ** Només es faran proves amb dades reals si s'assegura el nivell de seguretat corresponent al tipus de fitxer tractat i prèviament cal fer una còpia de seguretat.
AUDITORIA **(art. 96)**	**NIVELL MITJÀ** Al menys cada dos anys, interna o externa. Informe sobre l'adequació de les mesures i controls, identificar i proposar mesures correctores. Anàlisi del responsable de seguretat i conclusions al responsable del fitxer per a l'adopció de mesures correctores.
REGISTRE D'ACCESSOS **(art. 103)**	**NIVELL ALT** Registre i auditoria de la informació. Control per part del responsable de seguretat. Fer informe mensual. Conservació de les dades 2 anys
TELE-COMUNICACIONS **(art. 104)**	**NIVELL ALT** Comunicació segura de les dades.

Tabla 7. Mesures de seguretat (IV).

Capítol 3. Requisits de seguretat i privadesa exigits per la legislació.

En el capítol 2 s'ha fet un recull de la legislació internacional, estatal i autonòmica més rellevant per a la protecció de dades de caràcter personal. En aquest capítol ens centrarem en els requeriments de seguretat i privadesa dels historials mèdics i en els estàndards existents.

Un HCE presenta un conjunt d'avantatges en relació als registres en paper (reducció de costos, millora de la qualitat de l'atenció, conservació dels registres, mobilitat, etc.). D'altra banda, els registres en paper presenten un grau de llegibilitat pobra, el que pot contribuir a errors mèdics. Els registres electrònics ajuden a la normalització dels formularis, la terminologia, les abreviatures, i l'entrada de dades. La digitalització dels formularis facilita la recopilació de dades per a estudis clínics i epidemiològics.

No obstant això, l'augment de la portabilitat i l'accessibilitat dels registres mèdics electrònics també afavoreix la facilitat amb què poden ser accedits i robats per persones no autoritzades o per usuaris sense escrúpols.

Així ho reconeixen, d'una banda, l'HIPAA (Health Insurance Portability and Accountability Act) [17] que estableix un increment dels requisits de seguretat per als registres mèdics electrònics i, d'altra, els usuaris que informen de violacions a gran escala en els registres confidencials.

Aquestes preocupacions contribueixen a la resistència mostrada a la seva adopció de forma generalitzada. Als Estats Units, Gran Bretanya i Alemanya, el concepte d'un model nacional de salut centralitzat no ha estat ben rebut. Els aspectes de privacitat i seguretat del model han estat motiu de preocupació [18] [19].

Les preocupacions sobre la privacitat en l'assistència sanitària s'apliquen tant als registres en paper com als electrònics. Segons el diari Los Angeles Times, aproximadament 150 persones (des dels metges i infermeres fins als tècnics i empleats de facturació) tenen accés a almenys part dels registres d'un pacient durant una hospitalització, i moltes més persones també tenen algun tipus d'accés [20].

Recentment s'han detectat accessos a "dades segures" en diversos repositoris de dades centralitzats (en la banca i altres institucions financeres, en la indústria, i en bases de dades governamentals) que han causat preocupació sobre l'emmagatzematge electrònic de registres mèdics en una ubicació central [21].

Els registres que s'intercanvien a través d'Internet estan subjectes als mateixos problemes de seguretat que qualsevol altre tipus de transacció de dades a través d'Internet.

La Health Insurance Portability and Accountability Act (HIPAA) va ser aprovada als EUA el 1996 per establir normes d'accés, autenticació, emmagatzematge i auditoria, i la transmissió de registres mèdics electrònics. Aquesta norma va establir restriccions per als registres electrònics més estrictes que les dels registres en paper. No obstant això, hi ha dubtes pel que fa a l'adequació d'aquestes normes [22].

A la Unió Europea (UE), diverses directives del Parlament Europeu i del Consell d'Europa protegeixen el tractament i la lliure circulació de dades personals, també en el cas d'assistència sanitària.

L'amenaça a la privacitat que planteja la interoperabilitat d'una xarxa nacional és una preocupació clau. El professor Jacob M. Appel, de la Universitat de New York, ha afirmat que el nombre de persones que necessiten tenir accés a un sistema nacional veritablement interoperable, que ell estima en 12 milions, donarà lloc inevitablement a violacions de la intimitat a escala masiva [23].

Aquesta és una barrera important per a l'adopció d'un HCE. La responsabilitat entre totes les parts que intervenen en el processament de transaccions electròniques, incloent els pacients, el personal administratiu i les companyies d'assegurances, és clau per a l'èxit de l'HCE.

Als EUA, qualsevol proveïdor d'atenció mèdica que porti a terme les operacions en forma electrònica o qualsevol centre d'atenció mèdica o pla de salut constitueix el que s'anomena entitat coberta (covered entity) i és una entitat que està dins de l'àmbit d'aplicació de la Health Insurance Portability and Accountability Act de 1996 (HIPAA) [24].

3.1. Requeriments de seguretat i privadesa.

Hi ha una extensa legislació sobre seguretat i privacitat de la informació [25].

Les lleis de privacitat de la informació tenen per objectiu la protecció de la informació de les persones pel que fa a la divulgació o a l'ús indegut de la informació.

Donat que l'objectiu d'aquesta memòria és analitzar la seguretat i privadesa de les històries mèdiques en format electrònic s'ha fet una cerca de la legislació actual sobre aquest tema.

En aquest apartat es fa un estudi de la legislació que s'ha considerat més important.

En primer lloc, s'analitza la legislació existent a l'Estat espanyol ja que és l'àmbit territorial més proper a nosaltres.

En segon lloc, s'analitza la legislació existent als EUA ja que és la més completa i extensa.

3.1.1. Estat espanyol.

A l'Estat espanyol, els historials mèdics venen regulats per diverses disposicions de rang legal:

- Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de caràcter personal (articles 7 i 8) [15].
- Llei 14/86, General de Sanitat, de 25 d'abril (articles 10.3 i 23) [26].
- Llei 41/2002, del 14 de novembre, reguladora de l'autonomia del pacient i dels drets i obligacions en matèria d'informació i documentació clínica [27].
- Llei 21/2000, de 29 de desembre, sobre els drets d'informació concernent la salut i l'autonomia del pacient, i la documentació clínica [28].

Tot seguit detallem el contingut d'aquestes disposicions.

• Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de caràcter personal.

Defineix el concepte de dada de caràcter personal com a qualsevol informació que concerneixi a una persona física identificada o identificable. Les dades sanitàries són dades de caràcter personal i, per tant, dins de l'àmbit d'aplicació de la LOPD. La referència a aquest tipus de dades apareix als articles 7 i 8 de la LOPD.

• Llei 14/1986 General de Sanitat, de 25 d'abril.

Estableix en el seu article 10.3 el dret del ciutadà a la confidencialitat de les seves dades i en l'article 23 recull la potestat de l'administració sanitària per a crear registres.

"Article10.

Tots tenen els següents drets en relació a les diferents administracions públiques sanitàries:

3. A la confidencialitat de tota la informació relacionada amb el seu procés i amb la seva estada en institucions sanitàries públiques i privades que col·laborin amb el sistema públic.

Article 23.

Per a la consecució dels objectius que es desenvolupen en el present capítol, les Administracions sanitàries, d'acord amb les seves competències, crearan els registres i elaboraran les anàlisis d'informació necessàries per al coneixement de les diferents situacions de les que puguin derivar accions d'intervenció de l'autoritat sanitària".

• Llei 41/2002, del 14 de novembre, reguladora de l'autonomia del pacient i dels drets i obligacions en matèria d'informació i documentació clínica.

CAPÍTOL I

Principis generals

Article 1. Àmbit d'aplicació.

Aquesta Llei té per objecte la regulació dels drets i les obligacions dels pacients, usuaris i professionals, així com dels centres i serveis sanitaris, públics i privats, en matèria d'autonomia del pacient i d'informació i documentació clínica.

Article 2. Principis bàsics.

1. La dignitat de la persona humana, el respecte a l'autonomia de la seva voluntat i a la seva intimitat han d'orientar tota l'activitat encaminada a obtenir, utilitzar, arxivar, custodiar i transmetre la informació i la documentació clínica.

...

7. La persona que elabori o tingui accés a la informació i la documentació clínica està obligada a guardar la reserva deguda.

Article 3. Les definicions legals.

Documentació clínica: el suport de qualsevol tipus o classe que conté un conjunt de dades i informacions de caràcter assistencial.

Història clínica: 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.

Informació clínica: qualsevol dada, sigui quina sigui la forma, classe o tipus, que permet adquirir o ampliar coneixements sobre l'estat físic i la salut d'una persona, o la manera de preservar-la, cuidar-la, millorar-la o recuperar-la.

...

CAPÍTOL III

Dret a la intimitat

Article 7. El dret a la intimitat.

1. Qualsevol persona té dret al fet que es respecti el caràcter confidencial de les dades referents a la seva salut, i que ningú no hi pugui accedir sense autorització prèvia emparada per la llei.

2. Els centres sanitaris han d'adoptar les mesures oportunes per garantir els drets a què es refereix l'apartat anterior, i han d'elaborar, quan sigui escaient, les normes i els procediments protocol·litzats que garanteixin l'accés legal a les dades dels pacients.

CAPÍTOL V

La història clínica

Article 14. Definició i arxivament de la història clínica.

1. La història clínica comprèn el conjunt dels documents relatius als processos assistencials de cada pacient, amb la identificació dels metges i dels altres professionals que hi han intervingut, per tal d'obtenir la màxima integració possible de la documentació clínica de cada pacient, almenys, en l'àmbit de cada centre.

2. Cada centre ha d'arxivar les històries clíniques dels seus pacients, sigui quin sigui el suport, paper, audiovisual, informàtic o d'un altre tipus en què constin, de manera que en quedin garantides la seguretat, la conservació correcta i la recuperació de la informació.

3. Les administracions sanitàries han d'establir els mecanismes que garanteixin l'autenticitat del contingut de la història clínica i dels canvis que s'hi hagin produït, així com la possibilitat de reproduir-la en el futur.

4. Les comunitats autònomes han d'aprovar les disposicions necessàries perquè els centres sanitaris puguin adoptar les mesures tècniques i organitzatives adequades per arxivar i protegir les històries clíniques i evitar-ne la destrucció o la pèrdua accidental.

Article 15. Contingut de la història clínica de cada pacient.

1. 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. Qualsevol pacient o usuari té dret al fet que quedi constància, per escrit o en el suport tècnic més adequat, de la informació obtinguda en tots els seus processos assistencials, realitzats pel servei de salut tant en l'àmbit d'atenció primària com d'atenció especialitzada.

2. La història clínica té com a finalitat principal 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. El contingut mínim de la història clínica ha de ser el següent:

a) La documentació relativa al full clinicoestadístic.

b) L'autorització d'ingrés.

c) L'informe d'urgència.

d) L'anamnesi i l'exploració física.

e) L'evolució.

f) Les ordres mèdiques.

g) El full d'interconsulta.

h) Els informes d'exploracions complementàries.

i) El consentiment informat.

j) L'informe d'anestèsia.

k) L'informe de quiròfan o de registre del part.

l) L'informe d'anatomia patològica.

m) L'evolució i planificació de cures d'infermeria.

n) L'aplicació terapèutica d'infermeria.

ñ) El gràfic de constants.

o) L'informe clínic d'alta.

Els paràgrafs b), c), i), j), k), l), ñ) i o) només són exigibles en la formalització de la història clínica quan es tracti de processos d'hospitalització o es disposi d'aquesta manera.

3. La formalització de la història clínica, en els aspectes relacionats amb l'assistència directa al pacient, és responsabilitat dels professionals que hi intervinguin.

4. La història clínica s'ha de portar amb criteris d'unitat i d'integració, a cada institució assistencial com a mínim, per facilitar que els facultatius tinguin el coneixement millor i més oportú de les dades d'un determinat pacient en cada procés assistencial.

Article 16. Usos de la història clínica.

1. La història clínica és un instrument destinat fonamentalment a garantir una assistència adequada al pacient. Els professionals assistencials del centre que realitzen el diagnòstic o el tractament del pacient tenen accés a la història clínica del pacient com a instrument fonamental per a la seva adequada assistència.

2. Cada centre ha d'establir els mètodes que possibilitin a tota hora l'accés a la història clínica de cada pacient per part dels professionals que l'assisteixen.

3. L'accés a la història clínica amb finalitats judicials, epidemiològiques, de salut pública, d'investigació o de docència, es regeix pel que disposen la Llei orgànica 15/1999, de protecció de dades de caràcter personal, i la Llei 14/1986, general de sanitat, i altres normes d'aplicació 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 mateix hagi donat el seu consentiment per no separar-les.

Se n'exceptuen els casos d'investigació de l'autoritat judicial en què es consideri imprescindible unificar les dades identificatives amb les clinicoassistencials, en els quals cal

atenir-se al que disposin els jutges i tribunals en el procés corresponent. L'accés a les dades i els documents de la història clínica queda limitat estrictament a les finalitats específiques de cada cas.

4. El personal d'administració i gestió dels centres sanitaris només pot accedir a les dades de la història clínica relacionades amb les seves pròpies funcions.

5. El personal sanitari degudament acreditat que exerceixi funcions d'inspecció, avaluació, acreditació i planificació, té accés a les històries clíniques en el compliment de les seves funcions de comprovació de la qualitat de l'assistència, el respecte dels drets del pacient o qualsevol altra obligació del centre en relació amb els pacients i usuaris o l'Administració sanitària mateixa.

6. El personal que accedeix a les dades de la història clínica en l'exercici de les seves funcions queda subjecte al deure de secret.

7. Les comunitats autònomes han de regular el procediment perquè quedi constància de l'accés a la història clínica i del seu ús.

Article 17. La conservació de la documentació clínica.

1. Els centres sanitaris tenen l'obligació de conservar la documentació clínica en condicions que en garanteixin el manteniment correcte i la seguretat, encara que no necessàriament en el suport original, per a la deguda assistència al pacient durant el temps adequat en cada cas i, com a mínim, cinc anys comptats des de la data de l'alta de cada procés assistencial.

2. La documentació clínica també s'ha de conservar a efectes judicials de conformitat amb la legislació vigent.

S'ha de conservar, així mateix, quan existeixin raons epidemiològiques, d'investigació o d'organització i funcionament del Sistema Nacional de Salut. El seu tractament s'ha de fer de manera que s'eviti en la mesura possible identificar les persones afectades.

3. Els professionals sanitaris tenen el deure de cooperar en la creació i el manteniment d'una documentació clínica ordenada i seqüencial del procés assistencial dels pacients.

4. La gestió de la història clínica l'han de dur terme els centres amb pacients hospitalitzats, o els que atenguin un nombre suficient de pacients sota qualsevol altra modalitat assistencial, segons el criteri dels serveis de salut, a través de la unitat d'admissió i documentació clínica, encarregada d'integrar en un sol arxiu les històries clíniques. La custòdia d'aquestes històries clíniques està sota la responsabilitat de la direcció del centre sanitari.

5. Els professionals sanitaris que duen a terme la seva activitat de manera individual són responsables de gestionar i custodiar la documentació assistencial que generin.

6. Són aplicables a la documentació clínica les mesures tècniques de seguretat que estableix la legislació reguladora de la conservació dels fitxers que contenen dades de caràcter personal i, en general, la Llei orgànica 15/1999, de protecció de dades de caràcter personal.

Article 18. Drets d'accés a la història clínica.

1. El pacient té el dret d'accés, amb les reserves que assenyala l'apartat 3 d'aquest article, a la documentació de la història clínica i a obtenir còpia de les dades que hi figuren. Els centres sanitaris han de regular el procediment que garanteixi l'observança d'aquests drets.

2. El dret d'accés del pacient a la història clínica també es pot exercir per representació degudament acreditada.

3. 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 que participen en la seva elaboració, que poden oposar al dret d'accés la reserva de les seves anotacions subjectives.

4. Els centres sanitaris i els facultatius d'exercici individual només han de facilitar l'accés a la història clínica dels pacients morts a les persones que hi estan vinculades, per raons familiars o de fet, llevat que el mort ho hagi prohibit expressament i s'acrediti d'aquesta manera. En qualsevol cas l'accés d'un tercer a la història clínica motivat per un risc per a la seva salut s'ha de limitar a les dades pertinents. No s'ha de facilitar informació que afecti la intimitat del mort ni les anotacions subjectives dels professionals, ni que perjudiqui tercers.

Article 19. Drets relacionats amb la custòdia de la història clínica.

El pacient té dret al fet que els centres sanitaris estableixin un mecanisme de custòdia activa i diligent de les històries clíniques. Aquesta custòdia ha de permetre la recollida, la integració, la recuperació i la comunicació de la informació sotmesa al principi de confidencialitat d'acord amb el que estableix l'article 16 d'aquesta Llei.

Com s'acaba de veure, hi ha un conjunt de requisits legals que cal complir respecte a l'historial mèdic. Aquests requisits són intrínsecs a l'historial, alhora que són directrius per les persones que hi tinguin accés. En resum, cal:

- ✓ Garantir el dret de l'usuari a accedir a la seva història clínica i a obtenir-ne dades.
- ✓ Respectar la intimitat, la dignitat humana i les conviccions del pacient.
- ✓ Fer-lo disponible per l'usuari les 24 hores del dia, els set dies de la setmana.
- ✓ Arxivar-lo almenys deu anys després de la mort del pacient.

En aquesta llei es recull el dret del pacient a conèixer tota la informació sobre la seva salut, que aquesta informació sigui verídica i comprensible i el dret de tota persona al fet que es respecti la confidencialitat de les dades referents a la seva salut".

• Pel que fa a la legislació autonòmica existent relativa a les dades sanitàries, destaca la Llei 21/2000, de 29 de desembre, sobre els drets d'informació concernent la salut i l'autonomia del pacient, i la documentació clínica. La Llei 21/2000 és molt similar a la Llei estatal per la qual cosa no la detallarem aquí.

3.1.2. EUA.

La HIPAA (Health Insurance Portability & Accountability Act of 1996) [17] [29] [30] és la regulació més important pel que fa a la seguretat i privadesa de dades personals de salut als EUA.

La Health Insurance Portability and Accountability Act (HIPAA) va ser promulgada pel Congrés dels EUA el 1996. També es coneix com la Llei Pública 104-191 o la Llei Kennedy-Kassebaum. Va entrar en vigor el 21 d'agost de 1996. La idea bàsica de HIPAA és que un individu amb informació mèdica personal:

- Ha de disposar de procediments per exercir els drets de privacitat de la informació de salut personal.
- Ha d'autoritzar l'ús i divulgació de la seva informació personal de salut.

Una de les dificultats amb HIPAA és que cal un mecanisme per autenticar al pacient que demana l'accés a les seves dades. Com a resultat, els centres mèdics han començat a demanar els números de Seguretat Social dels pacients, el que podria reduir la privacitat.

A diferència de l'enfocament dels EUA a la protecció de la privacitat, que es basa en la legislació específica del sector, la Unió Europea es basa en una legislació de privadesa molt completa. La Directiva Europea de Protecció de Dades, que va entrar en vigor l'octubre de 1998, inclou, per exemple, l'obligació de crear organismes de protecció de dades del govern, el registre de bases de dades en les agències i, en alguns casos, l'aprovació prèvia abans de poder començar a processar les dades personals. Per tal de salvar aquests enfocaments diferents de privacitat i proporcionar un mitjà simplificat per donar compliment a la Directiva per part de les organitzacions dels EUA, el Departament de Comerç dels EUA, després de consultar amb la Comissió Europea, va elaborar un marc anomenat "port segur", en analogia a la seguretat d'un vaixell quan arriba a port. El port segur - aprovat per la UE el juliol de 2000 - permet complir a les empreses dels EUA amb les lleis de privacitat europees.

Per a la majoria dels consumidors de l'atenció sanitària als Estats Units, "HIPAA" és una referència en un formulari de consentiment que un metge demana omplir a un pacient abans que el pacient pugui rebre atenció mèdica.

En realitat, HIPAA és una iniciativa per reduir les despeses sanitàries mitjançant l'estandardització dels intercanvis de dades entre els proveïdors i les asseguradores.

Els reglaments HIPAA adrecen:

- Transaccions electròniques i conjunts de codis.
- Identificadors nacionals.
- Privacitat.
- Seguretat.

Entitats incloses.

Qui està cobert pel reglament?

- Els proveïdors sanitaris.
    - Les persones - metges, infermeres, farmacèutics, ...
    - Organitzacions - hospitals, laboratoris, serveis de manteniment (HMO), farmàcies, ...
- Els plans de salut (els qui contracten un pla).
- Els gestors de les dades (Healthcare clearinghouses). Entitat que estandarditza la informació de salut, per exemple un servei de facturació que processa o facilita el processament de dades des d'un format no estandarditzat a un format estandarditzat de facturació.

Qualsevol d'aquestes entitats que transmet qualsevol informació de salut de forma electrònica amb una transacció HIPAA, o paga a una altra entitat en el seu nom per a fer-ho, està coberta per HIPAA.

Els plans de salut inclouen les asseguradores públiques i privades. HIPAA cobreix Medicare, Medicaid i les assegurances dels funcionaris.

Qui no està cobert per HIPAA?

- Companyies d'assegurances de la propietat i d'accidents.
- Plans de salut petits (amb menys de 50 membres).
- Els proveïdors que realitzen totes les transaccions estàndards amb paper, telèfon o fax.

La norma de privacitat (Privacy Rule).

