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

Funktionsbeskrivning

2012-08-22

Utgåvehistorik

Revision Nr	Revision Datum	Kort beskrivning av ändring	Ändringarna gjorda av	Granskad av
1.0	2011-05-11	Första version	Björn Strihagen, Inera	
1.1	2012-08-22	Lagt till beskrivning av TGP_Admin	Björn Strihagen, Inera	

1. Bakgrund

Datainspektionens har i samband med vid sin tillsyn av NPÖ i Örebro konstaterat att det vid åtkomst av sammanhållen journalföring är nödvändigt att kunna begränsa åtkomsten så att en användare bara ges tillgång till vissa patienter eller kategorier av patienter (och inte automatiskt till alla patienter som ingår i den sammanhållna journalen). (Se [5] sid 10).

Programledningen för NPÖ/BIF har därför, efter bl.a. samråd med anslutande parter och Datainspektionen, beslutat att principen för en sådan begränsning skall baseras på om den aktuella patienten är en "egen patient", vilket i normalfallet innebär att patienten redan är känd i något lokalt vårdsystem.

Denna begränsning skall gälla utöver kravet på att användaren skall intyga att patientrelation och samtycke finns, och utformas så att användaren inte själv, ens olovligen, kan passera.

Det kan noteras att datainspektionens krav på en begränsning av åtkomst gäller all sammanhållen journalföring och inte är specifikt för NPÖ, så även om huvudfokus för just detta dokument är att beskriva den lösning som tillämpas i NPÖ så är målet att såväl innehållet i dokumentet som själva lösningen skall vara applicerbar även i andra sammanhang där sammanhållen journalföring tillämpas.

2. Princip

Den grundläggande principen för begränsning av åtkomst bygger på att endast sådana patienter som behandlas, eller planeras att behandlas, inom den egna vårdenheten skall vara tillgängliga att välja i samband med åtkomst av den sammanhållna journalen. Information om detta kan i de flesta fall hämtas från något lokalt vårdsystem[1].

Kommentar 1:
Att patienten är tillgänglig är ett nödvändigt, men inte tillräckligt villkor för att användaren skall komma åt patientuppgifterna. Därtill måste användaren intyga att patientrelation föreligger samt att patientens har gett sitt samtycke till åtkomsten (alternativt att nödsituation föreligger).

Förutom detta måste användaren dessförinnan tilldelats erforderliga rättigheter att ta del av den sammanhållna journalen och autentiserat sig med sitt elektroniska id-kort (SITHS-kort). Därtill sker loggning och uppföljning av användarens åtgärder.

Kommentar 2:
Det är fullt möjligt att även det lokala vårdsystemet hanterar information från olika vårdgivare (och därmed definitionsmässigt tillämpar sammanhållen journalföring). Att patienten förekommer 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 skall vara tillgängliga i NPÖ även om den inte finns i det lokala vårdsystemet. Dessa fall är dock ovanligare än man vid förstone kan tro eftersom samtliga verksamheter (möjligen med något undantag, t.ex. 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 3:
Formellt är det verksamhetschefen som ansvarar för behörighetsstyrning och därmed avgör regelverket för vilka patienter som skall vara tillgängliga via NPÖ. Datainspektionen har inte uttryckt krav på *hur* detta regelverk ser ut, däremot att det finns ett regelverk och att det finns en teknisk möjlighet att realisera implementera det.

3. Övergripande lösning

NPÖ:s webbtillämpning (här kallad NPÖ, se Kommentar 1) har ansvar för att kontrollen av att patienten är tillgänglig blir utförd innan patientinformation visas för användaren. Däremot utför inte NPÖ kontrollen själv. Detta sker istället genom anrop av en generell webbservice-baserad tjänst; *TGP (tillgänglig patient*).

