



Ökad tillgänglighet till patientuppgifter

Datainspektionens rapport 2005:1

Innehållsförteckning

| | |
|--|-----------|
| 1. Inledning | 2 |
| 2. Sammanfattning | 4 |
| 3. Allmänt | 6 |
| 4. Regler för tillgång till patientuppgifter | 6 |
| 4.1. Avgränsning | 6 |
| 4.2. Vårdregisterlagen | 6 |
| 5. Datainspektionens iakttagelser och synpunkter | 8 |
| 5.1. Utvecklingstendenser | 8 |
| <i>Sjukhusvården är ännu inte datoriserad</i> | 8 |
| <i>Allt större myndigheter</i> | 8 |
| <i>Nationella projekt</i> | 8 |
| 5.2. Sjukvårdspersonalens tillgång till patientinformation | 9 |
| <i>Datainspektionens iakttagelser</i> | 9 |
| <i>Några risker för patienters integritet vid öppna behörighetslösningar</i> | 11 |
| 5.3. Patienters egen åtkomst till journalinformation | 11 |
| 5.4. Hantering av recept – läkemedel | 12 |
| 5.5. Principer för samtycke | 13 |
| 5.6. Hantering av skyddade personuppgifter | 14 |
| 5.7. Hantering av patientuppgifter i olika IT-system | 16 |
| 5.8. IT-säkerhet | 17 |
| <i>Allmänt</i> | 17 |
| <i>Logguppföljning</i> | 18 |
| <i>Säker identifiering</i> | 19 |
| <i>Trådlösa nät</i> | 19 |
| 6. Avslutande synpunkter | 21 |

Bilaga

1. Inledning

Många av de uppgifter som hanteras inom sjukvården är bland de mest integritetskänsliga som finns om människor. Det kan röra sig om psykiatriska diagnoser, uppgifter om sociala problem, genetiska sjukdomsanlag, sexualvanor, familjerelationer, psykoterapeutisk behandling, missbruksproblem och genomgångna aborter. De nuvarande bestämmelserna i bland annat vårdregisterlagen har tillkommit i syfte att begränsa tillgången till denna känsliga information. I den allmänna diskussionen ställs ofta skyddet för den personliga integriteten mot patientsäkerheten, som om det råder ett motsatsförhållande däremellan. Enligt Datainspektionens uppfattning är integritetsskyddet en del av patientsäkerheten. Om inte enskilda och vårdpersonal har förtroende för hur informationen hanteras inom sjukvården kan det utgöra ett hot mot patientsäkerheten.

Datainspektionen har under 2004 och 2005 genomfört ett tillsynsprojekt och granskat personuppgiftsbehandling som utförs inom sjukvården. I uppdraget för projektet har ingått att kartlägga hur flödet av personuppgifter ser ut inom sjukvården och hur journaluppgifter lämnas ut mellan olika enheter inom sjukhus och mellan olika vårdinrättningar. Av särskilt intresse har varit hur långt eventuellt arbete med att införa sammanhållna journaler¹ har kommit. Säkerheten för personuppgifterna har kontrollerats, särskilt när uppgifterna behandlats i trådlösa nät. Granskningen har inriktats på sjukhus.

Datainspektionen har inspekterat sju landsting och en landstingsfri kommun under perioden mars till oktober 2004. Dessutom har inspektionen deltagit i nätverksmöten och haft kontakter med representanter för Carelink som är en intresseförening för landsting, regioner, kommuner och enskilda vårdföretag.

Inspektionerna är avslutade och de berörda landstingen har fått Datainspektionens beslut i inspektionsärendena.

IT-utvecklingen i vården går snabbt och omfattar många aktörer. Nya utvecklingsprojekt påbörjas ständigt. För en liten myndighet som Datainspektionen är det problematiskt att bevaka utvecklingen i alla delar och ha insyn i allt som pågår. Datainspektionen väljer därför att här redovisa några generella synpunkter på det som har framkommit i samband med tillsynen och uppmärksamma de särskilda integritetsrisker som inspektionen har noterat. Avsikten med denna rapport är att den dels ska tjäna som vägledning för de överväganden som måste göras i samband med att nya IT-system utvecklas inom vården och dels utgöra ett diskussionsunderlag. Datainspektionens synpunkter har markerats med grått i texten.

¹ Se avsnitt 3

De iakttagelser som Datainspektionen redogör för i denna rapport hänför sig i huvudsak till förhållanden 2004. Det innebär att enskilda landsting kan ha genomfört förändringar som inte finns redovisade här.