La data de compliment efectiu de la Regla de Privacitat va ser el 14 d'abril de 2003 amb una pròrroga d'un any per a determinats "plans petits". La Regla de Privacitat HIPAA regula l'ús i la divulgació de certa informació en poder de les "entitats cobertes" (en general, centres gestors, plans de salut patrocinats per l'empresari, les asseguradores de salut i els proveïdors de serveis mèdics). Estableix regulacions per a l'ús i la divulgació d'informació mèdica protegida (Protected Health Information, PHI). PHI és qualsevol informació en poder d'una entitat coberta que es refereix a l'estat de salut, prestació d'assistència sanitària, o pagament per serveis sanitaris que poden ser vinculats a una persona. Això s'interpreta de manera força àmplia i inclou a qualsevol part de l'expedient mèdic d'un individu o historial de pagaments.

Les entitats cobertes han de revelar la PHI a la persona dins de 30 dies posteriors a la petició. També han de revelar la PHI quan siguin requerides per la llei. Una entitat coberta pot divulgar la PHI per facilitar el tractament, pagament o operacions d'atenció mèdica, o si l'entitat coberta ha obtingut l'autorització de la persona. No obstant això, quan una entitat coberta revela qualsevol PHI, ha de revelar només la informació mínima necessària requerida per aconseguir el seu propòsit.

La Norma de Privacitat dóna als individus el dret de demanar que una entitat coberta esmeni qualsevol PHI inexacta. La norma també exigeix que les entitats cobertes adoptin mesures raonables per garantir la confidencialitat de les comunicacions amb els individus. Per exemple, una persona pot demanar que el truquin al número del seu treball, en lloc de trucar a la seva casa o al número de telèfon mòbil.

La Regla de Privacitat exigeix que les entitats cobertes notifiquin a les persones dels usos de la seva PHI. Les entitats cobertes també han de fer un seguiment de la informació PHI revelada i documentar els procediments i polítiques de privacitat. Cal designar un responsable de seguretat i una persona de contacte encarregada de rebre les queixes i formar a tot el personal en els procediments relatius a la PHI.

La norma de privacitat estableix que cal protegir la informació de salut individualment identificable (Individually Identifiable Health Information, IIHI). IIHI inclou qualsevol registre que contingui dades que identifiquen una persona o que són una base raonable per a la identificació d'una persona.

La informació mèdica protegida (PHI) no s'aplica a les dades desidentificades. HIPAA permet tres tècniques per a desidentificar dades:

- Safe harbor.
- Tècnica estadísticament fiable.
- Conjunt limitat de dades.

La norma Safe Harbor ("Port Segur").

Als EUA, l'HIPAA protegeix la confidencialitat de les dades del pacient, i la Common Rule protegeix la confidencialitat de les persones en una investigació. Aquestes lleis generalment requereixen el consentiment informat del pacient i l'aprovació de la Internal Review Board per utilitzar les dades amb propòsits d'investigació, però no cal aplicar aquests requisits si les dades són desidentificades, o si el consentiment del pacient no és possible. HIPAA estableix una llista precisa dels atributs sense els quals un registre no pot ser atribuït a una persona. Per tal que les dades clíniques es considerin desidentificades, la norma Safe Harbor [31] de l'HIPAA requereix eliminar els 18 tipus de dades de la taula (veure la pàgina següent).

Desidentificació estadísticament fiable.

Un algorisme de desidentificació sol implicar una combinació de:

- L'eliminació de determinats identificadors Safe Harbor.
- La substitució d'altres identificadors amb els valors calculats aleatòriament que garanteixin la distinció de les persones sense arribar a la seva identificació.

Conjunt de dades restringit.

Les normes HIPAA permeten un conjunt limitat de dades quan la tècnica "Safe Harbor" és massa restrictiva. En un conjunt limitat de dades, no es permeten la majoria dels identificadors "Safe Harbor". Les dades que es poden utilitzar són:

- Data d'admissió, d'alta i dates del servei.
- Data de defunció.
- Edat.
- Codi postal de 5 dígits.

1. Noms.

2. Qualsevol subdivisió geogràfica més petita que un estat, inclosa l'adreça del carrer, ciutat, comtat, districte, codi postal, o equivalents, amb l'excepció dels 3 primers dígits d'un codi postal si la zona conté més de 20000 persones.

3. Totes les dates (excepte l'any) relacionades directament amb una persona (data de naixement, data d'admissió, data d'alta, data de defunció). També totes les edats de més de 89 anys o dates que indiquin aquesta edat.

4. Números de telèfon.

5. Números de fax.

6. Adreços de correu electrònic.

7. Números de Seguretat Social.

8. Números d'expedient mèdic.

9. Números de beneficiari de pla de salut.

10. Números de compte.

11. Números de certificat o llicència.

12. Identificació del vehicle o números de sèrie, inclosos els números de la matrícula.

13. Identificadors o números de sèrie de dispositius.

14. URL's (Universal Resource Locators).

15. Adreces IP.

16. Identificadors biomètrics.

17. Fotos de cara completa i imatges similars.

18. Qualsevol altre número identificatiu únic, característica o codi.

Tabla 8. Requisits per desidentificar la informació de salut protegida. HIPAA § 164.514 (b).

Desidentificació acceptable: "El 2001, una dona de 30 anys llatina va donar a llum un fill amb síndrome de Down en un hospital de la comunitat. Anomenarem a la mare Maria i al nadó Roberto".

Desidentificació no acceptable: "El 23 de juliol de 2001, una dona de 30 anys llatina va donar a llum a un fill amb síndrome de Down a l'Hospital Memorial a Houston, TX. El seu nom era Letitia i el seu fill Antonio".

La norma de seguretat (HIPAA Security Rule).

La norma de seguretat abasta la mateixa informació que la que preveu la norma de privacitat, però només quan aquesta informació està en format electrònic. Mentre la norma de privacitat regula el que cal protegir, la norma de seguretat regula la forma de fer-ho.

La norma de seguretat exigeix:

- Un responsable de seguretat de la informació.
- Una anàlisi de riscos.
- L'assegurament de la qualitat (QA).
- Formació.

La norma de seguretat diu que la responsabilitat de la seguretat ha de ser assignada a una persona específica per a donar la importància deguda i un enfocament organitzatiu a la seguretat. El responsable de seguretat pot ser qualsevol persona de l'organització.

La norma de seguretat requereix l'anàlisi de riscos: la identificació de possibles amenaces i vulnerabilitats, l'estimació de les pèrdues potencials a partir de les amenaces, la identificació de les salvaguardes i la mesura en què aquestes redueixen l'exposició a les amenaces.

La norma de seguretat requereix l'elaboració i manteniment de polítiques i procediments de seguretat en forma escrita.

La norma de seguretat requereix la formació del personal de forma raonable i adequada per a realitzar les seves funcions en la instal·lació.

La norma es va publicar el 20 de febrer de 2003 i va entrar en vigor el 21 d'abril de 2003. La data de compliment és el 21 d'abril de 2005, per a les entitats cobertes i el 21 d'abril de 2006, per als plans d'assegurances petits. La norma complementa la norma de Privacitat. Si bé la norma de privacitat es refereix a tota la Informació de Salut Protegida (PHI), tant de forma electrònica com en paper, la regla de seguretat s'ocupa específicament de la Informació de Salut Protegida Electrònica (EPHI). S'estableixen tres tipus de mesures de seguretat: administratives, físiques i tècniques. Per a cadascun d'aquests tipus, estableix una sèrie de normes i, per a cada norma, cita tant especificacions d'implementació requerides com opcionals. Les especificacions requerides han de ser adoptades i administrades segons el que dicta la norma. Les especificacions opcionals són més flexibles. Les entitats cobertes poden avaluar la seva pròpia situació i determinar la millor manera d'implementar les especificacions opcionals.

Salvaguardes Administratives – polítiques i procediments dissenyades per mostrar clarament com l'entitat complirà amb la norma.

- ✓ Les entitats cobertes (entitats que han de complir amb els requisits HIPAA) han d'adoptar un conjunt escrit de procediments de privadesa i designar un responsable de desenvolupar i implementar tots els procediments i polítiques necessàries.
- ✓ Els procediments han d'identificar amb claredat les categories d'empleats que tindran accés a la informació electrònica de salut protegida (EPHI). L'accés a l'EPHI s'ha de limitar només a aquells empleats que la necessiten per fer el seu treball.
- ✓ Els procediments han d'abordar l'autorització d'accés, l'establiment, modificació i finalització.
- ✓ Les entitats han de demostrar que proporciona als empleats que realitzen funcions administratives del pla de salut un programa adequat de formació sobre el tractament de la PHI.
- ✓ Les entitats cobertes que externalitzen alguns dels seus processos de negoci a un tercer, s'han d'assegurar que els seus proveïdors també compleixen amb els requisits de la HIPAA.
- ✓ Cal un pla de contingència per a respondre a les emergències. Les entitats cobertes són responsables de les còpies de seguretat de totes les dades i de tenir procediments de recuperació davant de sinistres. El pla ha de documentar la prioritat de les dades i fer una anàlisi de fallides, activitats de comprovació, i procediments de control de canvis.
- ✓ Les auditories internes juguen un paper clau en el compliment de l'HIPAA mitjançant la revisió de les operacions amb l'objectiu d'identificar possibles violacions de seguretat. Les polítiques i procediments han de documentar l'abast, la freqüència i els procediments de les auditories. Cal que hi hagi auditories rutinàries i especials (basades en esdeveniments).
- ✓ Els procediments han de documentar les instruccions per fer front i respondre a les violacions de seguretat que s'identifiquin ja sigui durant l'auditoria o el curs normal d'operacions.

- ***Salvaguardes Físiques*** – control de l'accés físic per protegir l'accés inadequat a les dades.

  - ✓ Han de regular la introducció i eliminació del hardware i software de la xarxa. Quan es retira l'equip cal assegurar que no es posa en perill la PHI.
  - ✓ Cal monitoritzar i controlar detalladament l'accés als equips que contenen informació de salut.
  - ✓ Cal limitar l'accés del hardware i software a les persones autoritzades.
  - ✓ Els controls d'accessos consisteixen en plans de protecció de les instal·lacions, registres de manteniment, registre de visitants i serveis d'escorta.
  - ✓ Les polítiques han d'abordar l'ús adequat de l'estació de treball. Cal eliminar les estacions de treball de les àrees amb molt trànsit i els monitors no han d'estar a la vista directa del públic.
  - ✓ Si les entitats cobertes utilitzen contractistes o agents, ells també han de complir plenament les seves responsabilitats d'accés físic.

- ***Salvaguardes Tècniques*** – controlar l'accés als sistemes informàtics i habilitar a les entitats cobertes per evitar que siguin interceptades les comunicacions que continguin informació personal de salut transmesa electrònicament per xarxes obertes amb l'excepció del receptor legítim.

    - ✓ Cal protegir dels intrusos els sistemes d'informació que allotgen PHI. Si s'utilitzen xarxes obertes, cal utilitzar alguna forma d'encriptació. Si s'utilitzen xarxes tancades, es consideren suficients els controls d'accés existents i el xifrat és opcional.
    - ✓ Cada entitat coberta és responsable d'assegurar que les dades dins dels seus sistemes no han estat modificades o esborrades de manera no autoritzada.
    - ✓ Es pot utilitzar la verificació de dades, incloent l'ús de la suma de comprovació, doble codificació, autenticació de missatges, i la signatura digital per a garantir la integritat de les dades.
    - ✓ Les entitats cobertes han d'autenticar les entitats amb les quals es comuniquen. L'autenticació consisteix en comprovar que l'entitat és qui diu ser. Exemples de verificació inclouen: sistemes de contrasenyes, two or three-way handshakes (encaixades de mans de dues o tres vies), devolució de trucades de telèfon i sistemes de token.
    - ✓ Les entitats cobertes han d'enviar la documentació de les seves pràctiques HIPAA al govern per determinar el grau de compliment.
    - ✓ A més de les polítiques i procediments i els registres d'accés, la documentació també ha d'incloure un registre escrit de tots els valors de configuració dels components de la xarxa, ja que aquests components són complexos i en constant evolució.
    - ✓ És obligatori fer una anàlisi de risc documentat i programes de gestió de riscos. Les entitats cobertes han de considerar acuradament els riscos de les seves operacions. El requisit d'anàlisi de riscos i gestió del risc implica que els requisits de seguretat de la llei són un estàndard mínim. És responsabilitat de les entitats cobertes prendre totes les precaucions raonables necessàries per evitar que la PHI s'utilitzi per a fins no sanitaris.

Anàlisi de la HIPAA.

HIPAA té com a objectiu garantir la seguretat i privadesa de la informació mèdica personal. Per aconseguir aquests objectius estableix una sèrie de salvaguardes administratives, físiques i tècniques. La taules següents mostren les normes publicades, amb una referencia a la secció on es regulen i les implementacions associades. R vol dir que l'especificació descrita a la norma és obligatòria mentre que A vol dir que és opcional (es pot implementar com diu la norma o de manera alternativa). Les taules següents mostren les salvaguardes definides pel reglament de seguretat HIPAA [32].

Normes	Seccions	Especificacions d'implementació (R) Required, Requerit (A) Addressable, Opcional	
Procés de Gestió de Seguretat	164.308(a)(1)	Anàlisi de Risc	(R)
		Gestió de Risc	(R)
		Política de Sancions	(R)
		Revisió de l'Activitat del SI	(R)
Responsabilitat de Seguretat Assignada	164.308(a)(2)		(R)
Seguretat del Personal	164.308(a)(3)	Autorització i/o Supervisió	(A)
		Procediment d'Evacuació del Personal	(A)
		Procediments de Finalització	(A)
Gestió d'Accés a la Informació	164.308(a)(4)	Aïllament de les dependències	(R)
		Autorització d'accés	(A)
		Establiment i modificació de l'accés	(A)
Alertes de Seguretat i Formació	164.308(a)(5)	Avisos de Seguretat	(A)
		Protecció del Programari Maliciós	(A)
		Supervisió de log-in	(A)
		Gestió de contrasenyes	(A)
Procediments d'Incidències de Seguretat	164.308(a)(6)	Resposta i Informes	(R)
Pla de Contingència	164.308(a)(7)	Pla de Salvaguarda de Dades	(R)
		Pla de Recuperació d'Accidents	(R)
		Pla d'Operació de Recuperació	(R)
		Procediment de Revisió i Proves	(A)
		Anàlisi d'Aplicacions i Criticitat de les Dades	(A)
Avaluació	164.308(a)(8)		(R)
Contractes Associats al Negoci i Altres Acords	164.308(b)(1)	Contracte Escrit o un Altre Acord	(R)

Tabla 9. Salvaguardes administratives.

Normes	Seccions	Especificacions d'Implementació (R) Requerit (A) Opcional	
Control d'Accés a les Instal·lacions	164.310(a)(1)	Operacions de Contingència	(A)
		Pla de Seguretat de les Instal·lacions	(A)
		Procediments de Control d'Accés i Validacions	(A)
		Registres de Manteniment	(A)
Ús de l'estació de Treball	164.310(b)		(R)
Seguretat de l'estació de Treball	164.310(c)		(R)
Control de Dispositius i Mitjans de Comunicació	164.310(d)(1)	Eliminació	(R)
		Reutilització	(R)
		Responsabilitat	(A)
		Salvaguarda i emmagatzematge de dades	(A)

Tabla 10. Salvaguardes físiques.

Normes	Seccions	Especificacions d'Implementació (R) Requerit (A) Opcional	
Control d'Accés	164.312(a)(1)	Identificació Única d'Usuari	(R)
		Procediment d'Accés d'Emergència	(R)
		Logoff Automàtic	(A)
		Xifrat i Desxifrat	(R)
Controls d'Auditoria	164.312(b)		(R)
Integritat	164.312(c)(1)	Mecanisme per Autenticar la Informació de Salut Protegida Electrònica	(A)
Autenticació de Persona o Entitat	164.312(d)		(R)
Seguretat de la Transmissió	164.312(e)(1)	Controls d'Integritat	(A)
		Xifrat	(A)

Tabla 11. Salvaguardes tècniques.

3.2. Estàndards.

Mentre els Sistemes d'Informació Hospitalaris (HIS) o els Sistemes d'Informació Clínics (CIS) no utilitzin estàndards que facilitin l'intercanvi electrònic de les dades, no és possible que la informació estigui disponible al punt d'atenció on es troba el pacient, independentment de la institució prestadora de serveis de salut on sigui atès. L'ús d'una història clínica electrònica compartida per múltiples institucions i la interoperabilitat dels documents electrònics que componen l'HCE, independentment de les plataformes de programari que utilitzin, fa necessari que els sistemes d'informació que utilitzen les institucions implementin estàndards informàtics internacionalment reconeguts, per tal de garantir la seguretat i privadesa de la informació. Tot seguit es presenta una relació de les normes i especificacions més rellevants.

3.2.1. Normes.

- ANSI X12 : protocol utilitzat per transmetre dades del pacient (mèdiques, de facturació, etc.) [33].
- TC/251 de CEN : estableix diverses normes europees HCE.
  - ✓ EN 13606 : estàndard per a la comunicació d'informació de sistemes HCE [34].
  - ✓ CONTSYS (EN 13940) : sistema per donar suport a la continuïtat de l'atenció mèdica [35].
  - ✓ HISA (EN 12967) : estàndard de serveis per a la comunicació entre sistemes en un entorn d'informació clínica [36].
- Continuity of Care Record : norma ASTM (American Society for Testing and Materials) sobre continuïtat del registre d'atenció mèdica [37].
- DICOM : estàndard per a la representació i comunicació d'imatges radiològiques i presentació d'informes [38].
- HL7 : format de missatges per a l'intercanvi entre diferents sistemes de registres i sistemes de gestió [39].
- ISO TC 215 : estableix les especificacions tècniques internacionals HCE [40].
- Title 21 CFR Part 11 : estableix normes d'aplicació per als registres electrònics i per a la signatura electrònica [41].
- Guidance for Industry Computerized Systems Used in Clinical Investigations : estableix directrius d'aplicació en els sistemes informatitzats en les investigacions clíniques [42].

3.2.2. Especificacions obertes.

- openEHR : una especificació oberta per a una història clínica compartida amb contingut web desenvolupada online per experts. Forta capacitat multilingüe [43].

Capítol 4. Literatura científica.

Al capítol anterior, hem vist que la legislació estableix una sèrie de propietats que han de complir els historials mèdics electrònics per tal de garantir la seguretat i privadesa de la informació. En concret:

- Autenticació: Cal autenticar els usuaris (pacients, metges, infermeres, personal d'administració, etc.) ja que cada usuari tindrà unes funcions diferents.

    - ✓ Normes d'aplicació: RD art. 91, 93, 98 ; HIPAA 164.312(d)

- Confidencialitat: La informació ha de ser confidencial, ja que es tracta d'informació molt sensible. Aquesta confidencialitat s'ha de garantir tant durant el transport de la informació per una xarxa de comunicacions com en el moment de guardar la informació en una base de dades.

    - ✓ Normes d'aplicació: RD art. 104; HIPAA 164.312(a)(1); 164.312(e)(1)

- Integritat: Cal garantir la integritat de la informació per tal que aquesta no pugui ser modificada per personal no autoritzat.

    - ✓ Normes d'aplicació: LOPD art.9.2; HIPAA 164.312(c)(1)

- Control d'accés a la informació: També cal garantir l'accés a la informació de manera que el seu accés ha de quedar restringit exclusivament a aquelles persones que necessiten conèixer la informació per a realitzar el seu treball.

    - ✓ Normes d'aplicació: LOPD art. 9, RD art. 91, 103; HIPAA 164.312(a)(1)

- Privadesa: Finalment, cal garantir la privadesa de manera que la informació que fa referència a una persona no es faci pública sense el seu consentiment.

    - ✓ Normes d'aplicació: LOPD art. 3.f ; HIPAA 164.514

En aquest capítol es farà una recerca sobre la literatura científica relativa a historials clínics en format electrònic i també sobre les implementacions existents.

Per a realitzar aquest treball, s'ha començat per fer una prospecció dels articles científics relatius a aquest tema. A partir dels articles recollits, s'ha fet una selecció dels que s'han considerat més interessants des de la perspectiva de la seguretat.

L'objectiu d'aquest capítol és analitzar si els articles tracten aquestes propietats i amb quines tècniques.

Cadascuna d'aquestes propietats es tractarà en un apartat diferent d'aquest capítol.

4.1. Autenticació.

Abans que una persona pugui començar a treballar en el sistema, cal un control d'accés que identifiqui la persona i comprovi si està autoritzat a entrar en el sistema.

Amb l'autenticació es dóna resposta a la qüestió: És aquesta persona qui diu que és?

Els autors utilitzen diverses tècniques per a implementar l'autenticació de l'usuari:

- Targetes criptogràfiques.
- Certificats (criptografia de clau pública).
- Biometria.
- Validació de claus en una base de dades.
- Autenticació dels usuaris en un servidor RADIUS/LDAP.
- Signatura digital.
- Usuari i password.

4.1.1. Targetes intel·ligents.

Als treballs **[47]**, **[50]**, **[55]**, **[56]** i **[57]** l'autenticació dels usuaris és realitza a partir d'una targeta intel·ligent que se'ls lliura. En el llibre de W. Rankl i W. Effing **[59]** es pot consultar més informació sobre les característiques i funcionament de les targetes intel·ligents.

Un cas a destacar és el sistema nacional holandès **[55]** on els sistemes d'informació descentralitzats (p.e., hospitals, clíniques, etc.) estan connectats a la part central de la infraestructura, la qual autoritza i registra tots els intents d'accedir a la informació. El procés d'autorització porta implícit un mecanisme d'autenticació centralitzat. Els professionals sanitaris poden accedir al sistema amb una targeta intel·ligent personal que conté un parell de claus públiques i privades. Aquesta targeta intel·ligent està protegida amb un PIN, i s'anomena Unique Healthcare Provider Identification Pass (UZI pass). Cada targeta intel·ligent conté un certificat amb la titulació, l'especialització i la funció del professional sanitari, expedit per una PKI basada en els registres professionals d'Holanda. Aquesta informació és utilitzada pel sistema per implementar el control d'accés basat en rols.

