Begränsning av patientval vid sammanhållen vårddokumentation (Tillgänglig patient – TGP)

Funktionsbeskrivning

inera
Ett företag inom SKR

Innehåll

Revisionshistorik

VERSION	DATUM	FÖRFATTARE	KOMMENTAR
1.0	Björn Strihagen		Första version
1.1	Björn Strihagen		Lagt till beskrivning av TGP_Admin
1.2	Madeleine Marklund, Björn Strihagen		Redaktionella ändringar, revidering av mall. Uppdaterad med synpunkter från kommunprojektet
1.3	Björn Strihagen		Kompletterat med TGPx
1.4	Mats Pettersson	2017-04-28	Textuella justeringar
1.5	Anna Schreiber	2022-10-20	Uppdatering av icke aktuell information.
1.6	Annika Fredriksson	2023-01-27	Lagt till avsnitt om online-lösning.
1.7	Annika Fredriksson	2023-03-22	Uppdateringar i kap. 4.5. Mindre justeringar i andra kapitel.
1.8	Annika Fredriksson	2023-07-13	Ersatt ”Sammanhållen journalföring” med ”Sammanhållen vårddokumentation”. Flyttat över till ny dokumentmall.
1.9	Annika Fredriksson	2023-11-15	Uppdaterat avsnitt 4.3 och 4.4.

1. Bakgrund

Integritetsskyddsmyndigheten (dåvarande Datainspektionen) konstaterade vid sin tillsyn av Nationell Patientöversikt (NPÖ) i Örebro 2010 att det vid sammanhållen journalföring (numera Sammanhållen vårddokumentation) är nödvändigt att kunna begränsa åtkomsten, så att en användare enbart ges tillgång till vissa patienter eller kategorier av patienter, och inte automatiskt till samtliga patienter. (Se [2] sid 10).

Programledningen för NPÖ beslutade, efter samråd med anslutande vårdgivare och Integritetsskyddsmyndigheten, att principen för en sådan begränsning skulle baseras på om den aktuella patienten var en "egen patient", vilket i normalfallet innebär att patienten finns i något lokalt vårdsystem.

Denna begränsning gäller utöver kravet på att användaren ska intyga att patientrelation och samtycke finns, och utformas så att användaren inte själv, olovligt, kan passera.

Integritetsskyddsmyndighetens krav på en begränsning av åtkomst gäller all sammanhållen vårddokumentation och inte specifikt för NPÖ. Så även om huvudfokus för dokumentet är att beskriva den lösning som tillämpas i NPÖ, så är målet att såväl innehållet i dokumentet och själva lösningen ska vara applicerbar även i andra sammanhang där sammanhållen vårddokumentation tillämpas.

2. Princip

Den grundläggande principen för begränsning av åtkomst bygger på att endast patienter som behandlas eller har inbokad behandling inom den egna vårdenheten ska vara tillgängliga att välja i samband med åtkomst av den sammanhållna vårddokumentationen. Informationen kan i de flesta fall hämtas från något lokalt vårdsystem[1].

Funktionen Tillgänglig patient (TGP) ska inte ses som en ersättning av kravet på patientrelation eller samtycke enligt PDL. Syftet med TGP är snarare att förhindra att användare under normala omständigheter oavsiktligt (eller avsiktligt) kan komma åt information om patienter där det går att avgöra att patientrelation inte kan föreligga.

Förutom ovanstående måste användaren ha tilldelats rättigheter att ta del av den sammanhållna vårddokumentationen samt ha autentiserat sig med sitt elektroniska id-kort (SITHS-kort). Dessutom ska loggning och uppföljning av användarens åtgärder ske av den aktuella applikationen (NPÖ).

[1] Med vårdsystem avses här alla typer av system där information om den aktuella patienten finns såsom journalsystem, PAS-system och kassasystem.

Kommentar 1:

Det är fullt möjligt att det lokala vårdsystemet hanterar information från olika vårdgivare (och i och med det definitionsmässigt tillämpar sammanhållen vårddokumentation). Att patienten finns i det lokala vårdsystemet kan därför inte jämställas med att patienten är tillgänglig. Med andra ord är det inte säkert att alla patienter som användaren har tillgång till i sitt vårdsystem automatiskt är tillgängliga i NPÖ.