Stockholm i september 2005

2. Sammanfattning

Det har varit svårt att få något samlat grepp om hur flödet av personuppgifter ser ut inom vården eftersom sjukvårdshuvudmännen har valt sinsemellan olika lösningar. Enhetlighet saknas både när det gäller tekniken och synen på hur tillgängliga patienternas uppgifter ska vara. Sjukhusens journaler förs i stor utsträckning fortfarande på papper. En tydlig utvecklingstendens är dock att patientuppgifter, i takt med att elektroniska journaler införs, blir tillgängliga för allt fler användare över allt större geografiska områden.

Projekt som syftar till att göra patientuppgifter mer tillgängliga pågår på såväl regional som nationell nivå. Medel har till exempel delats ut för att utveckla en *nationell patientjournal*. Det pågår redan nu försöksverksamhet med en *nationell patientöversikt*. Samtidigt är de legala frågorna under översyn.

IT-systemen öppnas för allt fler användare men fortfarande saknas i stor utsträckning fungerande rutiner för att kontrollera att inte obehöriga tar del av uppgifterna. Vanligt är att landstingen förväntar sig att det ska finnas bättre rutiner på sikt. I praktiken innebär det att landstingen har liten eller ingen kontroll över vilka som bereder sig tillgång till information om enskilda patienter.

I vissa landsting framgår att man har gjort en analys av informationsflödet i organisationen för att därefter låta enheter med regelbundet samarbete få tillgång till varandras information. I andra landsting har inte framgått vilka eventuella överväganden som har gjorts när det gäller principer för tillgång till patientuppgifter. Vid en öppen behörighetstilldelning uppkommer ofta önskemål om att hålla viss information som bedöms vara särskilt känslig utanför det som alla har tillgång till. En svårighet är att bestämma vilken information som i så fall ska vara tillgänglig för alla och vilken information som är alltför känslig. Synen på vilken information som ska ”spärras” på detta sätt varierar såväl inom som mellan landstingen. Det finns landsting som anser att all sjukvårdsinformation ska behandlas på samma sätt och att ingen information ska spärras medan andra landsting väljer att begränsa åtkomsten till viss information.

Sammanfattningsvis bör följande gälla.

Utgångspunkten är att patientuppgifter inte ska göras tillgängliga i större utsträckning än nödvändigt.

En analys måste göras av vilka behov av information som finns i verksamheten. Det bör vara möjligt att variera tillgängligheten med hänsyn till vilket informationsbehov en viss befattningshavare har. Tillgängligheten kan bestämmas med utgångspunkt från exempelvis organisatorisk tillhörighet, medicinsk specialitet och etablerat samarbete. Enheter som har ett regelbundet samarbete på grund av att de ingår i samma vårdkedja bör normalt kunna få tillgång till varandras information under förutsättning att sekretessfrågorna är lösta. Det måste även finnas effektiva verktyg för uppföljning och spårbarhet. En säker identifiering av användare krävs.

Det bör finnas tekniska ”trösklar” som innebär att användaren måste göra aktiva val för att komma åt uppgifter om en viss patient.

Möjlighet till så kallad nödöppning i en akut situation kan finnas. Visar det sig att nödöppning ofta måste tillgripas kan principerna för åtkomst behöva ändras.

Verktyg för att hantera patienternas önskemål bör finnas.

Det måste finnas effektiva rutiner för att hantera sekretessmarkerade personuppgifter så att risken för att sådana uppgifter lämnas ut till fel personer minimeras.

Landstingen behöver skärpa sina rutiner för uppföljning och kontroll av loggar. Särskilt vid en öppen behörighetstilldelning krävs en regelbunden och systematisk uppföljning av loggar. För att kunna genomföra meningsfulla analyser behöver landstingen ha tekniska verktyg.

Landstingen måste ha bättre kontroll över både installationen och driften av trådlösa nät. Det bör finnas en särskild policy för trådlösa nät.

3. Allmänt

Det är vanligt att sjukvårdens patienter har kontakt med flera olika vårdgivare. Journalinformation om samma patient kan finnas lagrad på många ställen, något som sägs leda till bristande kontinuitet, dubbelarbete och risker för patientsäkerheten. Företrädare för sjukvården talar därför om behovet av en *sammanhållen patientjournal*. Någon entydig definition av begreppet finns inte. Vad en sammanhållen patientjournal innebär i praktiken, hur den ska vara utformad, vilken information som ska ingå och vilka som ska ha tillgång till informationen, är oklart. Som kommer att framgå av rapporten har sjukvårdshuvudmännen hittills valt sinsemellan olika lösningar. En sammanhållen patientjournal *kan* innebära att information som är knuten till en viss patient noteras i en patientjournal som är gemensam för flera vårdenheter. Begreppet kan också betyda att flera vårdenheter har tillgång till varandras journaler.