Els autors a **[56]** utilitzen targetes intel·ligents. Per accedir a les dades bàsiques d'una targeta intel·ligent, cal una operació d'identificació per activar la targeta, per exemple un mecanisme conegut és introduir un número d'identificació personal (PIN) o dades biomètriques.

En el sistema proposat a **[57]** cada pacient disposa d'una targeta intel·ligent que inclou informació personal, els registres mèdics d'emergència, les dades d'identificació personal, i la

clau per xifrar/desxifrar la informació personal de salut. Com a part del procés de registre, el pacient ha d'anar a l'autoritat sanitària i proporcionar la informació necessària i la contrasenya de la targeta intel·ligent. L'autoritat sanitària genera una clau secreta i la guarda en la targeta intel·ligent. La clau que s'utilitza en el sistema s'obté a través del PIN i la contrasenya. Per tant, si la persona va a l'hospital, la informació codificada a la targeta intel·ligent pot ser desxifrada amb el PIN i la contrasenya correctes. D'aquesta manera, es garanteix l'autenticació de la persona.

4.1.2. Criptografia de clau pública.

En el sistema proposat a **[44]** es garanteix l'autenticació dels usuaris amb **certificats.** Un certificat digital (també conegut com certificat de clau pública o certificat d'identitat) és un document digital mitjançant el qual un tercer confiable (una autoritat de certificació) garanteix la vinculació entre la identitat d'un subjecte o entitat (nom, adreça i altres aspectes d'identificació) i una clau pública.

En la referència **[60]** es pot consultar més informació sobre l'ús dels certificats digitals.

4.1.3. Identificació biomètrica.

Els autors a **[48]** fan servir el reconeixement de l'iris, una tecnologia **biomètrica** que escaneja l'iris d'una persona i mesura els seus patrons únics. Es considera el sistema d'autenticació més precís disponible en l'actualitat.

4.1.4. Validació de claus en una base de dades.

Els autors a **[46]** **validen les claus dels usuaris en una base de dades** central d'autenticació. Tots els accessos a pàgines web són autoritzats pel servidor web que utilitza aquesta base de dades.

4.1.5. Servidor d'autenticació.

Els autors a **[49]** realitzen l'autenticació dels usuaris en un servidor **RADIUS** (Remote Authentication Dial-In User Server) o en un servidor **LDAP** (Lightweight Directory Access Protocol)**.**

RADIUS és un protocol d'autenticació i autorització per a aplicacions d'accés a la xarxa. Quan es realitza la connexió s'envia una informació que generalment és un nom d'usuari i una contrasenya. Aquesta informació és transferida a un dispositiu NAS (Servidor d'Accés a la Xarxa) sobre el protocol PPP, qui redirigeix la petició a un servidor RADIUS sobre el protocol RADIUS. El servidor RADIUS comprova que la informació és correcta fent servir esquemes d'autenticació com PAP, CHAP o EAP. Si és acceptat, el servidor autoritza l'accés al sistema de l'ISP i li assigna els recursos de xarxa com una adreça IP. Una de les característiques més importants del protocol RADIUS és la seva capacitat de gestionar sessions, notificant quan

comença i finalitza una connexió, així es pot determinar el consum de cada usuari i facturar en conseqüència. Les dades també es poden emprar amb propòsits estadístics.

LDAP és un protocol a nivell d'aplicació que permet l'accés a un servei de directori ordenat i distribuït per a cercar diversa informació en un entorn de xarxa. Habitualment, emmagatzema la informació de login (usuari i password) i és utilitzat per a autenticar-se tot i que és possible emmagatzemar altres tipus d'informació (dades de contacte de l'usuari, ubicació de diversos recursos de la xarxa, permisos, certificats, etc.).

4.1.6. Signatura digital.

La signatura digital pot autenticar l'origen dels missatges. Quan la propietat d'una clau secreta de signatura digital està lligada a un usuari específic, una signatura vàlida mostra que el missatge va ser enviat per l'usuari.

El sistema proposat a **[52]** utilitza signatura basada en identitat jeràrquica (HIDS, hierarchical ID-based signature) en el cas de l'autenticació inter-domini i signatura basada en identitat estàndard (IBS, standard ID-based signature) en el cas de l'autenticació intra-domini.

4.1.7. Usuari i password.

Els autors a **[58]** avaluen HealthVault de Microsoft i Google Health. Pel que fa a l'autenticació, HealthVault és més flexible ja que és possible fer-ho amb **usuari i password** en un compte Windows Live ID o en comptes de diversos proveïdors, així com utilitzant altres dispositius de seguretat com ara targetes intel·ligents, certificats o tokens físics. En canvi, Google només ofereix un inici de sessió amb login i password en un compte propi de Google. El sistemes basats en usuari i password són fàcils de desplegar però el seu nivell de seguretat és baix.

4.2. Confidencialitat.

Cal protegir la informació de manera que només la pugui veure el personal autoritzat.

La propietat de la confidencialitat dóna resposta a la qüestió: Té accés a la informació només el personal autoritzat?

Cal tenir present que és important garantir la confidencialitat de la informació tant durant el seu transport per una xarxa de comunicacions com en el moment de guardar la informació en una base de dades. En el primer cas, la confidencialitat es garanteix amb xifrat a nivell de comunicació (SSL/TLS). En el segon cas, en el moment de guardar la informació en una base de dades generalment el text està en clar. Si volem garantir la confidencialitat de la informació emmagatzemada en la base de dades caldrà xifrar el text amb xifrat a nivell d'aplicació (sobre digital, AES, DES, etc.).

4.2.1. Protocol SSL.

Als treballs **[44]**, **[55]**, **[58]** es garanteix la confidencialitat de les dades durant el transport amb l'ús del protocol **SSL**.

4.2.2. Xifrat.

Els autors a **[45]**, **[48]**, **[47]**, **[49]**, **[50]**, **[52]**, **[56]**, **[57]** fan servir diverses tècniques de **xifrat** per garantir la confidencialitat a nivell d'aplicació.

Els treballs **[45]**, **[48]** garanteixen la confidencialitat de la informació amb l'ús de criptografia de clau pública.

El sistema proposat a **[47]** usa la targeta intel·ligent del pacient (P-SmartCard) per xifrar el contingut de l'HCE del pacient.

Els autors a **[49]** fan servir els protocols WPA, 802.11i, IPSec (ESP).

La descripció del protocol WPA (Wi-Fi Protected Access) es pot trobar a **[61]**. Per a més informació del protocol 802.11i consultar la referència **[62]**. El protocol IPSec (ESP) està descrit en la referència **[63]**. Triple DES-CBC i AES-CBC són els algorismes criptogràfics definits per a l'ús amb IPSec (ESP).

WPA, 802.11i, IPSec (ESP) garanteixen la confidencialitat a nivell de transport exclusivament.

El sistema proposat a **[50]** utilitza un algorisme de xifrat simètric per xifrar la informació de manera que només els pacients poden desxifrar la seva informació amb la clau de xifrat. Aquesta clau de xifrat és protegida amb paraula de pas o bé es xifra amb la clau pública del pacient mitjançant un algorisme de clau pública abans d'enviar-la per la xarxa (sobre digital).

El treball **[52]** garanteix la confidencialitat de les dades del pacient compartides entre el delegant i el delegat mitjançant PEKS. A més, es garanteix la confidencialtat dels missatges intercanviats amb esquemes de xifrat (HIBE, IBE).

Els autors a **[56]** utilitzen criptografia de clau simètrica AES (Advanced Encryption Standard) amb claus de 256 bits, que és un sistema que presenta alta seguretat i bon rendiment. AES és un dels algorismes més populars usats en criptografia simètrica. És un esquema de xifrat per blocs. Té una grandària de bloc fix de 128 bits i mides de clau de 128, 192 o 256 bits.

El sistema proposat a **[57]** aplica criptografia de clau simètrica DES (Data Encryption Standard). Avui es considera que el DES no és segur per moltes aplicacions, principalment perquè la mida de la clau de 56 bits és massa petita. Es creu que en la forma de Triple DES l'algorisme és pràcticament segur, tot i que en teoria els atacs continuen sent possibles. En els últims anys, aquest xifratge ha estat superat per l'AES (Advanced Encryption Standard).

4.3. Integritat.

Cal garantir que la informació només pugui ser modificada per personal autoritzat. En cas de modificació cal saber qui l'ha modificat, quan i com.

La propietat de la integritat dóna resposta a la qüestió: S'ha modificat la informació? Per qui, quan i com?

Aquesta propietat s'implementa principalment amb la signatura digital utilitzant criptografia de clau pública. També es poden utilitzar tokens criptogràfics.

4.3.1. Signatura digital.

Els autors a **[44]**, **[45]**, **[47]**, **[48]**, **[52]**, **[56]**, **[57]** garanteixen aquesta propietat mitjançant la **signatura digital** (criptografia de clau pública). Es pot trobar una descripció detallada del seu funcionament a **[64]**.

El treball **[47]** fa ús de les targetes intel·ligents (HP-SmartCard) per signar les transaccions.

El sistema que es proposa a **[52]** garanteix aquesta propietat mitjançant signatura digital (HIDS, IBS) o un codi d'autenticació de missatge (MAC). Es pot trobar una descripció detallada del funcionament del codi d'autenticació de missatge a la referència **[65]**.

Les propostes **[56]** i **[57]** adopten DSS (Digital Signature System). DSS fa servir DSA (Digital Signature System). A la referència **[66]** es pot trobar una descripció detallada de l'ús de l'algorisme DSA, la informació que se signa i la informació que cal protegir per evitar els atacs.

4.3.2. Tokens criptogràfics.

Un cas a destacar és el sistema nacional holandès **[55]** on totes les dades són transferides en un missatge HL7. Cada petició que s'envia al sistema central s'associa amb un token (estructura de dades amb informació utilitzada pel sistema central per verificar l'autenticitat i la integritat de la petició). El sistema central compara el contingut del token amb el missatge HL7. Els pacients són identificats amb un número anomenat BSN. El token conté el BSN del pacient que ha fet la petició i la categoria de la informació. El token és signat pel professional de salut amb la seva targeta intel·ligent abans d'enviar la petició al sistema central. La signatura en el token permet al sistema central autenticar el professional que ha fet la petició.

4.3.3. Protocol IPSec (AH).

Els autors a **[49]** garanteixen la integritat utilitzant el protocol IPSec (AH). El protocol està descrit en la referència **[63]**. HMAC-SHA-1 és l'algorisme criptogràfic definit amb IPSec (AH) per a protecció d'integritat. IPSec (AH) garanteix la integritat a nivell de transport exclusivament.

4.4. Accés a la informació.

Una vegada autenticada la persona, cal definir les funcions que podrà realitzar cada usuari.

En aquest cas es dóna resposta a la qüestió: qui pot accedir a què?

Hi ha diferents maneres de controlar l'accés a la informació. Bjørn-Erik Stenbakk et al. **[67]** fan un estudi dels models de control d'accés més utilitzats en el sector sanitari.

4.4.1. Control d'accés basat en rols.

Els autors a **[53], [55]** adopten el control d'accés basat en rols per controlar l'accés a la informació.

El treball **[53]** proposa un model de control d'accés basat en rols contextuals amb l'objectiu d'augmentar la privacitat i la confidencialitat de les dades del pacient, i que a la vegada sigui prou flexible. Aquest model regula l'accés de l'usuari a l'HCE sobre la base de les funcions de l'organització. Estableix una jerarquia de rols on les autoritzacions es poden heretar. També s'introdueix el concepte d'autorització positiva i negativa, així com la separació estàtica i dinàmica de funcions basada en conflictes en els rols. Les autoritzacions contextuals utilitzen informació de l'entorn, com la relació usuari/pacient, amb la finalitat de decidir si un usuari pot tenir accés a un recurs de l'HCE. Això permet especificar una política d'autorització més flexible i precisa, on el permís és concedit o denegat d'acord amb la necessitat de l'usuari per dur a terme una funció particular.

En el cas del sistema nacional holandès **[55]** els professionals de la salut poden tenir accés al sistema amb una targeta intel·ligent personal que conté un parell de claus públiques i privades. Aquesta targeta intel·ligent està protegida per un codi PIN, i s'anomena UZI pass. Cada usuari disposa d'una targeta intel·ligent que conté un certificat amb informació sobre titulació mèdica, especialitat i la funció del professional, expedit per una PKI en base als registres professionals holandesos. Aquesta informació és utilitzada pel sistema per al control d'accés basat en rols. El sistema defineix dues polítiques d'autorització per concedir l'accés als registres dels pacients. En primer lloc, el protocol d'autorització estableix si un determinat professional (metge, farmacèutic, etc.) està autoritzat a accedir a un determinat tipus de registre del pacient. Per exemple, a un metge se li permet inspeccionar els registres creats per un farmacèutic, així com els registres creats per altres metges que han tractat al pacient. En canvi, un farmacèutic no pot veure el registre d'un pacient creat per un metge. El protocol d'autorització és acordat a nivell nacional pels metges i les organitzacions de salut, i el sistema obliga al seu compliment. En segon lloc, els pacients poden definir un perfil d'autorització granular, que els permet definir quins professionals de la salut o quins proveïdors d'atenció mèdica (hospitals o altres organitzacions) poden accedir als seus registres.

4.4.2. Targetes intel·ligents.

Les propostes **[47], [56], [57]** controlen l'accés a la informació amb targetes intel·ligents.

Els autors a **[47]** estableixen un sistema de control d'accés basat en regles de l'historial mèdic del pacient amb una targeta intel·ligent de pacient anomenada P-SmartCard.

En el sistema proposat **[56]** la clau mestre del pacient (necessària per tal de desxifrar la informació personal de salut) és controlada pel propi pacient ja que és qui té la targeta intel·ligent i la informació per activar-la. Per tant, degut al mecanisme de seguretat de la targeta intel·ligent, el pacient pot controlar completament l'ús de la clau per mostrar la seva informació de salut personal en cas de consentiment.

Els autors a **[57]** controlen l'ús i divulgació de la informació personal de salut amb DES. L'hospital i l'autoritat sanitària han de garantir que només el pacient i els usuaris autoritzats poden tenir accés a la PHI. El pacient pot entrar la seva contrasenya per obtenir la seva clau mestra i, amb ella, recuperar la seva informació personal (PHI). Avui es considera que el DES no és segur per moltes aplicacions, principalment perquè la mida de la clau de 56 bits és massa petita i s'han proposat criptosistemes més robustos com TDES o AES.

4.4.3. Claus de validació.

Els autors de l'article **[46]** utilitzen claus de validació (I-Keys) tant per als professionals com per als pacients. Així, un pacient pot autoritzar a un professional que disposi d'una clau, prèviament validada en una base de dades, a accedir al seu historial mèdic. Es demana al metge que entri la clau cada vegada que arrenqui el seu equip. Si entra una clau vàlida, el metge és autoritzat a accedir a l'historial del pacient. Però només la inserció posterior d'una clau de pacient vàlida activa l'accés efectiu a la història clínica del pacient. Aquest procés substitueix el mètode que només permet a un únic metge a accedir a un registre d'un pacient determinat cada vegada. No obstant això, els pacients poden accedir externament al seu propi registre amb el mètode d'accés basat en nom d'usuari i contrasenya.

4.4.4. Certificat digital.

El sistema proposat a **[48]** fa servir un certificat digital que detalla els privilegis d'accés i d'escriptura del titular del certificat i el seu període de validesa. Per més informació sobre el control d'accés basat en els atributs de seguretat d'un certificat es pot consultar la referència **[68]**.

4.4.5. HDB.

Els autors del treball **[51]** especifiquen la política d'autorització en una base de dades hipocràtica (HDB) amb el llenguatge APPEL. Els metges són autoritzats en base a aquestes polítiques. El treball identifica la necessitat d'autoritzacions més granulars i proposa una solució basada en un esquema de BD modificat. El treball mostra l'ús d'estructures jeràrquiques per tal de millorar el control d'accés. La plataforma P3P (platform for privacy

preference) desenvolupada per W3C estableix una plataforma de preferències de privacitat que permet als usuaris declarar les polítiques i preferències de privacitat en un format llegible per un ordinador. D'altra banda, les bases de dades hipocràtiques constitueixen un marc ideal per obligar a complir les polítiques de privacitat. La integració de P3P i aquestes bases de dades suposen una solució natural per tal de preservar la privacitat dels sistemes d'eSalut. En aquest treball, es comenten diversos temes relacionats amb la integració de P3P i HDB. En primer lloc, es dissenya una arquitectura per integrar les preferències P3P amb les polítiques HDB. S'estableix una relació entre les preferències del pacient especificades en APPEL (el llenguatge de P3P per definir les preferències de privacitat) i les taules de metadades de privacitat de l'HDB. Els metges que demanin dades privades són autoritzats contra les metadades de privacitat contingudes en l'HDB. En segon lloc, es proposa un sistema que permet autoritzacions més granulars basades en la modificació de l'esquema de base de dades.

4.4.6. PEKS.

En la publicació **[52]** la delegació és el mecanisme de control d'accés a la informació. La delegació és un control d'accés general ja que només les persones amb els drets adients poden accedir a les dades del pacient. Tanmateix, la delegació de drets es basa en rols, el que significa que s'atorga al delegat tots els drets associats amb aquell rol, i això possiblement inclou més permisos dels necessaris. Aquest control d'accés és insuficient. Per tal de tenir més control sobre l'accés a les dades per part del delegat, el delegant pot establir un control d'accés més granular i fi que limiti l'accés exclusivament a les dades estrictament necessàries. Aquest control d'accés granular es basa en PEKS.

4.4.7. Perfils.

Els autors a **[58]** avaluen HealthVault de Microsoft i Google Health. En ambdós casos, l'usuari està autoritzat automàticament a veure i editar el seu compte. A més, és possible compartir el registre o afegir un perfil addicional. Amb HealthVault de Microsoft es pot especificar amb precisió el tipus de dades que l'usuari pot veure, mentre que amb Google Health la informació es comparteix a nivell de perfil.

4.5. Privadesa.

Segons el TERMCAT la privadesa és la condició per la qual la informació que fa referència o pertany a una persona física o jurídica no es pot fer pública sense el consentiment de l'afectat.

En aquest cas es dóna resposta a la qüestió: es poden assignar les dades a una persona concreta?

No ha de ser possible associar les dades de l'anamnesi amb un pacient concret. L'anamnesi és el terme mèdic emprat per referir-se a la informació proporcionada pel pacient al metge durant la consulta clínica i incorporada a la història clínica. És el conjunt de dades relatives al pacient, que comprenen antecedents familiars i personals, símptomes, experiències i records que es fan servir per analitzar la seva situació clínica. És un historial clínic que pot proporcionar informació rellevant per diagnosticar possibles malalties.

Aquesta propietat s'implementa principalment mitjançant el procediment de dissociació. La dissociació de la informació és el procés mitjançant el qual se separen les dades personals de les dades de l'anamnesi de manera que no és possible associar les dades mèdiques amb cap persona en concret. L'article 3 f) de la LOPD defineix el procediment de dissociació com qualsevol tractament de dades personals de manera que la informació que s'obtingui no es pugui associar a una persona identificada o identificable.

4.5.1. Dissociació.

Les propostes **[50] i [58]** fan servir la tècnica de la dissociació per garantir la privadesa de la informació.

Un cas a destacar és el treball **[50]** que, a més de la dissociació, proposa altres tècniques com l'ús de pseudònims, expressions regulars, filtres, etc.

Els autors a **[58]** avaluen HealthVault de Microsoft i Google Health. Sota la política de privadesa de Google Health, està protegida la informació d'identificació personal. La informació dissociada, incloent les dades dels logs anònims, és restringida i no pot ser compartida amb tercers. La informació dissociada i agregada de l'usuari es pot utilitzar per a publicar tendències.

4.5.2. Desidentificació.

El sistema proposat a **[54]** fa un estudi de diversos treballs orientats a garantir la privacitat d'un HCE. Aquests treballs utilitzen una tècnica anomenada desidentificació que consisteix en eliminar la informació personal de manera que la informació mèdica no pugui ser associada amb cap persona en concret. Anonimització i desidentificació s'utilitzen sovint indistintament, però desidentificació només significa que s'eliminen o s'amaguen els identificadors explícits. En canvi, anonimització implica que les dades no poden ser vinculades per a identificar el pacient. Per tant, sovint les dades desidentificades no són completament anònimes, és a dir, no es pot excloure la possibilitat de reidentificar el pacient.

Sweeny demostra que es pot reidentificar pacients a partir de dades desidentificades http://www.swiss.ai.mit.edu/classes/6.805/articles/privacy/sweeney-thesis-draft.pdf.

La desidentificació dels documents de text es fa sovint de forma manual i requereix molts recursos. Conscients d'això, diversos autors han investigat la desidentificació automatitzada d'un HCE. Els autors fan una revisió de diversos treballs de recerca sobre el tema. Tots els sistemes tenen com a objectiu identificar i eliminar noms de persones i molts inclouen altres tipus d'informació personal de salut (PHI). La majoria de sistemes només utilitzen un o dos tipus de documents, i es basen principalment en dos grups diferents de metodologies: la coincidència de patrons i l'aprenentatge automàtic. Molts sistemes combinen tots dos enfocaments per a diferents tipus de PHI, però la majoria no utilitza l'aprenentatge automàtic i es basen només en la coincidència de patrons, regles i diccionaris.

4.6. Comentari general de l'estudi realitzat.

La taula següent és un resum dels treballs analitzats. La primera columna mostra la referència del treball (consultar la bibliografia). Les columnes següents mostren una sèrie de requeriments de seguretat i privadesa. En la intersecció de les files i columnes es mostren les tècniques utilitzades per garantir el compliment dels requeriments.