Omvänt skulle det (teoretiskt) kunna finns fall där patienter ska vara tillgängliga i NPÖ även om den inte finns i det lokala vårdsystemet. De fallen är ovanligare än vad man kan tro, eftersom samtliga verksamheter (möjligen med något undantag, exempelvis i ambulanser) har som rutin att de patienter som ska behandlas antingen redan är kallade, kommer via remiss eller skrivs in i det lokala vårdsystemet i samband med besöket (gäller även akuten) och följaktligen finns registrerade i något lokalt vårdsystem.

Kommentar 2:

Formellt är det verksamhetschefen som ansvarar för behörighetsstyrning och därmed avgör regelverket för vilka patienter som ska vara tillgängliga via NPÖ. Integritetsskyddsmyndigheten har inte uttryckt krav på *hur* detta regelverk ser ut, däremot att det ska finnas ett regelverk och att det ska finnas en teknisk möjlighet att genomföra det.

3. Övergripande funktionsbeskrivning

NPÖ:s webbtillämpning (här kallad NPÖ) har ansvar för att kontrollen av att patienten är tillgänglig blir utförd innan patientinformation visas för användaren. Däremot utför inte NPÖ kontrollen själv. Det sker i stället med hjälp av en stödtjänst, *TGP (tillgänglig patient*).

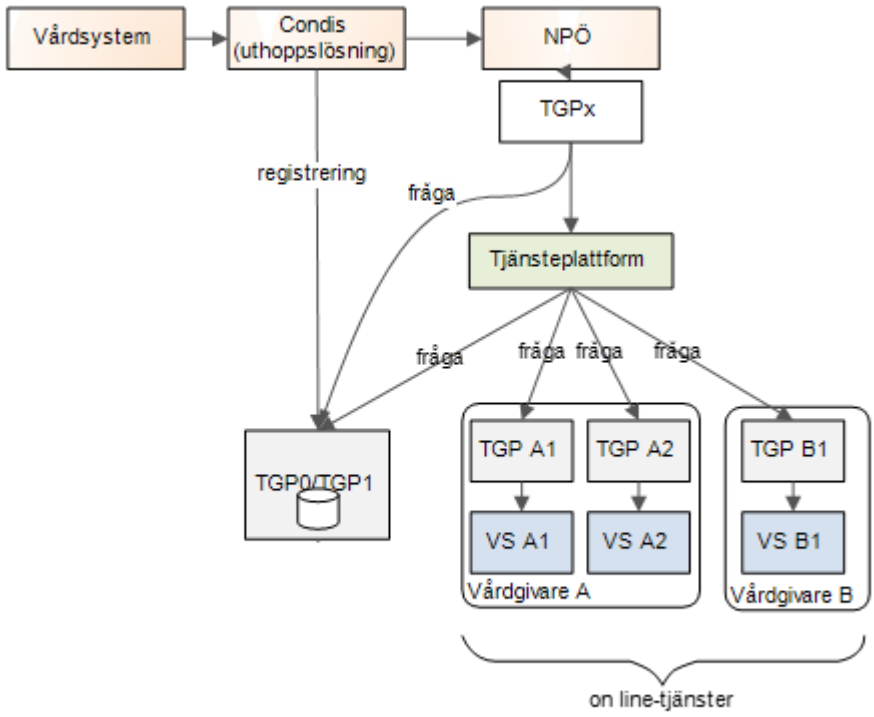
Enligt vanliga benämningar utgör NPÖ *policy enforcement point* (PEP) medan TGP-tjänsten utgör *policy decision point* (PDP).

Som indata från NPÖ till TGP-tjänsten används den aktuella patientens personnummer, användarens HSA-id, samt HSA-id för den vårdgivare och vårdenhet där åtkomsten sker (dvs. där användaren är verksam i sitt aktuella uppdrag).