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

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

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

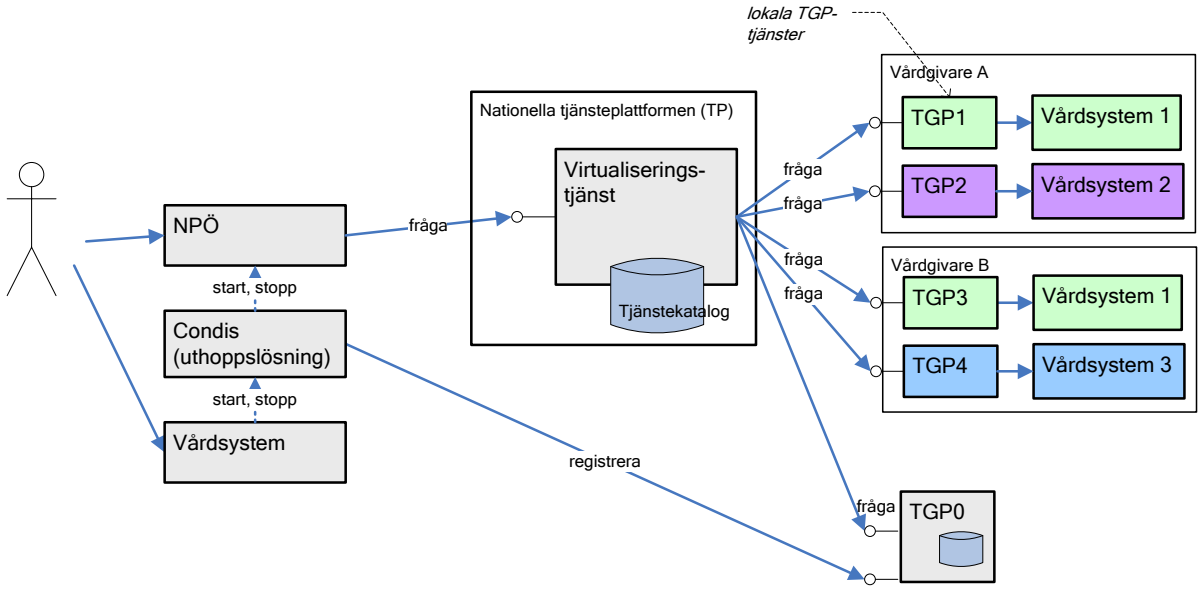
För att utföra kontrollen krävs att TGP-tjänsten har tillgång till information om vårdkontakter eller motsvarande för de patienter som finns i användarens lokala vårdsystem. Denna information kan TGP-tjänsten få tillgång till på flera olika sätt:

a) On-line. TGP-tjänsten gör en uppslagning direkt i vårdsystemet vid förfrågan (on-line). Detta ger möjlighet för respektive vårdgivare att själv realisera och ansvara för sin (eller sina) lokala TGP-tjänster med eget regelverk för vilka patienter som skall anses vara tillgängliga.

b) Off-line. TGP-tjänsten importerar en lista med tillgängliga patienter.
Tanken är att listan skapas genom regelbunden export från ett lokalt vårdsystem, men i undantagsfall kan listan även skapas manuellt.
Metoden lämpar sig bäst för verksamheter där det inte är kritiskt med den tidsfördröjning för nya patienter som orsakas av exportförfarandet. Idag tillämpas metoden t.ex. för äldreboende inom kommunerna.

c) Uthopp. I de fall där användaren startar NPÖ via sitt normala vårdsystem ska den aktuella patienten i normalfallet betraktas som tillgänglig. Det gäller bara att få även TGP-tjänsten att känna till detta vilket sker genom att patienten registreras i den gemensamma TGP-tjänsten (TGP0/TGP1) i samband med att NPÖ startas.
Rent praktiskt sker det genom användning av ett "uthoppsprogram" (Condis) på arbetsstationen som 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.

d) TGP-Admin. Via ett speciellt webb-progam (TGP-Admin) administreras tillgängliga patienter manuellt, dvs. kopplingen mellan en patient och en viss vårdenhet.
Denna lösning finns i dagsläget (2012-08) endast för vårdgivare på Internet och är avsedd främst för mindre vårdgivare såsom kommuner.
TGP-Admin är kopplad till samma TGP-instans som används för uthopp (dvs TGP1 för Internet) vilket innebär att kontroll sker mot TGP1.