Treball	Requeriments de seguretat i privadesa				
	Autenticació	Confidencialitat	Integritat	Accés a la informació	Privadesa
[44]	Certificat	SSL	Signatura	-	-
[45]	-	PKC	Signatura/HF	-	-
[46]	Claus Validades	-	-	Claus Validades	-
[47]	SmartCard	SmartCard	SmartCard	SmartCard	-
[48]	Biometria	PKC	Signatura	Certificat	-
[49]	RADIUS/LDAP	WPA/ IPSec (ESP)	IPSec (AH)	-	-
[50]	SmartCard	Sobre digital	Signatura	-	Dissociació/Altres
[51]	-	-	-	HDB	-
[52]	HIDS/IBS	PEKS	HIDS/IBS	PEKS	-
[53]	-	-	-	RBAC	-
[54]	-	-	-	-	Desidentificació
[55]	SmartCard	SSL	Tokens	RBAC	-
[56]	SmartCard	AES	Signatura/HF	SmartCard	-
[57]	SmartCard	DES	Signatura/HF	SmartCard	-
[58]	Usuari+password	SSL	-	Perfils	Dissociació

Tabla 12. Requeriments de seguretat i privadesa dels treballs analitzats.

A partir de l'estudi dels treballs es poden treure algunes conclusions significatives:

La majoria de treballs consideren l'autenticació i fan un tractament correcte. La tècnica més generalitzada és l'ús de les targetes intel·ligents (SmartCards) [47], [50], [55], [56], [57]. En la resta de treballs, el mecanisme per garantir l'autenticació varia. [44] utilitza certificats, els autors a [46] validen les claus en una base de dades, la biometria és la tècnica adoptada per [48], els autors a [49] fan servir l'autenticació d'usuaris en un servidor WPA/RADIUS, els autors a [52] fan ús de la signatura HIDS/IBS i [58] adopta la coneguda tècnica de la introducció d'usuari i password.

Igualment, la majoria de treballs consideren el tema de la confidencialitat i aporten diverses solucions. En general s'utilitza el xifrat per a garantir la confidencialitat, ja sigui durant el seu transport per una xarxa de comunicacions (SSL/TLS) com en el moment de guardar la informació en una base de dades (amb diverses tècniques de xifrat). Els treballs [44], [55] i [58] fan servir el protocol SSL. Els autors a [49], [50], [56] i [57] empren diverses tècniques de xifrat. La proposta a [49] fa ús dels estàndards WPA, 802.11i, i IPSec (ESP). [50] adopta la tècnica del sobre digital, mentre que [56] empra AES i [57] fa servir DES. Les propostes [45] i [48] fan ús de la criptografia de clau pública. [47] adopta la targeta intel·ligent mentre que els autors a [52] fan servir una variant de la criptografia de clau pública amb cerca de paraules clau que es diu PEKS.

El tema de la integritat de la informació també és considerat per la majoria de treballs. La solució més generalitzada és la signatura digital (solució implementada pels treballs [44], [45], [48], [50], [55], [56] i [57]) si bé també es proposen altres tècniques. [47] usa la targeta intel·ligent. [49] empra IPSec (AH). Els autors a [52] fan servir una variant de la signatura digital que s'anomena HIDS/IBS.

Hi ha alguns treballs que se centren en estudiar el control d'accés. Les solucions més generalitzades són les targetes intel·ligents (SmartCards) adoptades pels treballs [47], [56] i [57], i el control d'accés basat en rols (RBAC) utilitzat pels autors a [53] i [55]. La proposta [46] valida les claus en una base de dades. El treball [51] fa servir bases de dades jeràrquiques mentre que [48] usa certificats. Els autors a [52] adopten una variant de la criptografia de clau pública amb cerca de paraules clau anomenada PEKS. La proposta [58] fa servir perfils.

Hi ha menys treballs que considerin l'aspecte de la privadesa. Els treballs analitzen diferents tècniques per a garantir la privadesa. La tècnica més generalitzada és la dissociació de les dades personals i les dades de l'anamnesi, la qual és seguida pels treballs [50] i [58]. Els autors a [54] proposen la desidentificació de la informació. El treball [50] també realitza altres tècniques com pseudònims, filtres i expressions regulars.

Capítol 5. Projectes.

En aquest capítol s'enumeren els projectes més importants i es descriuen les seves característiques principals. S'inclouen implementacions d'organismes públics, sistemes HCE basats en programari de codi obert i sistemes HCE comercials.

5.1. Organismes públics.

En aquest apartat s'inclouen un projecte endegat per la Unió Europea i una sèrie de projectes nacionals del Regne Unit, França, Estònia, EUA i Austràlia, escollits per la seva importància.

5.1.1. Unió Europea. epSOS (Smart Open Services for European Patients).

epSOS [69] és un projecte per a la interoperabilitat de sistemes electrònics d'eSalut cofinançat per la Comissió Europea i els estats membre amb l'objectiu de millorar el tractament mèdic dels ciutadans a l'estranger, proporcionant als professionals de la salut les dades necessàries del pacient. El consorci epSOS segueix creixent: l'1 de gener de 2011, es van unir 11 nous països als 12 inicials. El projecte ara consisteix de 20 països de la UE i 3 països no comunitaris.

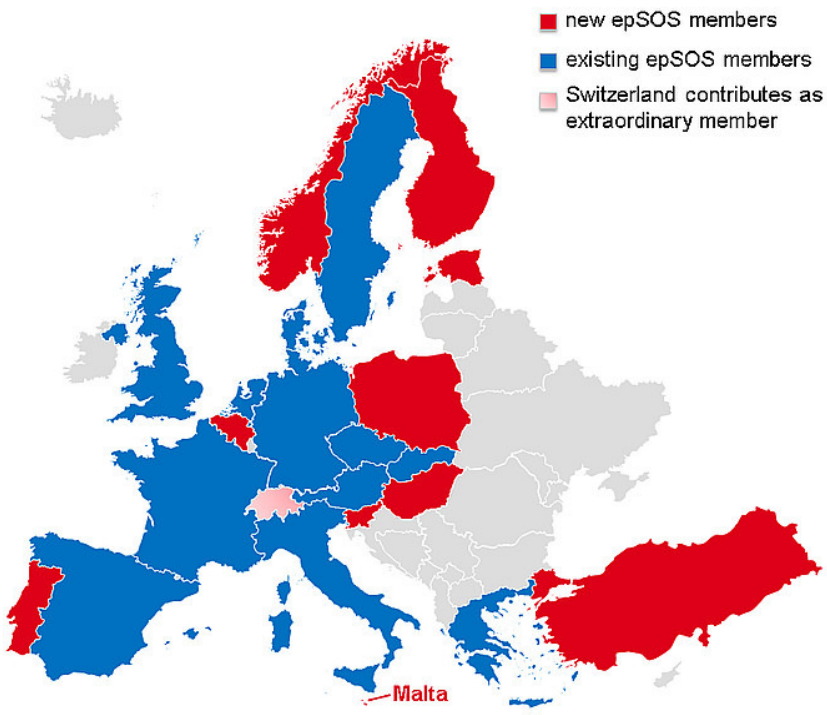

Figura 4. Projecte epSOS.

5.1.2. Regne Unit. The National Electronic Health Record Program.

El Servei Nacional de Salut (NHS), el sistema de salut finançat amb fons públics del Regne Unit, té una de les visions més ambicioses per a un HCE - el "Programa Nacional de Tecnologies de la Informació (NPfIT)" [70], establert l'octubre de 2002 amb la finalitat d'aconseguir un registre electrònic per a tots els pacients a nivell nacional per a l'any 2010. El projecte NHS Connecting for Health va ser creat pel Departament de Salut i va començar a funcionar a l'abril de 2005 per lliurar el "Programa Nacional" amb la finalitat d'implementar una infraestructura de TI integrada per a totes les organitzacions del Servei Nacional de Salut (NHS). Aquest projecte, que és el més gran del seu tipus al món, connectarà més de 100.000 metges, 380.000 infermeres i 50.000 professionals de la salut. Els professionals sanitaris hi podran accedir de manera segura des de qualsevol lloc del Servei Nacional de Salut i també els pacients. L'objectiu del Servei Nacional de Salut era tenir 60 milions de pacients amb una història clínica electrònica centralitzada per a l'any 2010.

5.1.3. França. Le Dossier Médical Personnel.

La peça central del programa TIC d'assistència sanitària francesa és el programa nacional basat en la web anomenat Dossier Médical Personnel (DMP) [71] o historial mèdic personal, que es posarà en marxa a través de sis consorcis regionals.

A més de l'atenció que prestarà als pacients i dels beneficis de seguretat, el govern francès ha estimat que el DMP reduirà el frau i estalviarà a l'estat de 2 a 3 mil milions d'euros cada any. El DMP es troba encara en fase de prototip i proves.

Tres agències principals són responsables del DMP. El DMP és administrat per una agència del govern central, el Groupement d'intérêt personal dossier médical personnel o GIP-DMP, responsable de la planificació del programa, la selecció i gestió de proveïdors. A més, el DMP també és supervisat per la Commission nationale de l'informatique et des libertés (CNIL), un organisme governamental responsable de les llibertats públiques i de la protecció de dades. Finalment, a més de la GIP-DMP i CNIL, una tercera agència, el Groupement d'intérêt pour la modernisation du système d'information hospitalier (GIP MISH) coordina a nivell nacional la modernització i adaptació de la informació dels hospitals i els sistemes d'informació del pacient per tal de garantir que compleixin amb els estàndards nacionals DMP.

El projecte ha estat objecte de controvèrsia a França, amb un recurs al Consell d'Estat per declarar la seva inconstitucionalitat. El Consell va rebutjar la demanda, però el govern ha instituït una major protecció posteriorment. Els metges no poden accedir a tot l'historial mèdic del pacient. Cada professional de la salut només està autoritzat a veure les àrees estrictament pertinents als seus interessos professionals. Aquesta autorització està continguda en la carta CPS del metge, que ha de coincidir amb els nivells d'autorització i els codis continguts en els servidors de seguretat centrals.

5.1.4. Estònia. The Estonian Electronic Health Record System.

Estònia és el primer país del món que ha implantat un sistema HCE a nivell nacional [72]. El sistema registra la història mèdica dels residents durant tota la seva vida.

5.1.5. EUA. Veterans Health Information Systems and Technology Architecture (VistA).

El Departament d'Afers de Veterans (Department of Veterans Affairs) té el major sistema d'informació sanitària dels EUA, conegut com a VistA [73]. Gairebé la meitat dels hospitals dels EUA utilitzen VistA.

VistA és un sistema d'informació sanitària construït al voltant del concepte HCE que conté prop de 100 mòduls de programari integrats. VistA és compatible tant per l'atenció ambulatòria com hospitalària, i inclou millores importants. La més significativa és una interfície gràfica d'usuari per als metges. A més, VistA inclou l'entrada automatitzada de comandes, l'administració de codis de barres per a medicaments, la prescripció electrònica i les guies clíniques.

Una condició per a la implementació d'un HCE als EUA és el desenvolupament de la Xarxa d'Informació Nacional de Salut (Nationwide Health Information Network), finançada pel Departament de Salut i Serveis Humans (Department of Health and Human Services).

El Departament d'Afers de Veterans treballa per desenvolupar un programari que permeti compartir informació amb els proveïdors privats de salut. Aquest programari s'anomena CONNECT i utilitza la xarxa Nationwide Health Information Network. CONNECT és una solució de programari de codi obert que permet l'intercanvi electrònic d'informació de salut.

D'altra banda, el Departament d'Afers de Veterans també utilitza un repositori de dades anomenat Clinical Data Repository/Health Data Repository (CHDR) que permet l'intercanvi de registres de pacients.

5.1.6. Austràlia. HealthConnect.

Austràlia està dedicada a l'elaboració d'un HCE vitalici per a tots els seus ciutadans. HealthConnect [74] és la principal iniciativa i abasta als diferents nivells de l'administració.

5.2. Programari de font oberta.

En les referències [75] i [76] podem trobar una recull de sistemes HCE de codi obert. Tot seguit es descriuen alguns dels sistemes HCE més importants.

5.2.1. OpenEHR.

OpenEHR [43] és un sistema de gestió HCE de codi obert.

Inclou especificacions i eines lliures i obertes per desenvolupar un repositori HCE interoperable per a una arquitectura orientada a serveis basada en arquetipus o en models clínics detallats.

El seu objectiu és ajudar per tal que les TICs suportin eficaçment l'assistència sanitària i la recerca mèdica.

5.2.2. OpenMRS.

OpenMRS [77] és un projecte col·laboratiu de codi obert per a desenvolupar programari per donar suport a la prestació d'assistència sanitària als països en desenvolupament.

Va sorgir de la necessitat imperiosa d'ampliar el tractament del VIH a l'Àfrica, però des del principi es va concebre com un sistema de registres mèdics electrònics de propòsit general.

OpenMRS es basa en els principis d'obertura i l'intercanvi d'idees, programes i estratègies per a la seva implementació i ús. El sistema està dissenyat per a ser utilitzable en entorns de recursos molt pobres i pot ser modificat afegint noves dades, formularis i informes sense necessitat de programació. Està concebuda com una plataforma que poden adoptar i modificar moltes organitzacions evitant la necessitat de desenvolupar un sistema de nou.

5.2.3. Tolven.

Tolven [78] és una plataforma de codi obert flexible per a recerca de l'àmbit clínic i de les ciències de la salut.

La plataforma Tolven és una plataforma de codi obert que permet emmagatzemar, indexar i mapar tota la informació clínica per al seu ús per aplicacions pròpies o externes. L'arquitectura Tolven permet emmagatzemar la informació clínica de forma segura i normalitzada en un repositori central.

5.2.4. MOSS.

MOSS [79] és la primera plataforma OpenExchange d'intercanvi d'informació sanitària de codi obert basada en normes IHE.

5.2.5. OpenExchange.

La plataforma OpenExchange [80] proporciona infraestructura bàsica basada en normes per a intercanviar informació de salut del pacient d'una manera segura, a fi de millorar la qualitat, la seguretat i l'eficàcia de l'assistència sanitària. La plataforma és un element crític de la infraestructura IHE que proporciona als metges i altres membres de la comunitat mèdica la informació correcta en el moment adequat. Es facilita i agilitza l'intercanvi d'informació del pacient. OpenExchange i tots els seus subprojectes es publiquen sota la llicència Apache v2.

5.2.6. IHE.

IHE (Integrating the HealthCare Enterprise) [81] és una iniciativa de professionals i de la indústria per millorar la forma en què els sistemes informàtics mèdics comparteixen la informació. IHE promou l'ús coordinat de normes, com DICOM i HL7, per fer front a les necessitats clíniques de suport a l'atenció al pacient. Els sistemes desenvolupats d'acord amb l'IHE es comuniquen entre si, són més fàcils d'implementar i permeten als proveïdors de salut d'utilitzar la informació amb més eficàcia.

5.2.7. Medfloss.

Medfloss [82] proporciona una visió global i estructurada de projectes Free / Lliure i Open Source Software (FLOSS) en els àmbits de la informàtica mèdica i l'atenció de la salut. Es tracta d'un portal d'informació obert que té com a objectiu fomentar l'intercanvi d'idees, coneixements i experiències sobre els projectes existents. Alguns dels projectes més coneguts són GNUmed, PatientOS, Open ISES Project, Clinic i Mirth.

5.3. Sistemes comercials.

En aquesta secció presentem les dues plataformes comercials més importants que permeten gestionar històries mèdiques online: Google Heath i Microsoft HealthVault.

Aquestes plataformes són dos exemples ben coneguts de registres personals de salut (RPS). La principal diferència entre un RPS i una HCE és que en el primer el pacient és responsable de gestionar el contingut dels registres de salut. Això no és compatible amb les normes legals que regulen la forma en què els metges han de mantenir els registres mèdics en molts països. En efecte, si els pacients fossin capaços de manipular la informació escrita pels metges, això podria donar lloc a importants problemes o errors mèdics. Per això, sembla poc probable que els registres personals de salut reemplacin fàcilment els registres utilitzats pels metges.

5.3.1. Google Health.

Google Health [83] és un servei d'informació personal centralitzat enfocat a la sanitat (també conegut com historial clínic electrònic de Google). El servei permet als usuaris de Google registrar voluntàriament el seu historial clínic, ja sigui manualment o en un compte dels serveis sanitaris associats al sistema de Google Health, de manera que es permet la fusió dels historials mèdics, que puguin estar dispersos, en un únic perfil de Google Health centralitzat.

La informació voluntàriament afegida pot incloure condicions de salut, medicaments, al·lèrgies i proves de laboratori. Un cop introduïda, Google Health fa servir la informació per proporcionar a l'usuari un registre clínic centralitzat, informació sobre medicaments, contraindicacions, al·lèrgies, etc.

Els centres sanitaris que intervenen en els projectes dels apartats 5.1 i 5.2 són entitats que estan sota l'àmbit d'aplicació de la Health Insurance Portability and Accountability Act (HIPAA), una llei federal que estableix les normes de confidencialitat de les dades d'informació de salut del pacient.

En canvi, a diferència d'un hospital, Google Health no està regulat per l'HIPAA. El motiu és que Google no emmagatzema les dades en nom dels centres sanitaris. La relació primària de Google Health és amb l'usuari.

Tot i que Google Health no està cobert per HIPAA, hi ha un compromís amb la privacitat dels usuaris i un conjunt de polítiques i mesures de seguretat, i s'assegura que els usuaris controlen l'accés a la seva informació.

Els usuaris trien qui consulta o afegeix informació al seu perfil, i poden revocar l'accés en qualsevol moment.

No hi ha publicitat en Google Health. No es ven informació de salut dels usuaris, ni es comparteix amb altres persones o serveis a menys que l'usuari ho autoritzi expressament, o en les circumstàncies que es descriuen en la política de privacitat de Google Health.

Els registres mèdics personals de l'usuari s'emmagatzemen en el seu compte i altres persones no poden accedir-hi amb el cercador.

A més, no s'utilitza la informació personal o mèdica emmagatzemada al perfil Google Health de cap usuari per personalitzar els resultats del cercador.

Google Health és un servei opcional, només es pot accedir a la informació mèdica introduïda voluntàriament pels usuaris. No s'inclou cap part de la història clínica d'un pacient sense el seu consentiment exprés. No obstant això, els usuaris poden gestionar els perfils d'altres persones. En un article després del llançament de Google Health, el New York Times va analitzar les qüestions de privacitat i va arribar a la conclusió que els pacients eviten els registres de Google Health perquè temen que el seu historial clínic pugui no estar segur en poder d'una gran empresa tecnològica. Google Health defensa que és més segur que l'historial mèdic en paper ja que no hi ha interacció humana.

L'API de Google Health es basa en un subconjunt del CCR (Continuity of Care Record).

5.3.2. Microsoft HealthVault.

Microsoft HealthVault [84] és una plataforma de Microsoft per emmagatzemar i mantenir informació de salut. El lloc web és accessible en www.healthvault.com. El servei va començar l'octubre de 2007 i està adreçat a les persones i als professionals de la salut.

Un registre HealthVault emmagatzema la informació de la salut d'una persona. L'accés a un registre és a través d'un compte de HealthVault, que pot ser autoritzat a accedir als registres de diverses persones, de manera que una mare pot administrar els registres de cada un dels seus fills o un fill pot tenir accés al registre del seu pare per ajudar el pare amb les qüestions mèdiques. L'accés al compte és a través de Windows Live ID.

Una persona interactua amb el seu registre HealthVault a través del lloc HealthVault o, més típicament, a través d'una aplicació que es comunica amb la plataforma HealthVault. Quan una persona utilitza per primera vegada una aplicació HealthVault, se'l demana que autoritzi l'aplicació per accedir a un conjunt específic de tipus de dades, i aquests tipus de dades són els únics que l'aplicació pot utilitzar. Una persona pot també compartir una part (alguns tipus de dades) o la totalitat del seu historial mèdic amb una altra persona interessada, com un metge, cònjuge, pare, etcètera.

El centre de connexió de HealthVault permet tranferir les dades de salut des de dispositius (com monitors de freqüència cardíaca, monitors de pressió arterial, etc.) al registre d'una persona. També es pot utilitzar per trobar i descarregar controladors de dispositius mèdics.

HealthVault és compatible amb diversos formats d'intercanvi, incloses les normes de la indústria com ara CCD i CCR. Aquest suport permet la integració amb molts registres personals de salut (RPS).

Capítol 6. Conclusions i treball futur.

6.1. Conclusions finals.

En aquest treball hem realitzat un estudi de la legislació de diferents països relatius a la protecció de dades de caràcter personal.

A partir d'aquest estudi, hem extret els requeriments bàsics de seguretat i privadesa exigits per la legislació.

Hem analitzat alguns projectes publicats en la literatura científica per tal de determinar el grau de compliment dels requeriments de seguretat i privadesa.

La majoria de treballs consideren l'autenticació i fan un tractament correcte. La tècnica més generalitzada és l'ús de les targetes intel·ligents (SmartCards). Altres treballs utilitzen altres tècniques com la biometria, combinació d'usuari i password, certificats, validació de claus en una base de dades, autenticació d'usuaris en un servidor WPA/RADIUS i signatura HIDS/IBS. La combinació d'usuari i password és fàcil d'implantar però el nivell de seguretat aportat és baix. En canvi, la identificació biomètrica és més difícil d'implantar però el nivell de seguretat garantit és molt alt. La resta de tècniques són relativament fàcils d'implantar a la vegada que garanteixen un nivell de seguretat alt.