För att utföra kontrollen krävs att TGP-tjänsten har tillgång till information om vårdkontakter eller motsvarande för de patienter som finns i användarens lokala vårdsystem. Denna information kan TGP-tjänsten få tillgång till på olika sätt:

a) Online. TGP-tjänsten gör en uppslagning direkt i vårdsystemet vid förfrågan (online).
   Det ger möjlighet för respektive vårdgivare att själv realisera och ansvara för sin (eller sina) lokala TGP-tjänster med eget regelverk för vilka patienter som ska vara tillgängliga.

b) Uthopp kombinerat med Ineras TGP. I de fall där användaren startar NPÖ via sitt normala vårdsystem ska den aktuella patienten i normalfallet betraktas som tillgänglig. Vid användning av Ineras TGP-tjänst registreras patienten i TGP-tjänsten i samband med att NPÖ startas genom uthopp från vårdsystemet.
I de flesta fall sker detta genom användning av ett "uthoppsprogram" (Condis) på arbetsstationen, vilket förutom att registrera patienten i TGP-tjänsten och starta NPÖ även kontrollerar att uthoppet kommer från en godkänd applikation och hanterar en gemensam patientkontext så att NPÖ kan avslutas då en ny patient väljs i vårdsystemet.



Figur 1. Övergripande arkitekturvy över anrop av WS-tjänst för tillgänglig patient (TGP) via nationella tjänsteplattformen (TP).

Som redan antytts ovan utgörs TGP-tjänsten i själva verket av flera fysiska implementationer (TGP-instanser), med samma tjänstekontrakt, som samverkar och där respektive vårdgivare själv kan ansvara för sin (eller sina) lokala TGP-instanser som var och en hämtar informationen från ett eller flera lokala vårdsystem enligt **on-line**-metoden.

För de vårdgivare som i stället vill använda **uthoppsmetoden** utan en egen TGP-lösning finns två ”hotell-instanser”, kallade TGP0 (på Sjunet) resp. TGP1 (på Internet). Dessa tillhandahålls av Inera som nationella tjänster.

NPÖ behöver inte känna till vilken av dessa fysiska instanser som ska tillfrågas vid kontroll. Frågan ställs från NPÖ till komponenten TGPX[2] som gör det möjligt att seriellt vidarebefordra frågan till flera olika TGP-instanser: till TGP0, TGP1, samt eventuell online-TGP. Det räcker med att patienten är tillgänglig i någon av dessa för att anses som tillgängligt (dvs. logiskt ELLER). Anrop görs inte direkt från TGPX till respektive online-TGP-instans, utan via den Nationella tjänsteplattformen. Med ledning av den vårdgivare och vårdenhet som anges som indata i anropet avgör Nationella tjänsteplattformen vilken online-TGP-instans som ska tillfrågas och vidarebefordrar anropet till denna.

Kommentar 1:

Det som i dokumentet benämns NPÖ avser egentligen NPÖ:s webbtillämpning (och andra applikationer där sammanhållen vårddokumentation tillämpas). Det är NPÖ:s webbtillämpning, och inte NPÖ-tjänsten, som ansvarar för att kontrollen blir utförd. Vid användning av NPÖ:s frågetjänst sker val av patient i den anropande applikationer och det är där som ansvaret ligger för att kontrollen blir utförd.

4. Detaljerade beskrivningar

4.1 Allmänt

4.1.1 Regelverk för tillgängliga patienter

Enligt PDL är verksamhetschefen ansvarig för behörighetsstyrning inom den aktuella vårdenheten, vilket även innebär ansvar för regelverket som gäller begränsning av patientval. Det är alltså vårdgivaren, eller ytterst verksamhetschefen för vårdenheten, som beslutar vilket regelverk som ska gälla.

Längre tillbaka har nationella rekommendationer och riktlinjer diskuterats, men inget formellt beslut har tagits. Den gemensamma riktlinje som tidigare har diskuterats baserades på det regelverk som infördes i Örebro efter Datainspektionens tillsyn, och innebär i korthet:

Patienten ska betraktas som tillgänglig om något av följande villkor är uppfyllt

- Finns patienten registrerad inom specialistvården med en aktuell eller historisk kontakt (3 år bakåt).
- Finns patienten registrerad med en mottagen vårdbegäran inom specialistvården
- Finns patienten på mottagningslistan i primärvården (90 dagar framåt eller bakåt)

[2] TGPX driftsattes i mars 2014.