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 istället vill använda **off-line-**, **uthopp**smetoden eller **TGP-Admin** finns två ”hotell-instanser”, kallade TGP0 (på Sjunet) resp. TGP1 (på Internet). Dessa tillhandahålls av Inera som nationella tjänster.

Men hur vet då NPÖ vilken fysisk instans som skall tillfrågas vid kontroll? Jo, detta sker genom att anropet inte görs direkt från NPÖ till respektive TGP-instans utan via den Nationella tjänsteplattformen (TP). Med ledning av den vårdgivare och vårdenhet som anges som indata i anropet avgör TP vilken TGP-instans som skall tillfrågas och vidarebefordrar anropet till denna.

Det är också möjligt att vidarebefordra samma fråga till flera olika TGP-instanser. Isåfall vägs svaren från dessa samman av tjänsteplattformen så att det räcker med att patienten anses tillgänglig i någon av dessa för att anses som tillgängligt (dvs. logiskt ELLER).

Kommentar 1:
Det som här benämns NPÖ avser egentligen NPÖ:s webbtillämpning (och andra applikationer där sammanhållen journalföring tillämpas). Det förtjänar dock att förtydligas att 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 följaktligen där som ansvarar ligger för att kontrollen blir utförd.

4. Detaljerade beskrivningar

4.5. Allmänt

4.5.1. Regelverk för tillgängliga patienter

Enligt PDL är verksamhetschefen som ansvarar för behörighetsstyrning inom den aktuella vårdenheten vilket även innebär ansvar för regelverket som avser begränsning av patientval.

Men även om det formella ansvaret ligger på verksamhetschefen så har en gemensam (nationell) rekommendation efterfrågats mot bakgrund av det är önskvärt att alla parter har ungefär samma regelverk för att därigenom skapa ett ömsesidigt förtroende.

Den gemensamma riktlinje som diskuterats (något formellt beslut är det ju inte fråga om) baseras på det regelverk som tillämpas i Örebro och innebär i korthet:

Patienten skall 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)

4.6. Uthoppslösningen

4.6.1. 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. Detta är teknik som ofta finns tillgänglig utan att programmen som ska integreras behöver modifieras.
Även om Condis är utvecklat med fokus på att stödja uthoppslösningen så kräver detta en rad grundläggande funktioner av mer generell karaktär som gör att Condis lämpar sig väl för användning även i många andra sammanhang där program på samma arbetsstation behöver startas, stoppas och utbyta små mängder information i realtid.

Med hjälp av Condis är det möjligt att använda de mekanismer som redan finns i de flesta vårdsystem för att aktivera externa program till att även starta NPÖ och registrera aktuell patient i TGP0/TGP1.

Condis beskrivs detaljerat i [1].

4.6.2. 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 pnr 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 1 minut.
7. Condis startar NPÖ med pnr som argument (format se [8]).
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.

4.6.3. 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 journal, 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 alltjämt vårdsystemet kunna göra just detta.

Problemet kompliceras av att registrering normalt inte kan ske direkt från vårdsystemet (vilket är tekniskt möjligt men kräver att de befintliga vårdsystemen modifieras). Istället sker det genom att vårdsystemet aktiverar det fristående programmet Condis med patientens pnr 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 kan noteras att det är *vårdsystemet* som ska identifieras mha fingeravtrycket. PKI-lösningar baserade på certifikat (som säkert kan identifiera såväl användaren som arbetsstationen) hjälper följaktligen inte.

Kommentar 2:
För att ett vårdsystem ska kunna godkännas för registrering i TGP0/TGP1krävs att uthopp från vårdsystemet endast kan ske med en patient som skall vara tillgänglig i NPÖ. Det ska

t.ex. inte vara tillåtet att göra ett uthopp med en patienten som sökts i vårdsystemet men där det saknas vårdinformation (då är vi ju tillbaks där vi började).

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 istället kontakta Inera.