Igualment, la majoria de treballs consideren el tema de la confidencialitat i aporten diverses solucions. En general s'utilitza el xifrat per a garantir la confidencialitat, ja sigui durant el seu transport per una xarxa de comunicacions (SSL/TLS) com en el moment de guardar la informació en una base de dades (amb diverses tècniques de xifrat). SSL garanteix la confidencialitat de la comunicació exclusivament. Cal tenir present que generalment les dades es guarden en clar en la base de dades. Si volem garantir la confidencialitat a nivell de la base de dades, cal xifrar la informació.

El tema de la integritat de la informació també és considerat per la majoria de treballs. La solució més generalitzada és la signatura digital. També es proposen altres tècniques com els tokens o el protocol IPSec (AH).

Hi ha alguns treballs que se centren en estudiar el control d'accés. Les solucions més generalitzades són les targetes intel·ligents (SmartCards) i el control d'accés basat en rols (RBAC). Altres treballs utilitzen diverses tècniques com claus validades en una base de dades, bases de dades jeràrquiques, certificats, perfils i PEKS (variant de criptografia de clau pública amb cerca de paraules clau).

Hi ha menys treballs que considerin l'aspecte de la privadesa. La tècnica més generalitzada és la dissociació de les dades personals i les dades de l'anamnesi. També es poden utilitzar altres tècniques: desidentificació, pseudònims, filtres i expressions regulars.

6.2. Opinió personal.

Com ha quedat palès en aquest treball, la seguretat té moltes dimensions i la majoria dels treballs només consideren alguns aspectes de la seguretat i la privacitat.

Crec que encara resta molt camí per recórrer en el sector de la salut per arribar a un nivell òptim que faci compatible la seguretat i privacitat de la informació de les dades de caràcter personal amb la seva flexibilitat i facilitat d'ús.

La normalització de la informació és un aspecte essencial per tal d'assolir la interoperabilitat dels sistemes a la vegada que es garanteix la seva seguretat i privacitat.

6.3. Treball futur.

En aquest treball només hem estudiat una sèrie de projectes de la literatura científica per tal d'analitzar el grau de compliment de la legislació en matèria de protecció de dades de caràcter personal.

Aquest treball es pot ampliar de manera natural a les implementacions existents en l'actualitat dels historials mèdics en format electrònic.

Entre les implementacions més importants podem esmentar els projectes nacionals de salut endegats per organismes governamentals o supragovernamentals.

Per exemple, l'anàlisi del projecte epSOS pot aportar informació molt reveladora de fins a quin punt els esforços normalitzadors poden millorar la seguretat i la privadesa de la informació a nivell de la Unió Europea.

Igualment, l'estudi dels diversos projectes nacionals del Regne Unit, França, EUA, etc., pot aportar informació sobre el nivell de protecció actual i les millores possibles.

D'altra banda, hi ha algunes propostes de codi obert com ara OpenEHR amb un gran potencial.

Del seu estudi es poden extreure conclusions importants i noves línies de treball.

Finalment, l'anàlisi dels productes comercials pot aportar una informació complementària molt interessant.

De tots aquests projectes es poden treure lliçons que han de servir per millorar la protecció de les dades de caràcter personal.

Glossari.

Accounting (Comptabilitat): Un individu té dret a rebre una relació de les revelacions d'informació protegida de salut realitzades per una entitat coberta en els sis anys anteriors a la data en què es demana la relació.

AHIC (American Health Information Community): Un organisme assessor federal creat amb l'objectiu que la majoria dels nord-americans tinguin registres electrònics de salut el 2014 (www.hhs.gov/healthit/ahic.html).

AHIMA (American Health Information Management Association): Una organització de professionals que treballen en la gestió d'informació sanitària, la prestació de suport als seus membres i l'enfortiment de la indústria i la professió (www.ahima.org).

Amending PHI (Modificació de la informació de salut protegida): Els individus tenen el dret de modificar la informació de salut protegida (PHI) en el conjunt de registres designat (designated record set).

AMIA (American Medical Informatics Association): El primer grup de professionals que va emetre directrius per a correu electrònic entre pacients i metges.

Ambulatory Medical Record, AMR (Història Clínica Ambulatòria): Un sistema informàtic per emmagatzemar, administrar i recuperar informació electrònica sobre la salut del pacient en el marc de l'atenció ambulatòria. En el marc dels pacients hospitalitzats, es refereix sovint com un registre mèdic electrònic (EMR).

Anonymized Data (Dades Anonimitzades): Dades anteriorment identificables que han estat desidentificades i per a les quals ja no hi ha un codi o un altre vincle. Un investigador no seria capaç de vincular informació anonimitzada amb una persona concreta.

Anonymous Data (Dades Anònimes): Dades que es van recollir sense identificadors i que mai van ser vinculades a un individu. Les dades codificades no són anònimes.

ANSI (American National Standards Institute): Organització d'estàndards americana que estableix els procediments per al desenvolupament i coordinació dels estàndards.

ASTM (American Society for Testing and Materials): Organisme de normalització dels EUA. Col·labora amb ISO i manté un sòlid lideratge en la definició dels materials i mètodes de prova.

Authorization (Autorització): Document que estableix un permís. La Regla de Privacitat HIPAA requereix l'autorització o dispensa de l'autorització per l'ús o la divulgació d'informació de salut identificable per a la recerca (entre altres). L'autorització ha d'indicar si la informació utilitzada o divulgada ja existeix o si es crearà durant la investigació. El formulari d'autorització pot ser combinat amb el formulari de consentiment informat, de manera que un subjecte ha de signar només un formulari.

Beaming: Transmissió de dades o programari entre dispositius, com ara assistents digitals personals (PDA), ordinadors personals i impressores, utilitzant transmissió infraroja o ones de ràdio.

Biometric authentication (autenticació biomètrica): Tecnologia que identifica una persona a través del reconeixement de característiques físiques úniques, com ara patrons de la retina o l'iris, forma de la cara, els patrons de veu, o les empremtes dactilars.

Bluetooth: un protocol dissenyat per a la comunicació sense fils de curt abast o la comunicació en xarxa entre una varietat de dispositius. És similar a Wi-Fi, però generalment s'utilitza per proporcionar una xarxa d'àrea personal (PAN), en lloc d'una xarxa d'àrea local sense fils (WLAN).

Business associate (Associat de negoci): Una persona o entitat externa que, en nom d'una entitat coberta, crea, usa o divulga la informació mèdica personal. [45 CFR § 160.103].

CCHIT (Certification Commission for Healthcare Information Technology): Una organització del sector privat inaugurada en 2004 per certificar productes de tecnologia d'informació de salut (HIT) com ara els historials mèdics electrònics i les xarxes sobre les quals interactuen.

CCR (Continuity of Care Record): Una especificació estàndard desenvolupada conjuntament per la ASTM International (originalment la American Society for Testing and Materials), la Massachusetts Medical Society (MMS), la Health Information Management and Systems Society (HIMSS), la American Academy of Family Physicians (AAFP), i la American Academy of Pediatrics. El seu objectiu és fomentar i millorar la continuïtat de l'atenció al pacient, reduir els errors mèdics, i assegurar almenys un mínim estàndard de transportabilitat de la informació de salut quan un pacient és enviat a un altre proveïdor. Està sent desenvolupat per a proporcionar la informació més rellevant i actualitzada sobre la condició del pacient incloent breus declaracions sobre diagnòstics, procediments recents, al·lèrgies, medicaments, la darrera atenció rebuda, així com recomanacions per a una futura cura.

CDA (Clinical Document Architecture): Proporciona un model d'intercanvi de documents clínics i apropa la indústria a la realització del registre mèdic electrònic.

CHI Iniciative, Consolidated Health Informatics Iniciative (Iniciativa d'Informàtica de Salut Consolidada): Una de les 24 iniciatives presidencials d'administració electrònica amb l'objectiu d'adoptar normes de vocabulari i de missatgeria per a facilitar la comunicació de la informació clínica a través de les empreses del sector sanitari. CHI pertany ara a la Federal Health Architecture.

CHR, Community Health Record (Registre de Salut Comunitari): Un registre mèdic electrònic que es comparteix entre una comunitat de proveïdors d'atenció mèdica i pagadors.

CIS, Clinical Information System (Sistema d'Informació Clínic): Un HCE que és un repositori de dades clíniques del pacient. El terme CIS s'utilitza de vegades indistintament amb EMR (electronic medical record).

Clinical decision support systems, CDSS (Sistemes de suport a les decisions clíniques): Ajuden al metge en l'aplicació d'informació nova per a la cura del pacient i ajuden a prevenir els errors mèdics i millorar la seguretat del pacient. Molts d'aquests sistemes inclouen programes informàtics que analitzen la informació entrada pel metge.

Coded (Codificat): Les dades són separades de la identificació personal a través d'un codi. Sempre que hi hagi un vincle, les dades es consideren indirectament identificables (i no anònimes o anonimitzades). Les dades codificades no estan cobertes pel Reglament de Privacitat HIPAA, però estan protegides pel Reglament Comú.

Common Rule (Reglament Comú): També conegut com 45 CFR 46. Descriu els requisits de la protecció de les persones i fa responsable d'aquesta protecció a les institucions, a les Juntes de Revisió Institucional (IRB) i als investigadors. Entre altres requisits, el reglament comú estableix que tots els investigadors obtinguin el consentiment informat de les persones que participen en la investigació, llevat que l'IRB hagi aprovat una exempció del requisit de consentiment informat.

Compliance Date (Data de compliment): Les entitats cobertes han de complir amb la Regla de Privacitat HIPAA ans del 14 d'abril de 2003.

Confidentiality (Confidencialitat): La protecció de la informació individualment identificable.

Consent, Informed (Consentiment informat): Requerit pel Reglament Comú. Es refereix a l'exigència que tots els investigadors expliquin els objectius, riscos, beneficis, proteccions de confidencialitat, i altres aspectes rellevants de la investigació a les persones perquè puguin prendre una decisió informada sobre la seva participació en la investigació. Els IRBs revisen el procés de consentiment informat per garantir el compliment de les regulacions. La Regla de Privacitat HIPAA permet a les entitats a incloure en el formulari de consentiment informat per a la investigació una "autorització" per l'ús o la divulgació de la informació de salut identificable individualment.

Covered Entity (Entitat Coberta): Es refereix a tres tipus d'entitats que han de complir amb la Regla de Privacitat HIPAA: proveïdors d'atenció mèdica, plans de salut i centres d'informació de salut. Als efectes de la Regla de Privacitat HIPAA, els proveïdors d'atenció mèdica inclouen hospitals i metges, així com els investigadors que presten serveis de salut i reben, accedeixen o generen informació d'identificació individual d'atenció mèdica [45 CFR § 160.103].

Covered functions (Funcions cobertes): Aquelles funcions de l'entitat coberta l'execució de les quals fan que l'entitat esdevingui un pla de salut, proveïdor d'atenció mèdica, o centre de salut [45 CFR § 164.103].

CPOE, Computerized Provider Order Entry (Entrada Automatitzada de Comandes al Proveïdor): Una aplicació que permet fer peticions de tractament i diagnòstic (com ara medicines, proves de laboratori i altres proves) per via electrònica en lloc de manualment. L'ordinador compara l'ordre amb les normes de dosificació, comprova les possibles al·lèrgies o interaccions amb altres medicaments, i avisa al metge sobre possibles problemes.

CPT, Current Procedural Terminology (Terminologia de Procediments Actual): Conjunt de codis elaborats per l'Associació Mèdica Americana utilitzats en la facturació dels serveis de salut.

Data Use Agreement (Acord sobre l'ús de les dades): Una garantia satisfactòria entre l'entitat coberta i un investigador que utilitza un grup limitat de dades que les dades només seran utilitzades per a usos específics.

Decedents (Difunts): Persones mortes que, d'acord amb la Regla de Privacitat HIPAA, tenen drets de privacitat. En la pràctica actual, tots els protocols d'investigació que impliquin la revisió d'històries clíniques dels difunts requereixen la revisió i aprovació per l'HRC / IRB (Human Rights Comitee / Institutional Review Board) i es pot dur a terme sense consentiment informat i autorització només si el protocol compleix els criteris per a una dispensa. Si la investigació inclou l'accés als registres de difunts, l'investigador haurà de documentar que s'utilitzarà la PHI dels morts només per a la investigació i que la informació és necessària per a la investigació. L'entitat coberta pot exigir a l'investigador a una prova de la mort.

Deidentified health information (Informació de salut desidentificada): La informació de salut que no identifica a una persona i respecte a la qual no existeix una base raonable per creure que la informació pugui ser utilitzada per identificar a una persona no és informació personal identificable. [45 CFR § 164.514 (a)]. La Regla de Privacitat HIPAA estableix que les dades estan desidentificades si bé (1) un expert amb experiència determina que el risc que es pugui utilitzar certa informació per identificar una persona és "molt petit" i documenta i justifica l'afirmació, o (2) les dades no inclouen cap dels divuit identificadors següents (de la persona o dels seus familiars, dels membres de la llar, o dels ocupadors), que es podrien utilitzar sols o en combinació amb una altra informació per identificar la persona: noms, subdivisions geogràfiques més petites que un estat (incloent codi postal), tots els elements de les dates, excepte l'any (llevat que el subjecte sigui major de 89 anys d'edat), números de telèfon, números de fax, adreça de correu electrònic, números de Seguretat Social, números de registre mèdic, números de beneficiaris de plans de salut, números de compte, números de certificat / llicència, identificadors de vehicle incloses les plaques de matrícula, identificadors

de dispositiu i números de sèrie, adreces URL, adreces IP, identificadors biomètrics, fotografies de cara completa i imatges comparables, i qualsevol número únic d'identificació, característica o codi. Fins i tot si aquests identificadors s'eliminen, el Reglament de Privacitat estableix que la informació es considerarà identificable si l'entitat coberta sap que la identitat de la persona encara es pot determinar.

Detailing (Informació sobre medicaments): La pràctica per la qual els representants farmacèutics proporcionen informació sobre medicaments als metges. Algunes empreses farmacèutiques estan recorrent a Internet per a realitzar "detailing", amb l'objectiu final de reduir els costos i augmentar l'eficàcia.

DICOM, Digital Imaging and Communications in Medicine (Imatges Digitals i Comunicacions en Medicina): Un estàndard per a la distribució i visualització de qualsevol tipus d'imatge mèdica, independentment de l'origen.

Digital Certificate (Certificat Digital): Certificat electrònic que estableix la identitat d'un usuari quan realitza negocis o transaccions segures en una xarxa com Internet.

Designated Record Set (Conjunt de registres designat): Registres mèdics i de facturació d'un proveïdor d'atenció mèdica de les persones i els registres utilitzats pel proveïdor per prendre decisions sobre les persones. En virtut de la regla de Privacitat HIPAA, les persones tenen dret a accedir i modificar la informació de salut protegida en un conjunt de registres designat.

Directly Identifiable (Directament identificable): Tota la informació que inclou identificadors personals. Per determinar quines dades es poden identificar es pot consultar els elements que han de ser eliminats d'acord amb la definició del Reglament de Privacitat HIPAA.

Disclosure (Divulgació): La publicació, transferència, provisió d'accés o divulgació de qualsevol altra manera d'informació fora de l'entitat que tingui la informació [45 CFR § 160.103].

Disease Management (Gestió de la malatia): Enfocament coordinat i proactiu a la gestió d'atenció i suport per als pacients amb malalties cròniques.

Distributed Computing (Computació distribuïda): Es tracta d'un sistema en el qual les tasques d'emmagatzematge i de càlcul es distribueixen entre diversos ordinadors en lloc de ser realitzades exclusivament per un ordinador central.

DMP, Dossier Médical Personnel (Dossier Mèdic Personal): Projecte nacional HCE a França.

DOQ-TI, Doctor's Office Quality-Information Technology (Tecnologia d'Informació de Qualitat en la Consulta Mèdica): Una iniciativa nacional que promou l'adopció dels sistemes HCE per millorar la qualitat i seguretat dels beneficiaris de Medicare en consultes mèdiques petites i mitjanes.

E-counseling: Teràpia psicològica realitzada per Internet, a través del correu electrònic, xats de text, videoconferència, o altres mètodes de comunicació en línia.

EDC, electronic data capture (captura electrònica de dades): L'ús de la tecnologia electrònica per recopilar i recollir dades, especialment en el context dels assaigs clínics. Permet agregar, ordenar, compartir i cercar les dades amb més facilitat que els registres en paper. Pot estar basada en la web, utilitzar ordinadors de mà, etc.

E-detailing (Informació electrònica sobre medicaments): L'ús d'Internet i les tecnologies relacionades per dur a terme "detailing" (presentacions realitzades pels visitadors mèdics als metges per tal de promoure els medicaments d'una empresa farmacèutica).

EDI, Electronic Data Interchange (Intercanvi Electrònic de Dades): Un intercanvi directe de dades entre dos ordinadors a través d'Internet o una altra xarxa, utilitzant formats de dades compartides i normes.

E-disease management (Gestió electrònica de la malaltia): L'ús de la tecnologia basada en la web per tal de proporcionar la comunicació metge-pacient i l'accés del pacient a la informació amb la finalitat de suportar la gestió de la malaltia del pacient.

E-encounter (Trobada virtual): Un tipus de comunicació electrònica metge-pacient que consisteix en un intercanvi bidireccional de la informació clínica al voltant d'una qüestió particular, clínica o un problema específic del pacient. Pot ser iniciat pel pacient o pel metge.

eHI, eHealth Initiative (Iniciativa eHealth): És una organització independent, sense ànim de lucre, que té com a objectiu impulsar la millora en la qualitat, seguretat i eficiència de l'atenció de salut a través de les TICs.

EHR, Electronic Health Record (Registre Electrònic de Salut): Un historial mèdic del pacient en temps real amb accés a eines de suport a la decisió basada en l'evidència que es pot utilitzar per ajudar els metges en la presa de decisions. És una història clínica relativa a la salut mental o física, passada, present o futura o a la condició d'un pacient i que resideix en ordinadors que capturen, transmeten, reben, emmagatzemen, recuperen, enllacen, i manipulen dades multimèdia amb l'objectiu principal de proporcionar atenció mèdica i serveis relacionats amb la salut. També pot donar suport a la recopilació de dades per a usos diferents de l'atenció clínica, com ara facturació, gestió de qualitat, vigilància de malalties i presentació d'informes. Pot incloure informació demogràfica, notes, problemes, medicaments, constants vitals, antecedents mèdics, vacunes, dades de laboratori i informes de radiologia. També s'anomena història clínica electrònica (HCE).

EHCR, Electronic Health Care Record (Registre Electrònic d'Atenció Sanitària): Hi ha cinc nivells d'EHCR.

1. AMR (Automated Medical Record) és un registre basat en paper amb alguns documents generats per ordinador.
2. CMR (Computerized Medical Record) permet l'accés a documents de nivell 1 de forma electrònica.
3. EMR (Electronic Medical Record) reestructura i optimitza els documents dels nivells anteriors garantint la interoperabilitat de tots els sistemes de documentació.
4. EPR (Electronic Patient Record) és un registre centrat en el pacient amb informació de múltiples institucions.
5. EHR (Electronic Health Record) afegeix al EPR informació general relacionada amb la salut que no està relacionada necessàriament amb una malaltia.

EMR, Electronic Medical Record (Registre Mèdic Electrònic): Un registre electrònic d'informació relacionada amb la salut d'un individu que pot ser creat, reunit, gestionat i consultat per metges i personal autoritzat dins d'una organització de salut.

Encryption (Xifrat): Traducció de les dades en un codi per tal de mantenir la informació segura de qualsevol persona diferent del seu destinatari.

E-prescribing, eRx (Recepta electrònica): Tecnologia en la qual els metges utilitzen ordinadors de mà o PCs per revisar els medicaments i enviar les receptes a una impressora, EMR, o farmàcia. Es pot integrar el seu programari amb sistemes d'informació existents per a permetre l'accés a la informació específica del pacient amb l'objectiu d'analitzar possibles interaccions farmacològiques i al·lèrgies.

E-procurement (Contractació electrònica): Contractació pública de béns i serveis a través d'Internet.

epSOS, Smart Open Services for European Patients (Serveis Oberts Intel·ligents per Pacients Europeus): Projecte per a la interoperabilitat de sistemes electrònics d'eSalut cofinançat per la Comissió Europea i els estats membre amb l'objectiu de millorar el tractament mèdic dels ciutadans a l'estranger, proporcionant als professionals de la salut les dades necessàries del pacient.

Extranet: Una Intranet que permet nivells especificats d'accés a usuaris externs autoritzats

Fat client (client pesant): En un sistema client / servidor, un client que realitza la major part del processament de les dades, en lloc de confiar en el servidor.

FCC, Federal Communications Commission (Comissió Federal de Comunicacions): Un organisme federal encarregat de regular les comunicacions per ràdio, televisió, cable, satèl·lit en els 50 estats d'EUA i a nivell internacional.

FHA, Federal Health Architecture (Arquitectura de Salut Federal): Un organisme de col·laboració compost per diversos departaments i agències federals que ofereix un marc de treball per vincular els processos de negoci del sector sanitari amb solucions i normes tecnològiques per tal de millorar els resultats del sector.

Firewall (tallafocs): Un dispositiu de seguretat situat entre una xarxa privada i xarxes externes com Internet. El tallafocs supervisa tota la informació que intenta entrar en la xarxa privada.

Formulary (Formulari): Una llista dels medicaments (genèrics i marques comercials) que estan coberts per un pla d'assegurança de salut específic, que serveix per fomentar l'ús de medicaments més rendibles. De vegades els hospitals utilitzen formularis d'ús propi, per la mateixa raó.

Google Health: Plataforma de Google que permet als usuaris registrar voluntàriament el seu historial clínic.

HAN, Health Action Network (Xarxa d'Acció Sanitària): Sistema de comunicació utilitzat pels Centres de prevenció i control de malalties (Centers for Disease Control and Prevention) per a intercanviar informació de malalties amb els departaments locals i estatals.