4.2 Uthoppslösningen (TGP0 och TGP1)

4.2.1 Kort om Condis (context and dispatch).

Condis är ett programpaket för att starta, stoppa och dela information mellan program genom enklast möjliga integrationsteknik. Start via Windows kommandorad med argument och stopp via Windows Close-kommando. Det är teknik som ofta finns tillgänglig utan att programmen som ska integreras behöver modifieras. Med hjälp av Condis är det möjligt att använda de mekanismer som redan finns i de flesta vårdsystem för att aktivera externa program, för att starta NPÖ och registrera aktuell patient i TGP0/TGP1.

4.2.2 Flödesbeskrivning vid uthoppslösning

Nedan följer ett exempel på ett typflöde (utan felfall) för användning av NPÖ via uthoppslösningen.

1. Användaren väljer en patient i sitt vårdsystem.
2. Användaren väljer att starta NPÖ genom en knapp i sitt vårdsystem.
3. Vårdsystemet gör uthopp med personnummer för aktuell patient och aktuell vårdgivare som argument till Condis.
4. Condis läser av vårdsystemets (eg. anropande systems) fingeravtryck (se nedan).
5. Condis anropar TGP0/TGP1 för registrering av patienten och bifogar fingeravtryck (krypterat).
6. TGP0/TGP1 kontrollerar att uthoppet är initierat av ett godkänt vårdsystem och registrerar patienten som tillgänglig inom angiven vårdgivare. Denna registrering är giltig under 120 sekunder.
7. Condis startar NPÖ med personnummer som argument.
8. NPÖ kontrollerar via TGP-tjänsten att det är en tillgänglig patient och visar patientdata.
9. Användaren jobbar med aktuell patient, både i sitt vårdsystem och i NPÖ.
10. Användaren väljer en annan patient i vårdsystemet.
11. Vårdsystemet meddelar Condis om patientbyte.
12. Condis avslutar pågående patientsession i NPÖ.
13. Klart.

4.2.3 Identifikation av vårdsystem vid uthopp

Bakgrund

Syftet med TGP-konceptet är att användaren inte ska kunna välja fritt bland alla de patienter som har en sammanhållen vårddokumentation, inte ens genom att olovligen intyga patientrelation och samtycke. Ett krav är därför att användaren inte själv ska kunna aktivera denna registrering med valfri patient. Däremot måste vårdsystemet kunna göra detta.

Problemet kompliceras av att registrering normalt inte kan ske direkt från vårdsystemet (vilket är tekniskt möjligt men kräver att de befintliga vårdsystemen modifieras). I stället sker det genom att vårdsystemet aktiverar det fristående programmet Condis med patientens personnummer och aktuell vårdenhet som argument. Det är därefter Condis som i sin tur gör registrering i TGP0/TGP1 och start av NPÖ.

Lösning
För att undvika att användaren kan göra samma aktivering som vårdsystemet tar Condis ett "fingeravtryck" på den process som aktiverat Condis. Detta fingeravtryck bifogas vid registreringen i TGP0/TGP1som kontrollerar att aktivering skett från ett godkänt vårdsystem.

Kommentar 1:

Det är *vårdsystemet* som ska identifieras med hjälp av fingeravtrycket. PKI-lösningar baserade på certifikat (som säkert kan identifiera både användaren som arbetsstationen) hjälper inte.

Kommentar 2:

För att ett vårdsystem ska godkännas för registrering i TGP0/TGP1 krävs att uthopp från vårdsystemet endast kan ske med en patient som ska vara tillgänglig i NPÖ. Det ska t.ex. inte vara tillåtet att göra ett uthopp med patienten som sökts i vårdsystemet, men där det saknas vårdinformation.

Kommentar 3:

Fingeravtryckets format är av naturliga skäl inte publikt. De vårdgivare som har för avsikt att modifiera vårdsystemet så att registrering sker direkt (dvs. inte via Condis) får i stället kontakta Inera.