4.6.4. Registrering i TGP0/TGP1direkt av vårdsystemet

Det är svårt, men inte omöjligt, att hantera registrering i TGP0/TGP1och start av NPÖ direkt från vårdsystemet (utan Condis).

Detta kräver att vårdsystemet hanterar följande:

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

4.7. Off-line lösning

Off-line lösningen kräver att filer med information om tillgängliga patienter överförs till TGP0/TGP-instansen. För själva filöverföringen används PLUSFTP. Nedan ges därför en kortfattad beskrivning av PLUSFTP samt av det filformat och regelverk som används i samband med TGP.
Se [4] för en mer fullständig beskrivning av PLUSFTP.

4.7.1. Kort om PLUSFTP

PLUSFTP är ett generellt programpaket för säker överföring av filer inom svensk hälso- och sjukvård. I likhet med andra programvaror för filöverföring (såsom FTP, SFTP) så är dess grundläggande funktion att flytta filer mellan två maskiner via ett nätverk, en lokal maskin (PLUSFTP-klient) och en fjärrmaskin (PLUSFTP-server).

Till skillnad från andra FTP-programvaror utnyttjar PLUSFTP den infrastruktur som finns inom svensk hälso- och sjukvård i form av HSA och SITHS för t.ex. autentisering och behörighetshantering. PLUSFTP är dessutom utformat för att följa arkitekturledningens anvisningar vilket bl.a. innebär att alla överföring mellan vårdgivare skall ske mha webb-service, vara krypterad och kräva säkerställd autentisering med certifikat samt att möjlighet skall finnas att erhålla digitalt signerat kvitto på genomförd överföring.

Överföring av TGP-filer sker mellan en ***arbetskatalog*** hos den sändande parten (hos vårdgivaren) och en ***virtuell katalog*** (på TGP-servern). Den virtuella katalogen är knuten till användarens vårdgivare (dvs. den vårdgivare som finns i medarbetaruppdraget).

Modellen kan liknas vid ***tårtbitar*** där olika användare från samma vårdgivare (inom samma tårtbit) kan se varandras filer, medan användare från olika vårdgivare inte har möjlighet att se varandras filer.

Det finns tre olika sorters program för att tillgodose något olika behov hos den sändande parten.

a) ***PLUSFTP_WIN*** - En fönsterbaserad applikation där användaren manuellt kan överföra och ta bort filer.

b) ***PLUSFTP_CMD*** - Ett kommandoradsbaserat program avsett att aktiveras tidsstyrt eller via scriptfiler.

c) ***PLUSFTP_SVC*** - Ett bakgrundsprogram (i form av en Windows service) som kontinuerligt övervakar den lokala arbetskatalogen och överför alla filer som läggs där och därefter flyttar filerna till arkivkatalogen.

All användning kräver att användaren (manuell eller maskinell) **autentiseras**. För manuella användare av *PLUSFTP_WIN* innebär det att de loggar med sitt SITHS-kort, och får sina rättigheter via sitt medarbetaruppdrag (som definieras i HSA). För maskinella användare av *PLUSFTP_CMD* och *PLUSFTP_SVC* innebär det att ett tjänstecertifikat på den lokala maskinen används.

4.7.2. Filformat för TGP-filer

- TGP-filerna är på formatet tab-separerad text.

- Varje fil har en header-rad med följande rubriker (tab-separerade):
  subjectOfCareId, careGiverHsaIdentity, careUnitHsaIdentity, performer.
  Dessa fält har exakt samma namn och betydelse som anges i gränssnittsdokumentationen för tjänsten [2].

- Följande fält kan anges: *startDate, endDate, revoked, reg_user* och *reg_time.*
  Dessa är dock för framtida bruk och är inte obligatoriska.

- Varje rad i filen skall ha lika många kolumner. Dessa ska vara separerade med en tab även om innehållet är tomt. (Fel antal kolumner ger varning varvid giltiga kolumner beaktas och saknade betraktas som tomma. Det är alltså "tillåtet" att ignorera tomma kolumner i slutet av raden)

- Filändelsen skall vara *.tgp*

Kommentar 1:
Filerna kan enkelt redigeras manuellt med t.ex. Excel (spara som text). Ett tips är dock att använda något redigeringsverktyg speciellt utvecklad för tab-separerad text, t.ex. Killink CSV Editor, (http://www.whitepeaksoftware.com/main/killink-csv-editor) .