Health care (Atenció sanitària): Atenció, serveis o subministraments relacionats amb la salut d'una persona. [45 CFR § 160.103].

Healthcare clearinghouse (Centre d'atenció sanitària): Una entitat pública o privada que 1) processa o facilita el processament de la informació sanitària rebuda d'una altra entitat en un format no estàndard o contingut no estàndard en elements de dades estàndard o una transacció estàndard o 2) rep una transacció estàndard d'una altra entitat i processa o facilita el processament de la informació sanitària en format no estàndard o contingut no estàndard per a l'entitat receptora [45 CFR § 160.103].

HealthConnect: Projecte nacional HCE a Austràlia.

Healthcare operations (Operacions d'atenció sanitària): Qualsevol activitat de l'entitat coberta relacionada amb les funcions cobertes.

Healthcare provider (Proveïdor d'atenció de la salut): Un proveïdor de serveis mèdics o de salut, i qualsevol altra persona o entitat que subministra, factura, o és pagat per l'atenció sanitària [45 CFR § 160.103].

Health information (Informació de salut): Qualsevol informació, ja sigui oral o registrada en qualsevol forma o mitjà, que: 1) és creada o rebuda per un proveïdor d'atenció mèdica, pla de salut, autoritat de salut pública, empresari, asseguradora de vida, escola, universitat o centre de salut, i 2) es refereix a la salut passada, present o futura física o mental o condició d'un individu, la prestació d'assistència sanitària a una persona, o el pagament passat, present o futur per a la prestació d'assistència sanitària a una persona [45 CFR § 160.103].

***Health Oversight Agency (Agència de Supervisió de Salut)*:** Una persona o entitat en qualsevol nivell del govern federal, estatal o local que supervisa el sistema d'atenció de salut o requereix informació de salut per determinar l'elegibilitat o el compliment o per fer complir les lleis.

Health plan (Pla de salut): Un pla individual o en grup que proveeix o paga el cost de l'atenció mèdica.

HIE, health information exchange (intercanvi d'informació sanitària): Moviment electrònic d'informació relacionada amb la salut entre organitzacions d'acord amb estàndards reconeguts a nivell nacional.

IEN, health information exchange network (xarxa d'intercanvi d'informació sanitària): Connecta diversos HIE i organitzacions de salut regionals.

HIO, health information organization (organització d'informació sanitària): Una organització que supervisa i regula l'intercanvi d'informació sanitària entre organitzacions d'acord amb normes reconegudes a nivell nacional.

HIPAA, Health Insurance Portability and Accountability Act (Llei de Comptabilitat i Portabilitat de les Assegurances de Salut): Una llei federal destinada a millorar la portabilitat de les assegurances de salut i simplificar l'administració sanitària. HIPAA estableix estàndards per a la transmissió electrònica d'informació relacionada amb la salut i per garantir la seguretat i la privacitat de tota informació de salut identificable individualment.

HISPC, Healthcare Information Security and Privacy Collaboration (Col·laboració de la Privacitat i Seguretat de la Informació d'Atenció sanitària): Projecte per avaluar com afecten les polítiques, pràctiques i lleis estatals relacionades amb la confidencialitat i la seguretat a l'intercanvi d'informació sanitària a nivell nacional.

HITSP, Health Information Technology Standards Panel (Grup de Normes de Tecnologies de la Informació de Salut): Organització de 18 entitats independents, patrocinada per l'Institut Americà d'Estàndards Nacionals (ANSI), que serveix com una associació de cooperació entre el sector públic i el privat per tal d'aconseguir un conjunt de normes específicament destinades a aconseguir la interoperabilitat del programari per a aplicacions del sector sanitari, i a la seva interacció en xarxes locals, regionals i nacionals.

HL7 (Health Level Seven): Normes per a dades administratives i clíniques. Els sistemes que són compatibles amb HL7 milloren la interoperabilitat i l'intercanvi electrònic de dades.

ICD-9, International Classification of Disease – 9th Revision (Classificació Internacional de Malalties, novena revisió): Sistema Internacional de classificació de malalties desenvolupat per l'Organització Mundial de la Salut (OMS) que proporciona una descripció detallada de malalties i lesions conegudes.

Indirectly Identifiable (Identificable Indirectament): Dades que no inclouen identificadors personals, però que enllacen les dades amb la informació identificativa mitjançant l'ús d'un codi. Aquestes dades encara es consideren identificables pel Reglament Comú. Consultar el terme Deidentified per determinar quines dades es poden considerar identificables.

Individually identifiable health information (Informació de salut individualment identificable): Un subconjunt d'informació de salut que identifica la persona o que es pot utilitzar raonablement per identificar una persona [45 CFR § 164.501].

Institutional Review Board, IRB (Junta de Revisió Institucional): Mètode exigit pel Common Rule per protegir les persones. Les regulacions de privacitat de HIPAA requereixen l'IRB per protegir els drets de privadesa dels subjectes d'una investigació.

Limited data set (Conjunt de dades limitat): Conjunt de dades que poden ser utilitzades per a la investigació, la salut pública o operacions d'atenció sanitària sense una autorització o dispensa d'autorització. El conjunt limitat de dades es defineix com la PHI que exclou els següents identificadors directes de la persona o familiars, ocupadors o membres de la família: nom, informació de l'adreça postal (que no sigui poble o ciutat, estat i codi postal), telèfon i fax, adreces de correu electrònic, números de registre mèdic, números de Seguretat Social, números de beneficiaris de pla de salut, números de compte, números de certificat o de llicència, identificadors del vehicle i números de sèrie incloent plaques de matrícula, identificadors de dispositiu i números de sèrie, URLs, adreces IP, identificadors biomètrics incloent els emprentes digitals i de veu, fotografies de cara completa i les imatges comparables. Els identificadors directes que cal excloure es troben en 45 CFR § 164.514 (e) (2).

Linked (Vinculat): Veure Coded.

LIS, Laboratory information system (Sistema d'informació de laboratori): Una HCE és un repositori de dades de pacients introduïdes directament o mitjançant aplicacions externes. Una d'aquestes aplicacions és el sistema d'informació de laboratori (LIS) que normalment s'utilitza pels departaments de patologia dels hospitals per gravar la seva activitat.

Leapfrog Group: Un grup de companyies que neix amb l'objectiu d'aprofitar el poder de compra de l'empresari per iniciar millores en la seguretat i en l'atenció mèdica. Leapfrog fomenta l'aplicació de CPOE (computerized physician order entry), un procés d'entrada electrònica d'instruccions del metge per al tractament dels pacients (en particular els pacients hospitalitzats), com a part de la seva iniciativa més àmplia de seguretat del pacient.

LHII, Local Health Information Infrastructure (Infraestructura d'informació sanitària local): Un terme que s'utilitza com a sinònim de RHIO (Regional Health Information Organization). Originalment va ser utilitzat per l'Oficina del Coordinador Nacional de Tecnologia d'Informació de Salut (Office of the National Coordinator of Health Information Technology, ONCHIT). Amb el temps ha donat lloc a la NHII (infraestructura nacional d'informació de salut).

Microsoft HealthVault: Plataforma de Microsoft per emmagatzemar i mantenir informació de salut.

Mínimum necessary (Mínim necessari): Les entitats cobertes han de desenvolupar i aplicar criteris destinats a limitar la divulgació d'informació protegida de salut a la informació raonablement necessària per complir el propòsit per al qual es demana la divulgació i revisar les sol·licituds individualment. L'estàndard mínim necessari també s'aplica als usos de la informació protegida de salut [45 CFR § 164.514 (d) (2)] i sol·licituds d'informació de salut protegida [45 CFR § 164.514 (d) (4)].

MPI, Master Patient Index (Índex Mestre de Pacient): Un programa de base de dades que recull els números d'identificació d'un pacient (per exemple, del laboratori de sang, de radiologia, i admissions), i els manté sota un únic número d'identificació.

NEDSS, National Electronic Disease Surveillance System (Sistema Nacional Electrònic de Seguiment de Malalties): La xarxa electrònica del CDC (Center for Disease Control and Prevention) per a la presentació d'informes sobre malalties que vincula l'agència amb els departaments estatals de salut pública.

NHII, National Health Information Infrastructure (Infraestrucura Nacional d'Informació Sanitària): Una iniciativa del Departament de Salut i Serveis Humans per millorar l'eficàcia, l'eficiència i la qualitat general de l'atenció mèdica en els EUA. Requereix una xarxa basada en el coneixement de sistemes interoperables de salut i informació personal de salut que millorin la presa de decisions, fent disponible la informació de salut quan i on es necessita.

NHIN, National Health Information Network (Xarxa Nacional d'Informació Sanitària): Descriu les instal·lacions físiques i la xarxa nacional necessària per a la interoperabilitat. Les especificacions de la xarxa descriuen les tecnologies, normes, lleis, polítiques, programes i pràctiques que permeten compartir la informació de salut entre els responsables de prendre les decisions, incloent els consumidors i els pacients, per tal de promoure millores en l'atenció mèdica. El seu desenvolupament va començar fa més d'una dècada amb la publicació de l'informe de l'Institute of Medicine anomenat "The Computer-Based Patient Record". El NHIN es concep com una xarxa nacional de xarxes que comparteix informació sanitària i que connecta les RHIOs (regional health information organizations, organitzacions regionals d'informació sanitària).

NIST, National Institute of Standards and Technology (Institut Nacional d'Estàndards i Tecnologia): Fundada el 1901, el NIST és una agència federal dins del Departament de Comerç dels EUA, que promou la competitivitat i la innovació industrial dels EUA establint normes i tecnologia avançada (www.nist.gov).

Notice (Avís): Una persona té dret a estar degudament informada dels usos i divulgacions d'informació mèdica protegida feta per l'entitat coberta així com dels drets de la persona i de l'entitat coberta pel que fa a la informació protegida de salut.

NPfIT (National Program for Information Technology): Projecte nacional HCE al Regne Unit.

NPI, National Provider Identifier (Identificador de Proveïdor Nacional): L'HIPAA de 1996 requereix l'adopció d'un identificador únic per a proveïdors d'atenció mèdica. La norma final NPI es va publicar el 23 de gener de 2004. L'NPI és un identificador numèric de 10 dígits, en què els números no contenen informació sobre els proveïdors de salut, com ara l'estat en què operen, el tipus de proveïdor o la seva especialització. L'NPI substitueix els identificadors anteriors (UPIN, OSCAR, PIN, i NSC) en les transaccions HIPAA estàndard. L'NPI d'un proveïdor no canviarà, independentment dels canvis de feina o d'ubicació.

ONCHIT, Office of the National Coordinator for Health Information Technology (Oficina del Coordinador Nacional per a la Tecnologia de la Informació de Salut): L'oficina del Departament de Salut i Serveis Humans dels EUA per al desenvolupament i aplicació a nivell nacional d'una infraestructura d'informació de salut interoperable.

OpenEHR: Sistema de gestió HCE de codi obert.

PAS, Patient Administration System (Sistema d'administració del pacient): Una història clínica electrònica pot incloure un PAS o ser connectat a un PAS a través d'HL7. PAS és una aplicació responsable de l'enregistrament i la presentació d'informes de dades administratives de la visita d'un pacient a un hospital.

Patient Record Locator (Localitzador de Registre del Pacient): Mitjans electrònics de localització dels arxius dels pacients per ajudar a trobar resultats de proves, historials clínics, dades de receptes, i informació de salut. Un localitzador actua com una eina de cerca d'informació de salut.

PHIT, personal health information technology (tecnologia de la informació personal de salut): PHIT permet la documentació completa de la història mèdica d'una persona, en un lloc privat i segur, en un format normalitzat, i accessible als proveïdors les 24 hores del dia des de qualsevol lloc.

Personal Health Record (Registre Personal de Salut): Un registre electrònic d'informació relacionada amb la salut d'una persona que s'ajusta a normes d'interoperabilitat, es pot recuperar des de múltiples fonts i pot ser gestionat, compartit, i controlat per la persona.

Pharmacy Information Management System (Sistema de Gestió d'Informació Farmacèutica): Els registres mèdics electrònics són repositoris de dades de pacients introduïdes directament o mitjançant aplicacions externes. Una d'aquestes aplicacions és el sistema de gestió d'informació farmacèutica (PIMS) que s'utilitza normalment en les farmàcies dels hospitals per a registrar la seva activitat.

PKI, Public Key Infraestructure (Infraestructura de clau pública): Un sistema que utilitza certificats electrònics i autoritats de certificació per a autenticar els usuaris.

Privacy (Privacitat): A l'efecte de la Regla de Privacitat HIPAA, la privacitat significa l'interès d'un individu per limitar qui té accés a la informació personal de salut.

***Privacy Board (Junta de Privacitat)*:** Una junta de membres autoritzats pel Reglament de Privacitat HIPAA per aprovar una dispensa per a l'ús i/o divulgació d'informació de salut identificable. Per a la investigació, la Junta de Revisió Institucional (IRB) funciona com la Junta de Privacitat.

***Privacy Notice (Notificació de Privacitat)*:** Avís institucional que descriu les pràctiques de l'entitat coberta en matèria d'informació de salut protegida i on s'explica l'ús de la informació protegida de salut. Els proveïdors de salut i altres entitats han de donar l'avís als pacients i subjectes de la investigació i han d'obtenir un justificant de recepció signat.

***Protected Health Information, PHI (Informació de Salut Protegida)*:** Informació de salut Individualment identificable transmesa o mantinguda en qualsevol forma o mitjà.

Psychotherapy Notes (Notes de Psicoteràpia): Notes gravades per un un professional de salut mental durant una sessió de psicoteràpia, ja sigui en una sessió privada o en grup. Aquestes notes estan separades en la història clínica i no inclouen les receptes. Cal l'autorització expressa del pacient per a l'ús i la divulgació de les notes de psicoteràpia.

Public Health Authority (Autoritat de Salut Pública): Una persona o organització necessària per a realitzar una activitat de salut pública.

Public health authority (Autoritat pública sanitària): Un organisme o autoritat dels EUA responsable de qüestions de salut pública com a part del seu mandat oficial [45 CFR § 164.501]. Són exemples d'autoritat pública sanitària els departaments locals i estatals de salut, CDC (Centers for Disease Control) , National Institutes of Health (NIH), Food and Drug Administration (FDA), and Occupational Safety and Health Administration (OSHA).

Required by law (Requerit per la llei): Un mandat contingut en la llei que obliga a una entitat a utilitzar o divulgar informació protegida de salut [45 CFR § 164.103].

RHIO, Regional Health Information Organizations (Organitzacions Regionals d'Informació Sanitària): Una organització d'informació de salut que reuneix a les parts interessades dins d'una àrea geogràfica definida i controla el seu intercanvi d'informació per tal de millorar la salut i l'atenció en aquesta comunitat.

RLS, Record Locator Service (Servei de Localització de Registres): Proporciona als usuaris autoritzats d'una xarxa d'informació sanitària regional punters a la ubicació de la informació de salut del pacient a través de la xarxa, permetent als usuaris accedir i integrar la informació sanitària del pacient des de fonts distribuïdes sense utilitzar identificadors nacionals de pacient (NPIs) o bases de dades centralitzades.

Safe harbor method (Mètode port segur): Eliminació de divuit identificadors enumerats a la Regla de Privacitat per aconseguir la desidentificació [45 CFR § 164.514 (b)].

SDO, Standards Development Organization (Organització de Desenvolupament de Normes): Una organització que desenvolupa estàndards per proporcionar estabilitat i consistència a un producte o servei amb l'objectiu de reduir les despeses i millorar la qualitat.

Smart card (Targeta intel·ligent): un dispositiu electrònic de la mida d'una targeta de crèdit que conté memòria electrònica i un microxip incorporat. Les targetes s'utilitzen per emmagatzemar dades. En un context de salut, emmagatzemen la informació mèdica personal. Es pot accedir a les dades mitjançant un lector, un dispositiu en el qual s'insereix la targeta. Normalment pot emmagatzemar més informació que una targeta de banda magnètica.

Sniffer: Programa que monitoritza i analitza el flux d'informació en una xarxa per trobar colls d'ampolla i problemes. Els administradors de xarxa utilitzen programes rastrejadors per a monitoritzar el trànsit de la xarxa. Un sniffer es pot utilitzar legítimament o il·legítimament per a capturar la informació transmesa per la xarxa.

Standards (Normes):

- ASTM CCR (American Society for Testing and Materials Continuity of Care Record). Un estàndard sobre un resum de la salut del pacient basat en XML. Els CCRs es poden crear, llegir i interpretar per diversos sistemes HCE, el que permet una fàcil interoperabilitat entre entitats.

- ANSI X12 (també conegut com EDI, Electronic Data Interchange). Un format estàndard utilitzat per a la transmissió de dades de negocis, desenvolupada per la Data Interchange Standards Association. Les parts que intercanvien transmissions EDI s'anomenen trading partners (socis comercials). Les dades que es transmeten sovint inclouen el que generalment es recolliria en un document o formulari.

- CEN (Comitè Europeu de Normalització). Fundat el 1961 pels organismes de normalització nacionals de la Comunitat Econòmica Europea. Desenvolupa normes tècniques per a molts àmbits de negoci, inclosa l'atenció mèdica.

- Norma CEN EN13606. Desenvolupada pel Grup de treball CEN TC 251 sobre comunicacions HCE. El grup de treball se centra en l'elaboració de normes que inclouen requisits per a una estructura d'informació de salut que suporti els procediments clínics i administratius, mètodes tècnics per donar suport als sistemes interoperables, així com els requisits en matèria de seguretat i qualitat.

- DICOM (Digital Imaging and Communications in Medicine). Molt utilitzada per a la representació i la comunicació d'imatges radiològiques i per a presentació d'informes.

- HL7 (Health Level 7). Estàndard ANSI per a l'intercanvi de dades d'atenció sanitària entre aplicacions informàtiques. Els missatges HL7 s'utilitzen per a l'intercanvi entre els sistemes de registre de l'hospital i del metge i també entre els sistemes HCE i els sistemes de gestió. S'utilitzen documents HL7 CDA (Clinical Document Arquitecture) per a la comunicació de documents mèdics.

- ISO/TC 215 (ISO Technical Committee on health informatics). ISO/TC 215 treballa en la normalització de les TICs de salut (HITC) per aconseguir la compatibilitat i la interoperabilitat entre sistemes independents. ISO és una organització d'establiment de normes integrada per representants dels organismes de normalització nacionals. Fundada el 1947, l'organització realitza normes industrials i comercials a nivell mundial, inclosa la normalització en el camp de la informació de salut i les TICs de salut per aconseguir compatibilitat i interoperabilitat entre sistemes independents.

- OpenEHR. Especificacions i implementacions públiques de sistemes i comunicació HCE sobre la base d'una separació completa entre el programari i els models clínics.

- OpenEHR Foundation. Una fundació sense ànim de lucre que suporta la investigació oberta, el desenvolupament i l'aplicació de sistemes HCE oberts. Les seves especificacions es basen en una combinació de 15 anys de recerca en sistemes HCE i nous paradigmes dissenyats per ser la base d'una infraestructura HCE correcta des del punt de vista mèdic i jurídic, distribuïda i amb control de versions. OpenEHR també desenvolupa i publica especificacions i implementacions de codi obert HCE.

- HIMSS (Healthcare Information and Management Systems Society). Organització que pretén l'ús òptim de la tecnologia d'informació de salut i de la gestió de sistemes per a la millora de la salut humana. HIMSS lidera polítiques públiques de salut i pràctiques de la indústria a través de la promoció educativa i iniciatives professionals per garantir una atenció de qualitat al pacient.

- XML (Extensible Markup Language). Un llenguatge de marcat de propòsit general per a la creació de llenguatges de marcat de propòsit especial, capaç de descriure molts tipus diferents de dades. El seu objectiu principal és facilitar l'intercanvi de dades a través de diferents sistemes, en particular els sistemes connectats a través d'Internet.

Statistical deidentification (Desidentificació estadística): El procés pel qual un estadístic qualificat, utilitzant tècniques analítiques acceptades, conclou que es limita el risc d'utilitzar la informació, sola o en combinació amb una altra informació raonablement disponible, per identificar el subjecte de la informació [45 CFR § 164.514 (b)].

Subscription-based model (model basat en subscripció): Un model de negoci basat en el pagament d'una quota mensual per l'ús d'equips, programari, serveis o continguts, o una combinació d'aquests. Usat per molts venedors, com ara els proveïdors de sistemes de receptes electròniques.

Telehealth (Tele-salut, Telemedicina): L'ús de les TICs per oferir serveis de salut i transmetre informació de salut a distància.

Teleradiologia: Una forma de telemedicina que implica la transmissió electrònica d'imatges radiogràfiques de pacients.

Transaction (Transacció): La transmissió d'informació entre dues parts per dur a terme activitats financeres o administratives relacionades amb la cura de la salut. [§ 45 CFR 164.103].

Thin client (client lleuger): En un sistema client / servidor, un client amb poca capacitat de processament o d'emmagatzematge de dades que es basa principalment en un servidor central per realitzar aquestes funcions.

Tracking of Disclosures (Seguiment de les Revelacions): El Reglament de Privacitat HIPAA dóna als individus el dret de demanar una relació de la informació protegida de salut divulgada en els últims sis anys. Si una persona autoritza l'ús o revelació de la investigació, no és necessari fer un seguiment de la informació divulgada, però cal fer el seguiment si l'investigador rep una dispensa aprovada per l'IRB. Aquesta relació ha d'incloure: la data de la divulgació, el nom de l'entitat o persona (i direcció si es coneix) que va rebre la informació de salut protegida, una breu descripció de la informació divulgada, i una breu exposició dels efectes de la divulgació.

