

Center för eHälsa i samverkan
Hornsgatan 20, 118 82 Stockholm
Vxl: 08-452 70 00
Tel: 010-1030395

Moa Malviker Wellermark
moa.malviker.wellermark@lio.se
www.cehis.se | info@cehis.se

Råd

Checklista för kravspecifikation för IT-stöd innehållande patientuppgifter (Informationssäkerhet inkl. Patientdatalagen)

Innehåll

| | |
|------------------|---|
| Inledning | 3 |
| Syfte | 4 |
| Checklista | 5 |

Utgåvehistorik för dokumentet

| Utgåva | Datum | Kommentar |
|---------------|--------------|------------------|
| 1.0 | 2011-08-30 | Första utgåva |

Inledning

Patientdatalagen, PDL, (2008:355) och Socialstyrelsens föreskrifter (SOSFS 2008:14) beskriver hur elektroniska patientuppgifter ska hanteras. PDL ger möjligheter för att elektronisk patientinformation kan göras tillgänglig, men förutsätter då att grundläggande säkerhetskrav uppfylls.

Syfte

Checklistan är inte uttömmande och alla punkter på checklistan behöver inte vara behandlade i en kravspecifikation, för att den ska vara tillfyllest och komplett. Innehållet i kravspecifikationen styrs till stor del av omfång och utformning av det aktuella systemet som ska upphandlas. Checklistan skall ses som ett stöd vid upprättande av kravspecifikation för IT-stöd rörande krav på informationssäkerhet som finns grundlagda i PDL och SOSFS 2008:14.

I checklistan står skall vid samtliga krav, huruvida kravet ska vara skall eller bör är upp till upphandlande enhet att avgöra beroende på vilka planer som finns på utveckling och funktionalitet.

Vid användande av checklistan bör egna riktlinjer och rutiner bifogas som kan belysa hur dessa krav ser ut just hos er vårdgivare. Vid krav på detaljstyrning bör förtydligande göras, t.ex. på pkt 13 där det endast står att IT-stödet ska stödja rutin för utdrag enligt PuL 26 § men inte på vilket sätt. Det är här viktigt att den egna vårdgivarens rutin och krav på rutin framställs i kravspecifikationen om det finns särskilda önskemål om detta.

Checklista

- 1) Patienten **skall** ges en unik identitet i IT-stödet . Följande identiteter skall hanteras i IT-stödet
 - Personnummer
 - Samordningsnummer
 - Reservnummer
 - Nationellt reservnummer (när tjänst med specificerat nationellt format är tillgänglig)
- 2) Patientuppgifter registrerade under reservnummer **skall** kunna kopplas till/ slås ihop med personnummer/samordningsnummer i samma IT-stöd.
- 3) IT-stödet **skall** kunna hantera olika typer av skyddade personuppgifter.
- 4) Hälso- och sjukvårdspersonal (de som är delaktiga i vården) **skall** i IT-stödet vara starkt autentiserade enligt PKI-standard med SITHS-certifikat som innehåller unik identitet i form av HSA-ID. SITHS CA kommer framledes att finnas i mer än en version. IT-stödet skall därmed parallellt kunna hantera olika certifikatversioner och tillhörande CA-certifikat.
- 5) Patienter **skall** i IT-stöd, som ger patienter direktåtkomst till egna patient- eller logguppgifter, vara starkt autentiserad enligt PKI-standard med e-legitimation som innehåller unik identitet i form av personnummer och med smartkort som bärare av privat nyckel.
- 6) Övrig personal som har rättigheter i IT-stödet, t ex systemadministratörer, **skall** också vara starkt autentiserade.
- 7) Hälso- och sjukvårdspersonal och patientinformation **skall** vara identifierbara utifrån patientdatalagens definitioner av termerna vårdgivare och vårdenhet, vilka finns i HSA-katalogen. Detta innebär att begreppen vårdgivare och vårdenhet skall hanteras i tjänsternas informations- och datamodell.
- 8) Behörighetstilldelning **skall** grundas på överenskomna rättighetsstyrande egenskaper och medarbetaruppdrag i HSA-katalogen generellt eller i kombination med i IT-stödet definierade roller.
- 9) IT-stödet **skall** göra patientuppgifter tillgängliga stegvis med aktiva val utanför egen vårdenhet. Dessa steg är: andra vårdenheter inom samma vårdgivare och andra vårdgivare. Det betyder att användaren aktivt måste ta ställning till om denne har behov av uppgifterna hos en annan vårdenhet genom t.ex. ett musklick innan denne får ta del av patientuppgifterna. Aktiva val **skall** loggas.
- 10) IT-stödet **skall** stödja rutin för automatisk låsning av patientuppgifter som ej aktivt bekräftats/signerats. Låsta uppgifter skall inte kunna låsas upp men skall ändå kunna bekräftas/signeras i efterhand. Status avseende om patientuppgift är bekräftad/signerad eller