Exempel

(som word-tabell för läsbarhet)

subjectOfCareId	careGiverHsaIdentity	careUnitHsaIdentity	performer
191212121212	*	*	*
192411219047	Proj-NPO_VG1-0001	Proj-NPO_VG1-0003	*
199303092390	Proj-NPO_VG1-0001		*

4.7.3. Regelverk

Vid tolkning av filens innehåll tillämpas följande regelverk i TGP0/TGP1

1. Varje rad i tabellen definierar ett villkor. Om minst en rad matchar en inkommande förfrågan returneras sant, dvs. den patient som förfrågan avser betraktas som tillgänglig.

2. För att matcha en förfrågan skall fälten *subjectOfCareId, careGiverHsaIdentity, careUnitHsaIdentity, performer* i förfrågan samtliga överensstämma med de på raden.

3. Fälten överensstämmer om de antingen är lika (vid textjämförelse) eller om fältet i tgp-filen är * (stjärna) eller är tomt.
   Undantag: Fältet `subjectOfCareId` får inte vara tomt i TGP-filen.

4. Ogiltiga rader ignoreras (dvs. övriga rader i samma fil beaktas)

5. Samtliga filer med ändelsen .tgp läses in.
   Det innebär att flera olika filer från samma vårdgivare kan samexistera. T.ex. en fil från varje vårdenhet.

Kommentar 1:
TGP0/TGP1 indexerar TGP-filerna på pnr. Det innebär att svarstiden för tjänsten är relativt oberoende av antalet rader i TGP-filerna (som typiskt kan innehålla flera tusen rader).

4.8. Nationella tjänsteplattformen (TP)

4.8.1. Konfigurering av Nationella tjänsteplattformen (TP)

Som tidigare beskrivits avgör TP med ledning av den vårdgivare och vårdenhet som anges som indata i anropet vilken (eller vilka) fysisk TGP-instanser som skall tillfrågas och vidarebefordrar anropet till dessa. Det innebär att TP måste konfigureras för att kunna koppla ihop samtliga förekommande vårdenheter med rätt TGP-instans.

Denna konfiguration sker på två nivåer
1) På vårdgivarnivå anges en grundkonfiguration som gäller för samtliga vårdenheter inom hela vårdgivaren om inget annat sägs (s.k. *default vårdgivare*).
2) På vårdenhetsnivå för att ange undantag från ovanstående grundkonfiguration.

Det är vårdgivaren eller vårdenheten själva som beslutar om konfigurationen och anmäler detta till tjänsteplattformförvaltningen i enlighet med den beskrivna processen för TGP-tjänsten [6, 7].

Förutom ovanstående konfigurering som berör vårdgivaren krävs även följande konfigurering av TP:

Giltig anropare	Anrop till TP sker via https med krav på klientautentisering med certifikat. Endast registrerade certifikat släpps fram. I NPÖ-fallet är NPÖ anropare.
Åtkomstkontroll	Anrop via TP 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

(Nedanstående är planerat men ej driftsatt i TP 2011-05-10)
Vid konfigurationen (på båda nivåerna) kan mer än en TGP-instans anges. En inkommande fråga kommer då att vidarebefordras till samtliga dessa och svaren vägas samman så att det räcker med att patienten är tillgänglig i någon av dessa för att vara tillgängligt (dvs. logiskt ELLER).
Syftet med detta förfarande är att möjliggöra utveckling av i form av återanvändbara TGP-komponenter för varje specifik vårdsystemtyp som kan användas av flera vårdgivare (dvs. koden är återanvändbar men var och en driftar sin egen instans). De vårdgivare som har flera olika vårdsystem (t.ex. PAS och reimss) som samtliga ska tillfrågas vid varje fråga använder då helt enkelt en TGP-instans för var och en av dessa.