Treatment (Tractament): La prestació d'assistència sanitària per un o diversos proveïdors d'atenció mèdica. El tractament inclou qualsevol consulta, derivació o intercanvi d'informació per a gestionar l'atenció d'un pacient.

Use (Ús): L'intercanvi d'informació mèdica personal dins d'una entitat coberta.

VistA (Veterans Health Information Systems and Technology Architecture): Projecte nacional HCE als EUA.

VPN (Virtual Private Network (Xarxa Privada Virtual): Una xarxa que utilitza connexions públiques, com Internet, per connectar els usuaris, però que es basa en mesures de seguretat com el xifrat per assegurar que només els usuaris autoritzats poden accedir a la xarxa.

Waiver of Authorization (Dispensa de l'autorització): En determinades circumstàncies, l'investigador pot obtenir de l'IRB una dispensa del requisit d'autorització per a l'ús o la divulgació d'informació de salut privada.

WAP, Wireless Application Protocol (Protocol d'aplicació sense fils): Una norma per al lliurament de continguts en dispositius mòbils sense fils, com telèfons mòbils i ordinadors de mà.

WEP, Wired Equivalent Privacy (Privacitat Equivalent Cablejada): Un protocol de seguretat per a xarxes sense fils (WLAN) que utilitza l'estàndard 802.11b.

Wi-Fi: Un estàndard de xarxa sense fils ratificat per l'Institut d'Enginyers Elèctrics i Electrònics (IEEE) a finals de 1999 i amb el suport de la majoria de venedors de xarxes d'àrea local sense fils (WLAN). Wi-Fi és l'abreviatura de Wireless Fidelity. També conegut com IEEE 802.11b.

Wireless Internet (Internet sense fils): Computació mòbil sense fils que utilitza Internet com a infraestructura de comunicació de xarxa.

WLAN (Xarxa d'àrea local sense fils): Una LAN que utilitza tecnologia de radiofreqüència per transmetre dades a través de distàncies relativament curtes.

WML, Wireless Markup Language (Llenguatge de marcat sense fils): Llenguatge que té el seu origen en l'XML (eXtensible Markup Language). Aquest llenguatge s'utilitza per construir les pàgines que apareixen en les pantalles dels telèfons mòbils i els assistents personals digitals (PDA) dotats de tecnologia WAP. És una versió reduïda del llenguatge HTML que facilita la connexió a Internet d'aquests dispositius i que a més permet la visualització de pàgines web en dispositius sense fils que incloguin la tecnologia WAP.

Bibliografia

[1] eSalud

http://es.wikipedia.org/wiki/ESalud

[2] Impacto, ventajas e inconvenientes de la Historia Clínica Electrònica

http://www.tel.uva.es/personales/jgompil/ctmiii/HCE.pdf

[3] Electronic health record (EHR)

http://en.wikipedia.org/wiki/Electronic_health_record

[4] Historia clínica electrònica (HCE)

http://es.wikipedia.org/wiki/HCE

[5] Richard S. Dick, Elaine B. Steen, and Don E. Detmer. The Computer-Based Patient Record: Han Essential Technology for Health Care. National Academy of Sciences, Washington, D.C., revised edition, 1997.

http://www.nap.edu/catalog.php?record_id=5306#toc

[6] To Err is Human: Building a Safer Health System (2000), Institute of Medicine (IOM), National Academy Press

http://www.nap.edu/books/0309068371/html/

[7] Declaració Universal dels Drets Humans, de 10 de desembre 1948, adoptada per l'Assemblea General de Nacions Unides

http://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=cln

[8] Agència Espanyola de Protecció de Dades. Memòria 2009.

https://www.agpd.es/portalwebAGPD/canaldocumentacion/memorias/memoria_2009/common/AEPD_memoria_2009.pdf

[9] Conveni Europeu per a la protecció dels drets humans i les llibertats fonamentals, de 4 de novembre de 1950

http://constitucion.rediris.es/legis/1950/tr1950-11-04_roma.html

[10] Carta de Drets Fonamentals de la Unió Europea

http://www.apdcat.com/media/675.pdf

[11] Conveni 108/1981 del Consell d'Europa per a la protecció de les persones envers el tractament automatitzat de dades de caràcter personal

http://www.informatica-juridica.com/anexos/Convenio_108_Consejo_Europa_Proteccion_Personas_Tratamiento_Automatizado_Datos_Caracter_Personal_Estrasburgo_28_Enero_1981.asp

[12] Directiva 95/46/CE del Parlament Europeu i del Consell, de 24 d'octubre de 1995, relativa a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades

http://www.apdcat.com/media/676.pdf

[13] Directiva 2002/58/CE del Parlament Europeu i del Consell, de 12 de juliol de 2002, relativa al tractament de les dades personals i a la protecció de la intimitat en el sector de les comunicacions electròniques

http://www.apdcat.com/media/677.pdf

[14] Constitució Espanyola, de 27 de desembre de 1978

http://www.boe.es/aeboe/consultas/enlaces/documentos/ConstitucionCATALAN.pdf

[15] Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal

http://www.boe.es/boe_catalan/dias/1999/12/30/pdfs/A01399-01411.pdf

[16] Reial Decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament que desenvolupa la LOPD

http://www.boe.es/boe_catalan/dias/2008/01/19/pdfs/BOE-A-2008-979-C.pdf

[17] HIPAA (Health Insurance Portability and Accountability Act)

http://www.hhs.gov/ocr/privacy/

[18] "Opposition calls for rethink on data storage". e-Health Insider (UK). December 2007.

http://www.ehi.co.uk/news/ehi/3343

[19] "German doctors say no to centrally stored patient records". e-Health Insider (UK). January 2008.

http://www.ehi.co.uk/news/ehi/3384

[20] Health & Medicine (2006-06-26). "At risk of exposure: In the push for electronic medical records, concern is growing about how well privacy can be safeguarded.". Los Angeles Times.

http://articles.latimes.com/2006/jun/26/health/he-privacy26

[21] CNN.com (May 23, 2006): FBI seeks stolen personal data on 26 million vets. Retrieved July 30, 2006

http://www.cnn.com/2006/US/05/22/vets.data/index.html

[22] Tim Wafa (J.D.). "How the Lack of Prescriptive Technical Granularity in HIPAA Has Compromised Patient Privacy". Northern Illinois University Law Review, Volume 30, Number 3, Summer 2010.

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1547425

[23] JM Appel. Why shared medical database is wrong prescription. *Orlando Sentinel*, December 30, 2008.

http://articles.orlandosentinel.com/2008-12-30/news/OPappel30_1_medical-records-medical-system-electronic-medical

[24] Covered entities

https://www.cms.gov/HIPAAGenInfo/06_AreYouaCoveredEntity.asp

[25] Information privacy law

http://en.wikipedia.org/wiki/Information_privacy_law

[26] Llei 14/1986 General de Sanitat, de 25 d'abril (art. 10.3, 23)

http://noticias.juridicas.com/base_datos/Admin/l14-1986.t1.html#a10

[27] Llei 41/2002, del 14 de novembre, reguladora de l'autonomia del pacient i dels drets i obligacions en matèria d'informació i documentació clínica.

http://www.boe.es/boe_catalan/dias/2002/12/02/pdfs/A03057-03062.pdf

[28] Llei 21/2000, de 29 de desembre, sobre els drets d'informació concernent la salut i l'autonomia del pacient, i la documentació clínica.

https://www.gencat.cat/salut/depsalut/html/ca/professionals/spbioe08.htm

[29] Health Insurance Portability and Accountability Act

http://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act

[30] About HIPAA

http://www.phoenix.tc-ieee.org/0001_Bibliography/20060830adam_About%20HIPAA1.pdf

[31] DeIdentifying Data According to the HIPAA Safe Harbor Standard

http://www.press.jhu.edu/journals/narrative_inquiry_in_bioethics/HIPAA_Safeharbor.pdf

[32] Reglament de Seguretat HIPAA. Matriu de Normes de Seguretat

http://www.bricker.com/documents/resources/hipaa/appendix.pdf

[33] ANSI X12

http://en.wikipedia.org/wiki/ANSI_X12

[34] EN 13606

http://en.wikipedia.org/wiki/EN_13606

[35] CONTSYS (System of concepts to support continuity of care) EN 13940

http://en.wikipedia.org/wiki/CONTSYS

[36] HISA (Health Informatics Service Architecture) EN 12967

http://en.wikipedia.org/wiki/HISA

[37] Continuity of Care Record

http://en.wikipedia.org/wiki/Continuity_of_Care_Record

[38] DICOM

http://en.wikipedia.org/wiki/DICOM

[39] HL7

http://en.wikipedia.org/wiki/HL7

[40] ISO/TC 215

http://en.wikipedia.org/wiki/ISO_TC_215

[41] Title 21 CFR Part 11

http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfCFR/CFRSearch.cfm?CFRPart=11&showFR=1

[42] Guidance for Industry Computerized Systems Used in Clinical Investigations

http://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/UCM070266.pdf

[43] OpenEHR

http://www.openehr.org/home.html

[44] WRM Dassen, ED Gommer, CCW Bonnemayer, HJ Sprujit, WA Dijk and MH Baljon. A generic secure internet-based facility to support multiple registers using modern encryption technology and client certicates. Computers in Cardiology, 29:273-276, Setembre 2002.

[45] Ana Ferreira, Ricardo Correia, Luis Antunes, Ernesto Palhares, Pedro Marques, Pedro Costa and Altamiro da Costa Pereira. Integrity for electronic patient record reports. Proceedings. 17th IEEE Symposium of Computer-Based Medical Systems, pages 4-9, Juny 2004.

[46] Andrew Dalley, John Fulcher, David Bomba, Ken Lynch and Peter Feltham. A Technological Model to Define Access to Electronic Clinical Records. IEEE Transactions on Information Technology in Biomedicine, Vol. 9, No. 2, Juny 2005, 289-290.

[47] Weider D. Yu Mark and A. Chekhanovskiy. An Electronic Health Record Content Protection System Using SmartCard and PMR, 9th International Conference on e-Health Networking, Application and Services, 19-22 June 2007, pages 11-18.

[48] Ashish Dwivedi, Rajeev K. Bali, Meletis A. Belsis, Raouf N G. Naguib, Peter Every and Nahy S. Nassar. Towards a practical healthcare information security model for healthcare institutions. Proceedings of the 4th Annual IEEE Conference on Information Tecnology Applications in Biomedicine, pages 114-117, Abril 2003.

[49] Ana Ferreira, Luís Barreto, Pedro Branão, Ricardo Correia, Susana Sargento and Luís Antunes. A secure wireless architecture to access a virtual electronic patient record. Pervasive Health Conference and Workshops, pages 1-8, Novembre 2006.

[50] Lu-Chou Huang, Huei-Chung Chu, Chung-Yueh Liea, Chia-Hung Hsiao and Tsair Kao.

Privacy preservation and information security protection for patients' portable electronic health records, Computers in Biology and Medicine, Volume 39, Issue 9, pages 743-750, Elsevier, Septembre 2009.

[51] Qian Liu Yuan Hong, Shuo Lu and Rachida Dssouli Lingyu Wang. Preserving privacy in e-health systems using hippocratic databases. Annual al IEEE International Computer Software and Applications Conference, pages 269-297, 2008.

[52] Jinyuan Sun and Yuguang Fang. Cross-Domain Data Sharing in Distributed Electronic Health Record Systems. IEEE Transactions On Parallel And Distributed Systems, Vol. 21, No. 6, Juny 2010, 754-764.

[53] Gustavo H. M. B. Motta and Sergio S. Furuie. A contextual role-based access control authorization model for electronic patient record. IEEE Transactions on Information Technology in Biomedicine, 7(3):202-207, Setembre 2003.

[54] Meystre et al. Automatic de-identification of textual documents in the electronic health record: a review of recent research. BMC Medical Research Methodology 2010, 10:70. http://www.biomedcentral.com/content/pdf/1471-2288-10-70.pdf

[55] Guido van 't Noordende. Security in the Dutch Electronic Patient Record System.

Proceedings of the second annual workshop on *Security* and privacy in medical and home-care systems, ACM New York, NY, USA 2010.

[56] W.-B. Lee and C.-D. Lee. A Cryptographic Key Management Solution for HIPAA Privacy/Security Regulations. IEEE Trans. Information Technology in Biomedicine, vol. 12, no. 1, pp. 34-41, Jan. 2008.

[57] Jing Li, Jung-San Lee i Chin-Chen Chang. Preserving PHI in compliance with HIPAA privacy/security regulations using cryptographic techniques. Proceedings of the 2008 International Conference on Intelligent Information Hiding and Multimèdia Signal Processing IEEE Computer Society Washington, DC, USA.

[58] Ali Sunyaev, Dmitry Chornyi, Christian Mauro i Helmut Krcmar. Evaluation Framework for Personal Health Records: Microsoft HealthVault vs. Google Health. Proceedings of the 43rd Hawaii International Conference on System Sciences, 5-8 January 2010, IEEE Computer Society.

[59] Smart Card Handbook, Wolfgang Rank i Wolfgang Effing, John Wiley & Sons, 2004.

[60] Public key certificate

http://en.wikipedia.org/wiki/Public_key_certificate

[61] Wi-Fi Protected Access

http://ca.wikipedia.org/wiki/Wi-Fi_Protected_Access

[62] IEEE 802.11i-2004

http://en.wikipedia.org/wiki/IEEE_802.11i-2004

[63] IPSec

http://en.wikipedia.org/wiki/IPsec

[64] Digital signature

http://en.wikipedia.org/wiki/Digital_signature

[65] Message authentication code

http://en.wikipedia.org/wiki/Message_authentication_code

[66] Digital Signature Algorithm

http://en.wikipedia.org/wiki/Digital_Signature_Algorithm

[67] Bjørn-Erik Stenbakk et al., Role models in healthcare, Norwegian University of Science and Technology, Department of computer and information science, 2004.

http://www.pvv.ntnu.no/~gunnarre/studies/for/rmhcStenbakkOie.pdf

[68] Mary Thompson et al., Certificate-based Access Control for Widely Distributed Resources, Proceeding SSYM'99 Proceedings of the 8th conference on USENIX Security Symposium - Volume 8 USENIX Association Berkeley, CA, USA, 1999.

http://acs.lbl.gov/~mrt/papers/AkentiUsenixSec.pdf

[69] Sistema HCE de la Unió Europea

http://www.epsos.eu/home.html

[70] Sistema nacional HCE al Regne Unit

http://www.clinfowiki.org/wiki/index.php/National_Electronic_Health_Record_Program_in_United_Kingdom

[71] Sistema nacional HCE a França

http://www.ehealtheurope.net/Features/item.cfm?docId=194

[72] Sistema nacional HCE a Estònia

http://eng.e-tervis.ee/overview.html

[73] VistA (sistema americà)

http://en.wikipedia.org/wiki/VistA

[74] HealthConnect (sistema australià)

http://en.wikipedia.org/wiki/HealthConnect

[75] List of open source healthcare software

http://en.wikipedia.org/wiki/List_of_open_source_healthcare_software

[76] Open Source Software for Públic Health

http://www.ibiblio.org/pjones/wiki/index.php/Open_Source_Software_for_Public_Health

[77] OpenMRS

http://en.wikipedia.org/wiki/OpenMRS

[78] Plataforma Tolven

http://www.tolven.org/

[79] MOSS

http://www.misysoss.com/

[80] OpenExchange

https://www.projects.openhealthtools.org/sf/projects/openexchange/

[81] IHE

http://www.ihe.net/

[82] Medfloss

http://www.medfloss.org/

[83] Google Health

http://es.wikipedia.org/wiki/Google_Health

[84] HealthVault de Microsoft

http://en.wikipedia.org/wiki/Microsoft_HealthVault

[85] Normes de privacitat i seguretat HIPAA.

http://www.bricker.com/services/resource-details.aspx?resourceid=217

[86] Meaningful use. Descripció general.

http://en.wikipedia.org/wiki/Electronic_health_record#Meaningful_Use

[87] Meaningful use. Programa de certificació.

http://healthit.hhs.gov/portal/server.pt?open=512&objID=2885&parentname=CommunityPage&parentid=72&mode=2&in_hi_userid=12059&cached=true

[88] Meaningful use. Organismes de certificació autoritzats.

http://healthit.hhs.gov/portal/server.pt?open=512&mode=2&objID=3120

[89] Meaningful use. Descripció de les tres etapes.

https://www.cms.gov/apps/media/press/factsheet.asp?Counter=3794&intNumPerPage=10&checkDate=&checkKey=&srchType=1&numDays=3500&srchOpt=0&srchData=&keywordType=All&chkNewsType=6&intPage=&showAll=&pYear=&year=&desc=&cboOrder=date

[90] Meaningful use. Objectius i mesures de l'etapa 1 (2011-2012).

http://mycourses.med.harvard.edu/ec_res/nt/26F568D6-E6F3-418A-96B9-497666DEF5C0/MUQuick.pdf

[91] Meaningful use. Comparativa de les tres etapes.

http://www.worh.org/hit/2011/02/stage-2-and-3-meaningful-use-objective-proposed-recommendations/

Annexos.

Annex 1. Normes HIPAA de seguretat i privadesa.

Aquest annex recull secció per secció documentació de les normes HIPAA de seguretat i privadesa [85].

INTRODUCTORY MATERIAL: Relationship to Other Federal Laws PART 160 GENERAL ADMINISTRATIVE REQUIREMENTS
General Provisions: Subpart A
Statutory Basis and Purpose - Section 160.101
Applicability - Section 160.102
Definitions - Section 160.103
Modifications - Section 160.104
Preemption of State Law: Subpart B
Applicability - Section 160.201
Definitions - Section 160.202
General Rule and Exceptions - Section 160.203
Process for Requesting Exception Determinations - Section 160.204
Duration of Effectiveness of Exception Determinations - Section 160.205
Compliance and Enforcement: Subpart C
Applicability - Section 160.300
Definitions - Section 160.302
Principles for Achieving Compliance - Section 160.304
Complaints to the Secretary - Section 160.306
Compliance Reviews - Section 160.308
Responsibilities of Covered Entities - Section 160.310
Secretarial Action Regarding Complaints and Compliance Reviews - Section 160.312
PART 164 SECURITY AND PRIVACY
General Provisions: Subpart A
Statutory Basis - Section 164.102
Definitions- Section 164.103
Applicability - Section 164.104
Organizational Requirements - Section 164.105
Relationship to Other Parts - Section 164.106

Tabla 13. Normes HIPAA de seguretat i privadesa (I).

Security Standards for the Protection of Electronic Protected Health Information: Subpart C
Applicability - Section 164.302
Definitions - Section 164.304
General Rules - Section 164.306
Administrative Safeguards - Section 164.308
Responsibilities of Covered Entities - Section 160.310
Technical Safeguards - Section 164.312
Organizational Requirements - Section 164.314
Policies and Procedures and Documentation Requirements - Section 164.316
Compliance Dates for the Initial Implementation of the Security Standards - Section 164.318
Appendix: Matrix
Notification in the Case of Breach of Unsecured Protected Health Information: Subpart D
Applicability - Section 164.400
Definitions: Breach - Section 164.402
Definitions: Unsecured Protected Health Information - Section 164.402
Notification to Individuals: General Rule - Section 164.404(a)
Notification to Individuals: Timeliness of Notification - Section 164.404(b)
Notification to Individuals: Content of Notification - Section 164.404(c)
Notification to Individuals: Methods of Individual Notification - Section 164.404(d)
Notification to the Media - Section 164.406
Notification to the Secretary of HHS - Section 164.408
Notification By Business Associates- Section 164.410
Law Enforcement Delay- Section 164.412
Administrative Requirements and Burden of Proof - Section 164.414
Applicability - Section 164.500
Definitions: Section 164.501
General Rules for Uses and Disclosures of Protected Health Information: Section 164.502
Uses and Disclosures - Organizational Requirements - Component Entities, Affiliated Entities, Business Associates and Group Health Plans: Section Section 164.504
Uses and Disclosures to Carry Out Treatment, Payment or Health Care Op.: Section 164.506
Uses and Disclosures For Which an Authorization is Required: Section 164.508
Uses and Disclosures Requiring an Opportunity for the Individual to Agree or to Object: Section 164.510
Uses and Disclosures For Which Consent, an Authorization, or Opportunity to Agree or Object is Not Required: Section 164.512
Other Requirements Relating to Uses and Disclosures of PHI: Section 164.514
Notice of Privacy Practices for Protected Health Information: Section 164.520
Rights to Request Privacy Protection for Protected Health Information: Section 164.522
Access of Individuals to Protected Health Information: Section 164.524
Amendment of Protected Health Information: Section 164.526
Accounting of Disclosures of Protected Health Information: Section 164.528
The Administrative Requirements: Section 164.530
Transition Provisions - Section 164.532
Compliance Dates - Section 164.534

Tabla 14. Normes HIPAA de seguretat i privadesa (II).

Annex 2. Ús assenyat (Meaningful Use).

El terme ús assenyat (en anglès, meaningful use) descriu l'ús de la tecnologia d'informació sanitària (HIT) de manera que condueixi a la millora de la salut i a la promoció dels objectius d'intercanvi d'informació entre els professionals de la salut. Es tracta d'un conjunt coordinat de regulacions per ajudar a crear un sistema electrònic d'informació de salut privat i segur [86].

Per arribar a ser un "usuari assenyat" els proveïdors han de superar un programa de certificació [87] supervisat per una entitat certificadora acreditada [88].

El programa de TI de salut de l'Administració d'Obama té la intenció d'utilitzar les inversions federals per estimular el mercat HCE.

La definició detallada dels objectius i de les mesures s'ha d'establir en tres etapes durant un període de temps fins l'any 2015 [89]. Fins ara només s'ha definit l'etapa 1.