låst skall tydligt framgå. Tidsintervall på låsning ska kunna ändras av vårdgivaren under avtalets gång.

- 11) Patientuppgifter **skall** kunna bekräftas/signeras och låsas genom e-underskrift, det vill säga med användande av certifikat.
- 12) Tidpunkt för en patients vårdkontakt, tidpunkt för en journalanteckning samt tidpunkt för bekräftelse/signering och/eller låsning **skall** finnas registrerad i IT-stödet.
- 13) IT-stödet **skall** möjliggöra förstöring av patientuppgifter efter beslut av Socialstyrelsen. Leverantören **skall** förbinda sig att tillhandahålla resurser, vilka mot överenskommen ersättning, ska ombesörja att förstörande av patientjournal kan ske i enlighet med beslut från Socialstyrelsen alt. **skall** leverantören tillhandahålla beskrivning hur kunden kan genomföra förstöringen på egen hand.
- 14) IT-stödet **skall** stödja rutin för uttag enligt Personuppgiftslagen § 26 och Tryckfrihetsförordningen kap 2 § 1.
- 15) IT-stödet **skall** vid integration/kommunikation till och från andra IT-stöd kunna tillhandahålla säkerhet med stark autentisering av avsändare och mottagare, insynsskydd och förvanskningsskydd.
- 16) IT-stödet **skall** vid behörighetshantering kunna hantera uppgifter om samtycke, ospärrad och spärrade patientuppgifter via anvisat gränssnitt. Samtycke och spärr **skall** registreras i central spärrtjänst och ej bundet till det enskilda IT-stödet, finns inte central spärrtjänst tillgänglig **skall** egenutvecklad spärrfunktion implementeras.
- 17) IT-stödet **skall** registrera (logga) uppgifter som möjliggör uppföljning avseende informations- och säkerhetsrelaterade händelser. Logguppgifterna ska sparas i minst 10 år. Uttag av logguppgifter ska behörighetshandteras och loggas.

Logguppföljning **skall** ske centralt och ej bundet till det enskilda IT-stödet, finns däremot inte tillgång till central loggfunktion **skall** funktion för registrering och uppföljning finnas i IT-stödet.

För logguppföljning från verksamheten enligt PDL skall följande logguppgifter finnas:

- vem som tagit del av patientuppgifter
- vilka patientuppgifter man tagit del av (bland annat typ av information och organisatoriskt ansvar (vårdgivare/vårdenhet))
- vad som gjorts
- när detta gjorts

- 18) Leverantörens **skall** förbinda sig att anpassa offererat IT-stöd till de Nationella Säkerhetstjänsterna inom separat förhandlad tid och ersättningsmodell. Följande tjänster **skall** hanteras genom att systemet utnyttjar antingen nationellt överenskomna tjänster i de nationella säkerhetstjänsterna för autentisering, rättighetstilldelning (behörighetsstyrning), samtycke och spärr, loggning och logganalays, utlämnande och kontexthantering eller centralt etablerad funktion i landstinget för motsvarande tjänster.