4.2.4 Registrering i TGP0/TGP1 direkt av vårdsystemet

För att hantera registrering i TGP0/TGP1 och start av NPÖ direkt från vårdsystemet, utan Condis, krävs att vårdsystemet kan hantera följande:

- kryptering och formatering av fingeravtrycket
- kryptering och formatering av personnummer i NPÖ:s URL (för att det inte ska synas i klartext i webbläsarens historik).
- start av NPÖ
- avslut av rätt webbläsarfönster vid avslut eller byte av patient
- skydd av nycklar för kryptering

4.3 TGP online (lokal TGP)

Vid användning av online-lösning gör TGP-tjänsten en slagning direkt i vårdsystemet vid förfrågan från NPÖ (on-line). Denna lösning ger möjlighet för vårdgivaren att själv införa och ansvara för

lokala TGP-tjänster med eget regelverk för vilka patienter som ska vara tillgängliga. Detta gör också att NPÖ kan användas fristående, det vill säga utan att göra uthopp från vårdsystemet. Det är även möjligt att kombinera TGP online med ett egenbyggt uthopp från vårdsystemet till NPÖ. I det fallet krävs ingen TGP-registrering i någon av Ineras TGP-tjänster i samband med uthoppet.

För att kunna använda TGP online krävs att vårdgivaren har en tjänsteproducent som i realtid kan besvara TGP-frågorna från NPÖ och som är ansluten till Nationella tjänsteplattformen. För varje vårdenhet som ska använda NPÖ behöver sedan konfiguration ske i Nationella tjänsteplattformen så att TGP-anropen från NPÖ kan skickas till rätt lokal TGP-tjänst. TGP-tjänsten besvarar frågan från NPÖ med ett true eller false (beroende på om vårdrelation föreligger eller ej). Se mer information om konfiguration av Nationella tjänsteplattformen i avsnitt 4.4.1.

Tjänsteproducenten ska byggas i enighet med regelverken på RIV-TA (se [3]). Tjänstekontraktet som ska implementeras heter AssertCareEngagement.

För kommunikation mellan Nationella tjänsteplattformen och tjänsteproducenten krävs SITHS funktionscertifikat.

4.4 Nationella tjänsteplattformen

4.4.1 Konfigurering av Nationella tjänsteplattformen

Som tidigare beskrivits avgör Nationella tjänsteplattformen med ledning av den vårdgivare och vårdenhet som anges som indata i anropet vilken fysisk TGP-instans som ska tillfrågas och vidarebefordrar anropet till denna. Det innebär att Nationella tjänsteplattformen måste konfigureras för att kunna koppla ihop samtliga förekommande vårdenheter med rätt TGP-instans. Vårdgivaren/vårdenheten beställer konfigurationen i enlighet med den beskrivna processen för anslutning till NPÖ som konsument [4].

Förutom ovanstående konfigurering som berör vårdgivaren krävs även följande konfigurering av Nationella tjänsteplattformen:

Giltig anropare	Anrop till Nationella tjänsteplattformen sker via https med krav på klientautentisering med certifikat. Endast registrerade certifikat släpps fram. I NPÖ-fallet är NPÖ anropare.
Åtkomstkontroll	Anrop via Nationella tjänsteplattformen släpps bara fram till de bakomliggande instanser (tjänsteproducenter) som anroparen är behörig att komma åt. I NPÖ-fallet är NPÖ behörig att komma åt samtliga bakomliggande TGP-instanser.

4.5 TGPx

TGPx gör det möjligt att ställa samma fråga till flera olika TGP-instanser: Ineras TGP0 och TGP1, samt en ansluten online-TGP. Svaren från dessa vägs då samman så att det räcker med att patienten är tillgänglig i någon av dessa för att anses som tillgängligt (dvs. logiskt ELLER).

Frågan från TGPX ställs först till TGP0. Om patienten inte är tillgänglig i TGP0 (Sjunet) ställer TGPX samma fråga till TGP1 (Internet). Om patienten inte heller är tillgänglig i TGP1 ställer TGPX frågan till ansluten online-TGP via Nationella tjänsteplattformen.

5. Referenser

	Dokumentnamn/filnamn	Författare	Beskrivning
1	Condis.docx	Inera	Detaljbeskrivning av uthoppslösningens startprogram.
2	DI_beslut_Landsting_Örebro_Övrigt_100701.pdf	DI	Datainspektionens tillsynsrapport avseende Örebro landsting.
3	RIV TA: https://www.rivta.se		
4	Checklista: Tillgänglig patient (TGP) och Nationella tjänsteplattformen	Inera	Beskrivning av beställning av teknisk anslutning (konfiguration av Nationella tjänsteplattformen).