Etapa 1

Els criteris de l'etapa 1 s'orienten a la captura d'informació de salut electrònica en un format codificat, usant aquesta informació per tal de trobar condicions clíniques claus, comunicant aquesta informació a efectes de coordinació de l'atenció mèdica, i informant de les mesures de qualitat clínica i de salut pública.

Els criteris es basen en una sèrie de categories específiques, cadascuna de les quals està vinculada a una sèrie d'objectius i mesures que permeten demostrar que els professionals i els hospitals són usuaris assenyats de tecnologia HCE certificada.

Per a l'etapa 1 (2011-2012), hi haurà 25 categories per als professionals (EPs o eligible professionals) i 24 categories per als hospitals.

Les categories s'han dividit en un conjunt bàsic (Core Set) i un conjunt opcional (Menu Set).

De les 16 categories del Core Set, una no s'aplica als EPs per la qual cosa hauran de complir-ne 15.

D'altra banda, hi ha dues categories que no s'apliquen als hospitals per la qual cosa hauran de complir-ne 14.

Igualment, de les 12 categories del Menu Set, n'hi ha dues que no s'apliquen als EPs per la qual cosa el conjunt efectiu de categories es redueix a 10. D'aquestes 10 categories hauran de seleccionar 5.

El mateix passa amb els hospitals. Hi ha dues categories que no s'apliquen als hospitals per la qual cosa el conjunt efectiu de categories es redueix a 10. D'aquestes 10, n'hauran de seleccionar 5.

Etapa 2

L'etapa 2 amplia els criteris de l'etapa 1 en les àrees de gestió de la malaltia, suport de decisions clíniques, suport de gestió a la medicació, el mesurament de la qualitat i la recerca, i la comunicació bidireccional amb els organismes de salut pública. Aquests canvis es reflectiran en un major nombre de requisits bàsics per a l'etapa 2. S'està considerant aplicar els criteris de manera més àmplia als pacients ambulatoris de l'hospital (i no només el servei d'urgències). L'intercanvi d'informació és una part fonamental per a la coordinació de l'atenció i s'espera que la infraestructura suporti més requisits per a establir els intercanvis d'informació sanitària de l'etapa 2.

Etapa 3 s'orientarà a la consecució de millores en la qualitat, la seguretat i l'eficiència, centrant-se en el suport a les decisions nacionals d'alta prioritat, l'accés del pacient a eines d'autogestió, l'accés global a les dades del pacient, i la millora dels resultats de salut de la població.

Les taules següents mostren una llista completa de les categories per a l'etapa 1 [90].

En el CORE SET els professionals i hospitals han de complir tots els objectius i mesures de les categories que siguin aplicables. En el MENU SET, els professionals i hospitals han de complir tots els objectius i mesures de les 5 categories que seleccionin (les altres 5 es deixen per l'etapa 2).

Categoria	Aplicable a
1. Fer les comandes de medicaments de forma automàtica.	Hospitals i EPs
2. Establir controls sobre les interaccions entre medicaments i els seus efectes sobre les al·lèrgies.	Hospitals i EPs
3. Generar i transmetre les receptes electrònicament.	Només EPs
4. Registrar les dades demogràfiques.	Hospitals i EPs
5. Mantenir una llista actualitzada dels diagnòstics actuals.	Hospitals i EPs
6. Mantenir la llista de medicaments activa.	Hospitals i EPs
7. Mantenir la llista d'al·lèrgies a medicaments.	Hospitals i EPs
8. Portar un registre gràfic dels canvis en els signes vitals.	Hospitals i EPs
9. Registrar els pacients fumadors de 13 anys o més.	Hospitals i EPs
10. Implementar regles de suport a les decisions clíniques.	Hospitals i EPs
11. Informar sobre mesures de qualitat ambulatòria al CMS (Center for Medicare & Medicaid Services) o als estats.	Hospitals i EPs
12. Proporcionar als pacients una còpia electrònica de la seva informació mèdica quan ho demanin.	Hospitals i EPs
13. Proporcionar als pacients una còpia electrònica de les instruccions de l'alta.	Només Hospitals
14. Proporcionar resums clínics als pacients per cada visita al consultori.	Només EPs
15. Capacitat d'intercanvi d'informació clínica electrònica entre els proveïdors i les entitats autoritzades.	Hospitals i EPs
16. Protegir la informació de salut electrònica (privacitat i seguretat).	Hospitals i EPs

Tabla 15. CORE SET.

Categoria	Aplicable a
1. Establir controls de medicaments amb formularis.	Hospitals i EPs
2. Testament vital.	Només Hospitals
3. Incorporar els resultats de proves clíniques de laboratori com dades estructurades en els HCEs certificats.	Hospitals i EPs
4. Generar llistes dels pacients segons condicions específiques per a millorar la qualitat, la recerca i la divulgació.	Hospitals i EPs
5. Enviar recordatoris als pacients per a seguiment / atenció preventiva.	Només EPs
6. Proporcionar als pacients l'accés a la seva informació electrònica de salut (incloent resultats de laboratori, llista de problemes, llistes de medicaments, al·lèrgies)	Només EPs
7. Educació específica del pacient	Hospitals i EPs
8. Utilitzar HCEs certificats per identificar informació específica d'interès per a cada pacient.	Hospitals i EPs
9. Comprovar la compatibiltat dels medicaments.	Hospitals i EPs
10. Proporcionar informació resumida de l'atenció rebuda en cas de derivació del pacient a altres institucions.	Hospitals i EPs
11. Enviar dades electròniques als registres de vacunació.	Només Hospitals
12. Enviar dades de seguiment de síndromes a les agències de salut pública.	Hospitals i EPs

Tabla 16. MENU SET.

Les taules següents mostren una comparativa de les tres etapes [91]. Llegenda: EP (Eligible Professional); EH (Eligible Hospital); CAH (Critical Access Hospital); CPOE (Computerized Provider Order Entry); ED (Emergency Department) ; CMS (Center for Medicare & Medicaid Services); PCP (Primary Care Physician); IIS (Immunization Information Systems)

Mesura	**Proveïdor**	**Objectius de l'etapa 1**	**Etapes 2 i 3: Proposta del HIT Policy Committee**
Core-1	Hospitals i EPs	Un professional autoritzat utilitza CPOE per fer comandes de medicaments del 30% dels pacients ingressats i d'urgències.	La proposta per l'etapa 2 és fer comandes de radiologia i de laboratori, i incrementar el llindar al 60%. El llindar proposat per l'etapa 3 és 80%
Core-2	Hospitals i EPs	Establir controls sobre les interaccions entre medicaments i els seus efectes sobre les al·lèrgies.	La proposta per l'etapa 2 és fer controls basat en evidències. L'etapa 3 pot afegir contraindicacions entre medicaments i laboratori.
Core-3	Només EPs	Generar i transmetre electrònicament el 40% de les receptes (eRx).	La proposta per l'etapa 2 és incrementar al 60 % el llindar de les comandes (pacients ambulatoris i altes hospitalàries). El llindar proposat per l'etapa 3 és 90%.
Core-4	Hospitals i EPs	Mantenir una llista d'incidències actualitzada de diagnosis del 80% dels pacients ingressats i d'urgències com a mínim.	La proposta per l'etapa 2 és continuar l'etapa 1. La proposta per l'etapa 3 és actualitzar el 80% de les llistes d'incidències.
Core-5	Hospitals i EPs	Mantenir una llista de medicaments actualitzada del 80% dels pacients ingressats i d'urgències com a mínim.	La proposta per l'etapa 2 és continuar l'etapa 1. La proposta per l'etapa 3 és actualitzar el 80% de les llistes de medicaments.
Core-6	Hospitals i EPs	Mantenir una llista d'al·lèrgies a medicaments actualitzada del 80% dels pacients ingressats i d'urgències com a mínim.	La proposta per l'etapa 2 és continuar l'etapa 1. La proposta per l'etapa 3 és actualitzar el 80% de llista d'al·lèrgies a medicaments.
Core-7	Hospitals i EPs	Registrar les dades demogràfiques (llengua materna, sexe, ètnia, data de naixement, data i motiu de la mort si s'escau) del 50% dels pacients ingressats i d'urgències com a mínim.	La proposta per l'etapa 2 és incrementar el llindar al 80% (i usar les dades per generar informes estratificats de qualitat). El llindar proposat per l'etapa 3 és 90%.
Core-8	Hospitals i EPs	Registre gràfic i canvis en els signes vitals (alçada, pes, pressió arterial, IMC, gràfics de creixement de nens amb 2-20 anys d'edat) del 50% dels pacients hospitalitzats i d'urgències com a mínim.	La proposta per les etapes 2 i 3 és incrementar el llindar al 80%
Core-9	Hospitals i EPs	Registrar la condició de fumador del 50 % dels pacients hospitalitzats i d'urgències amb 13 anys d'edat o més.	La proposta per l'etapa 2 és incrementar el llindar al 80% i per l'etapa 3 al 90%.
Core-10	Hospitals i EPs	Informar sobre mesures de qualitat ambulatòria al CMS o als estats.	Ho està tractant el grup de treball de mesures de qualitat.

Tabla 17. Meaningful use. Comparativa de les tres etapes (I).

Mesura	Proveïdor	Objectius de l'etapa 1	Etapes 2 i 3: Proposta del HIT Policy Committee
Core-11	Hospitals i EPs	Implementar una regla de suport a la decisió clínica relacionada amb les condicions dels hospitals prioritaris que sigui rellevant per a les mesures de qualitat clíniques, (incloent peticions de proves diagnòstiques) i veure el seu compliment.	La proposta per les etapes 2 i 3 és usar sistemes de suport a la decisió clínica per millorar les condicions dels hospitals prioritaris, i afegir requisits de certificació.
Core-12	Hospitals i EPs	Proporcionar com a mínim al 50 % dels pacients una còpia electrònica de la seva informació mèdica (incloent resultat de proves, llista de problemes, llista de medicament, al·lèrgies, informe d'alta mèdica i procediments), quan ho demanin i en un termini màxim de 3 dies feiners.	La proposta per l'etapa 2 és continuar l'etapa 1. La proposta per l'etapa 3 és incrementar el llindar al 90%.
Core-13	Només Hospitals	Proporcionar als pacients en el moment de l'alta mèdica una còpia electrònica del seu informe d'alta del 50% dels pacients que ho demanin com a mínim.	La proposta per l'etapa 2 és incrementar el llindar al 80%. El llindar proposat per l'etapa 3 és 90%.
Core-14	Només EPs	Proporcionar als pacients resums clínics de cada visita a la consulta.	La proposta per l'etapa 2 és permetre als pacients veure o descarregar dades de forma llegible en les 24 hores posteriors a la consulta. La proposta per l'etapa 3 és que les dades estiguin de forma estructurada.
Core-15	Hospitals i EPs	Capacitat d'intercanviar informació clau clínica (per exemple, l'informe d'alta, procediments, llistes de problemes, llistes de medicaments, al·lèrgies, i resultats de les proves) entre els proveïdors de l'atenció mèdica i les entitats autoritzades per via electrònica.	La proposta per l'etapa 2 és connectar a 3 proveïdors externs com a mínim a la xarxa de referència primària o establir una connexió bidireccional com a mínim amb un node d'intercanvi. La proposta per l'etapa 3 és connectar al 30% dels proveïdors externs com a mínim a la xarxa de referència primària o establir una connexió bidireccional com a mínim amb un node d'intercanvi..
Core-16	Hospitals i EPs	Protegir la informació mèdica electrònica creada o mantinguda per la tecnologia HCE certificada amb tècniques adients.	L'equip de privacitat i seguretat està considerant objectius de privacitat i seguretat addicionals.

Tabla 18. Meaningful use. Comparativa de les tres etapes (II).

Mesura	Proveïdor	Objectius de l'etapa 1	Etapes 2 i 3: Proposta del HIT Policy Committee
Menu-1	Hospitals i EPs	Establir controls de medicaments amb formularis.	La proposta per l'etapa 2 és passar aquesta mesura a la part bàsica (core). La proposta per l'etapa 3 és controlar el 80% de les comandes amb formularis.
Menu-2	Només Hospitals	Registrar directives per al 50 % dels pacients hospitalitzats amb 65 anys o més.	La proposta per l'etapa 2 és registrar el resultat de la directiva del 50% dels pacients hospitalitzats amb 65 anys o més. La proposta per l'etapa 3 és incrementar el llindar al 90%.
Menu-3	Hospitals i EPs	Incorporar el 40% dels resultats de les proves de laboratori a l'HCE com dades estructurades	La proposta per l'etapa 2 és passar aquesta mesura a la part bàsica (core). La proposta per l'etapa 3 és incrementar el llindar al 80% , i conciliar la informació amb les comandes de laboratori.
Menu-4	Hospitals i EPs	Generar llistes de pacients per condicions específiques per a millorar la qualitat, la reducció de les disparitats i la divulgació.	La proposta per l'etapa 2 és generar llistes de pacients d'acord a múltiples paràmetres (i passar aquesta mesura a la part bàsica). La proposta per l'etapa 3 és usar les llistes per gestionar els pacients prioritaris.
Menu-5	Només EPs	Enviar recordatoris als pacients per a seguiment / atenció preventiva segons les seves preferències.	La proposta per l'etapa 2 és passar aquesta mesura a la part bàsica. La proposta per l'etapa 3 és que el 20% dels pacients que vulguin rebin els recordatoris preventius o de seguiment de forma electrònica.
Menu-6	Només EPs	Proporcionar als pacients l'accés oportú a la informació electrònica de salut (incloent resultats de laboratori, llistes de problemes, llistes de medicaments, al·lèrgies a medicaments) en un termini de 4 dies hàbils des que el proveïdor té la informació.	La proposta per l'etapa 2 és permetre als pacients veure o descarregar dades de forma llegible. La proposta per l'etapa 3 és que les dades estiguin disponibles de forma estructurada.
Menu-7	Hospitals i EPs	Identificar i proveir recursos educatius per al 10% dels pacients hospitalitzats i d'urgències.	La proposta per l'etapa 2 és continuar l'etapa 1. La proposta per l'etapa 3 és incrementar el llindar al 20% i oferir els recursos en línia en els llenguatges comuns.
Menu-8	Hospitals i EPs	Conciliar les dades mèdiques durant les visites i derivacions per al 50% dels pacients hospitalitzats i d'urgències derivats.	La proposta per l'etapa 2 és incrementar el llindar al 80%. La proposta per l'etapa 3 és incrementar el llindar al 90%.

Tabla 19. Meaningful use. Comparativa de les tres etapes (III).

Mesura	Proveïdor	Objectius de l'etapa 1	Etapes 2 i 3: Proposta del HIT Policy Committee
Menu-9	Hospitals i EPs	Proporcionar resums de les derivacions per al 50% dels pacients hospitalitzats derivats.	La proposta per l'etapa 2 és passar aquesta mesura a la part bàsica. La proposta per l'etapa 3 és incrementar el llindar al 80%.
Menu-10	Hospitals i EPs	Capacitat per presentar les dades electròniques als registres de vacunació i la presentació real d'acord amb la llei i la pràctica mèdica.	La proposta per l'etapa 2 és que la prova sigui obligatòria i que, per a algunes vacunes, es presentin a l'IIS. La proposta per l'etapa 3 és que les vacunes es presentin a l'IIS i que els proveïdors revisin els seus registres IIS mitjançant el seu HCE.
Menu-11	Només Hospitals	Capacitat per presentar de forma electrònica les proves de laboratori a les agències de salut pública.	La proposta per l'etapa 2 és passar aquesta mesura a la part bàsica, i fer un nou requisit per als proveïdors. La proposta per l'etapa 2 és que la prova sigui obligatòria i enviar els resultats de les proves de laboratori.
Menu-12	Hospitals i EPs	Capacitat per enviar dades de seguiment de síndromes a les agències de salut pública.	La proposta per l'etapa 2 és passar aquesta mesura a la part bàsica. La proposta per l'etapa 3 és que la prova sigui obligatòria.

Tabla 20. Meaningful use. Comparativa de les tres etapes (IV).

Mesura	Proveïdor	Nous objectius de l'etapa 2	Nous objectius de l'etapa 3
Nova	Només EPs	El 30% de les visites tenen una anotació electrònica com a mínim. Pot ser escanejada, narrativa, estructurada, etc.	El 90% de les visites tenen una anotació electrònica com a mínim. Pot ser escanejada, narrativa, estructurada, etc.
Nova	Només Hospitals	El 30% de les visites tenen una anotació electrònica feta per un metge, infermera o assistent com a mínim. Pot ser escanejada, narrativa o estructurada.	El 80% de les visites tenen una anotació electrònica feta per un metge, infermera o assistent com a mínim. Pot ser escanejada, narrativa o estructurada
Nova	Només Hospitals	30% de les prescripcions de medicaments de l'hospital són rastrejades automàticament a través del registre electrònic d'administració de medicaments.	80% de les prescripcions de medicaments de l'hospital són rastrejades automàticament a través del registre electrònic d'administració de medicaments.
Nova	Només Hospitals	80% dels pacients tenen la possibilitat de veure i descarregar a través del portal, dins de les 36 hores posteriors a l'alta, informació pertinent continguda en el registre sobre les visites als pacients hospitalitzats. Les dades estan disponibles en forma llegible (PDF o text).	80% dels pacients tenen la possibilitat de veure i descarregar a través del portal, dins de les 36 hores posteriors a l'alta, informació pertinent continguda en el registre sobre les visites als pacients hospitalitzats. Les dades estan disponibles en forma estructurada (Continuity of Care Record o Continuity of Care Document).
Nova	Hospitals i EPs	Registrar les preferències de comunicació per a un mínim del 20% dels pacients.	Registrar les preferències de comunicació per a un mínim del 80% dels pacients.
Nova	Hospitals i EPs		Oferir eines electròniques d'autogestió a pacients prioritaris.
Nova	Hospitals i EPs		Les HCEs poden intercanviar dades amb els registres de salut personals utilitzant estàndards.
Nova	Hospitals i EPs		Els pacients poden informar en línia sobre les experiències obtingudes de les mesures d'atenció mèdica adoptades.
Nova	Hospitals i EPs		És possible pujar i incorporar dades generades pel pacient en les HCEs.
Nova	Hospitals i EPs	Disponible a l'HCE la llista dels membres de l'equip d'atenció mèdica (incloent el metge d'atenció primària) del 10% dels pacients com a mínim.	Disponible la llista dels membres de l'equip d'atenció mèdica del 50% dels pacients com a mínim via intercanvi electrònic.
Nova	Hospitals i EPs	Registrar un pla d'atenció mèdica per a un 20% dels pacients prioritaris com a mínim.	Disponible via intercanvi electrònic un pla d'atenció mèdica per a un 50% dels pacients prioritaris com a mínim.

Tabla 21. Meaningful use. Comparativa de les tres etapes (V).

Annex 3. HL7.

Health Level Seven (HL7), és una organització sense ànim de lucre formada per voluntaris, involucrades en el desenvolupament de les normes internacionals d'interoperabilitat informàtica del sector sanitari. HL7 s'utilitza també per referir-se a alguns dels estàndards específics creats per l'organització. Les normes, que donen suport a la pràctica clínica i a la gestió, execució i avaluació dels serveis de salut, són les més utilitzades en el món.

L'organització

HL7 és la sigla de Health Level Seven Inc. La paraula "Health" (Salut) fa relació a l'àrea de treball de l'organització i les paraules "Level Seven" (Nivell Set) fan referència a l'últim nivell del model OSI-ISO. El "Nivell Set" dins del model és el nivell aplicació, que s'ocupa de la definició i l'estructura de les dades que seran intercanviades.

Els estàndards

HL7 compta amb especificacions de missatges, documents electrònics i vocabularis controlats per a dominis de salut com ara CDA, registres mèdics, laboratori, medicació, DICOM, atenció mèdica, banc de sang, teixits i òrgans, etc. Alguns d'aquests estàndards són:

- Missatgeria HL7 Versió 2: Estàndard de missatgeria per a l'intercanvi electrònic de dades de salut.
- Missatgeria HL7 Versió 3: Estàndard de missatgeria per a l'intercanvi electrònic de dades de salut basada en RIM (Reference Information Model).
- CDA HL7: (Clinical Document Architecture): Estàndard d'arquitectura de documents clínics electrònics.
- SPL HL7: (Structured Product Labeling): Estàndard electrònic d'etiquetatge de medicaments.
- HL7 Medical Records: Estàndard d'administració de Registres Mèdics.
- GELLO: Estàndard per a l'expressió de regles de suport de decisions clíniques.
- Arden Sintax: Estàndard sintàctic (if then) per compartir regles de coneixement clínic.
- CCOW (Clinical Context Object Workgroup): Estàndard dissenyat per a permetre la sincronització en temps real de diferents aplicacions a nivell de la interfície d'usuari.

Annex 4. ISO TC 215.

L'ISO / TC 215 és el Comitè de Normalització Tècnica (CT) en informàtica de la salut d'ISO.

TC 215 treballa en la normalització TIC en l'àrea de la Salut, per permetre la compatibilitat i la interoperabilitat entre sistemes independents.

ISO TC 215 es compon de diversos grups de treball (GT), cadascun dedicat a un aspecte dels historials clínics electrònics (HCE):

• CAG 1: Consell Executiu, l'harmonització i les operacions.

• Grup de Treball 1: Estructura de dades.

• Grup de Treball 2: Missatgeria i comunicacions.

• Grup de Treball 3: Representació del concepte de salut.

• Grup de Treball 4: Privacitat i Seguretat.

• Grup de Treball 5: Targetes Sanitàries.

• Grup de Treball 6: Farmàcia i medicaments.

• Grup de Treball 7: Dispositius.

• Grup de Treball 8: Requeriments de negoci dels HCEs.

• Grup de Treball 9: Harmonització de les organitzacions de desenvolupament d'estàndards (SDO).