5. Möjlig framtida utveckling

5.5. Arkitektur

Arkitekturledningen (AL-T) har beskrivit en arkitektur för en nationell tjänst för *Engagemangsindex* – en slags kombination av TGP och patientrelation. Den häri beskrivna TGP-tjänsten skulle vid en framtida utveckling enligt AL:s förslag ingå som en del av ett sådant Engagemangsindex.

5.6. TGP som en del av ÅKT

En möjligt framtida utveckling är att TGP kopplas till åtkomstkontrollen (ÅKT) i de nationella säkerhetstjänsterna (antingen direkt eller indirekt via ovan beskrivna engagemangsindex) på motsvarande sätt som görs med patientrelation och samtycke idag. Därmed skulle de enskilda vårdapplikationerna inte behöva anropa TGP-tjänsten direkt utan detta skulle ske i samband med anrop av ÅKT.

5.7. NPÖ som TGP-instans

För de vårdgivare som redan idag laddar upp information om vårdkontakter till NPÖ kan det synas som att gå över ån efter vatten att dessutom sätta upp en TGP-instans som beräknar sitt svar på exakt den information som redan laddats upp till NPÖ.

En möjlig utveckling är därför att antingen
a) bygga in en TGP-kontroll i NPÖ-tjänsten som baseras på den information som NPÖ redan har eller
b) tillhandahålla en nationell TGP-instans baserad på information via NPÖ:s frågetjänst.

Det skall dock noteras att dagens TGP-tjänst har som syfte att vara användbar för fler än NPÖ vilket talar emot a) samt att NPÖ:s frågetjänst hanterar mycket mer data än enbart det som är nödvändigt för TGP och därför lämpar sig dåligt ur prestandaperspektiv TGP vilket talar emot b).

5.8. Manuell registrering

Det kan finnas skäl manuellt kunna registrera en patient som tillgänglig.

Exempel på detta är då:
a) NPÖ skall fungera som reservsystem för det lokala vårdsystemet och antingen den lokala TGP-instansen är kopplad till samma lokala vårdsystem eller TGP-registrering sker i samband med uthopp från det lokala vårdsystemet.

b) Den lokala TGP-instansen endast kan komma åt information ur vårdsystemet med viss fördröjning eller då off-line metoden används (varvid inskrivna patienter inte blir tillgängliga omedelbart).

c) För teständamål

Det är tekniskt sätt relativt enkelt att tillhandahålla en lösning för manuell registrering av tillgängliga patienter baserad på samma teknik som vid uthoppslösningen. Svårigheten är

istället att hitta en lösningen som inte användaren själv, inte ens olovligen, kan passera. Då är vi ju tillbaks där vi började.

Några olika lösningförslag som diskuterats är

- En centralt aktiverad nöd-funktion som under en begränsad tid gör alla patienter tillgängliga för all personal inom hela vårdenheten (enligt fall a ovan).
- Dubbelkommando (det krävs två användare för att registrera en patient som tillgänglig).
- Registrering kan endast ske av personer som inte själva ha behörighet att använda NPÖ (s.k. *separation of duties*).

6. Referenser

	dokumentnamn/filnamn	förf.	beskrivning
1	Condis.docx	Inera	Detaljbeskrivning av uthoppslösningens startprogram.
2	Tjänstekontrakt TGP v1.0.doc	Inera	Textuell detaljbeskrivning av TGP-tjänsten
3	ServiceContracts_ehr_accesscontrol_beta_r275.zip	Inera	Tekniska specifikationer (wsdl- och xsd-filer) för TGP-tjänsten.
4	PLUSFTP.docx	Speedsoft	PLUSFTP
5	DI_beslut_Landsting_Örebro_Övrigt_100701.pdf	DI	Datainspektionens tillsynsrapport avseende Örebro landsting.
6	Process för TGP-jänst.doc	Inera	
7	Anmälan om publicering av TGP (mall).doc	Inera	
8	Gränssnittsspecifikation_NPÖ_ver_1.3.0.docx	Tieto	