Gemensamt journalsystem innebär i denna rapport att alla vårdgivare inom ett sjukhus eller ett landsting använder samma journalsystem. Uppgifterna kan göras tillgängliga för alla anställda. Det är dock möjligt att begränsa åtkomsten till uppgifterna.

Öppen behörighetstilldelning innebär att personalen får tillgång till all eller i stort sett all information som finns i det aktuella journalsystemet, oavsett om det i verksamheten finns ett behov av uppgifterna eller inte.

4. Regler för tillgång till patientuppgifter

4.1. Avgränsning

Skyddet för patientuppgifter regleras i flera lagar. Datainspektionens tillsynsansvar när det gäller sjukvården begränsas till vårdregisterlagen och personuppgiftslagen. Den praktiska tillämpningen av bestämmelserna om sekretess och tystnadsplikt har givetvis också stor betydelse för skyddet av den personliga integriteten. Dessa frågor faller dock utanför Datainspektionens tillsynsområde.

4.2. Vårdregisterlagen

Enligt 8 § lagen (1998:544) om vårdregister (vårdregisterlagen) ska bara den som behöver tillgång till uppgifterna för att kunna utföra sitt arbete ha direktåtkomst till uppgifter i ett vårdregister. Åtkomsten får endast avse de uppgifter som behövs för att utföra arbetet. Bestämmelsen har införts i syfte att erinra om vad som brukar kallas den inre sekretessen i patientjournallagen (1985:565). Enligt 7 § patientjournallagen ska varje journalhandling hanteras och förvaras så, att obehöriga inte får tillgång till den. Bestämmelserna syftar till att skydda

patienten mot obehörig insyn i privatlivet. Det är bara en begränsad del av personalen som i sitt arbete behöver och ska ha tillgång till journalen (jfr prop. 1997/98:108).

Avgörande för hur vidsträckt behörighet en viss anställd ska ha är *behovet* av uppgifter. Den personuppgiftsansvarige måste därför ordna tilldelningen av behörigheter på ett sådant sätt att sjukvårdsanställda inte får tillgång till mer uppgifter än vad som behövs för att de ska kunna utföra sitt arbete. Det krävs att varje landsting analyserar och *aktivt* tar ställning till vilken information som är nödvändig för en viss tjänst och tilldelar användaren behörighet till landstingets vårdregister härefter. Den som arbetar i ett landsting ska inte medges obegränsad tillgång till alla patientuppgifter som behandlas inom myndighetsgränsen, om det inte är nödvändigt för att utföra arbetet. En konsekvens av det sagda blir att det landsting som avser att införa nya behörighetsrutiner först måste fastställa vilka informationsbehov som finns.

Datainspektionen anser att landstingen bör ha klara gemensamma riktlinjer så att journaluppgifter hanteras på ett enhetligt sätt. Det finns annars risk för att tillgängligheten till uppgifterna kan variera beroende av var i landet en person söker vård.

Det är inte möjligt för Datainspektionen att ha någon uppfattning om vilka uppgifter en viss befattningshavare inom vården behöver ha tillgång till för att kunna utföra sitt arbete. Det är inte heller möjligt för inspektionen att ange en viss ”skälig nivå” för tillgången till patientinformation. Den bedömningen måste göras i respektive verksamhet. Samtliga läkare och sjuksköterskor i ett landsting bör normalt inte få läsbehörighet till all sjukvårdsinformation från samtliga enheter inom landstinget. Det finns inget hinder mot att informationen lagras i samma IT-system, under förutsättning att åtkomsten till uppgifterna begränsas på ett sätt som motsvaras av behovet och att gällande sekretessbestämmelser kan iakttas. Tillgången till uppgifterna måste begränsas och styras av behörighetssystem. Vid utformningen av ett behörighetssystem måste man kunna variera tillgängligheten med hänsyn till vilket informationsbehov en viss befattningshavare har. Det är givetvis svårt att i förväg avgöra behovet av uppgifter. Fullständig precision är inte möjlig. Tillgången bör dock kunna bestämmas med utgångspunkt från exempelvis organisatorisk tillhörighet, medicinsk specialitet och etablerat samarbete. Om landstingen bedömer att en vidsträckt behörighet krävs för en viss tjänst bör man samtidigt ha tekniska ”trösklar” som innebär att användaren tvingas att göra aktiva val för att komma åt uppgifter om en viss patient. Sådana tekniska ”trösklar” kombinerat med fungerande loggningsrutiner bör ha en preventiv effekt. Möjlighet till så kallad nödöppning i en akut situation kan finnas. Om det visar sig att nödöppning ofta måste tillgripas kan principerna för åtkomst behöva revideras.

5. Datainspektionens iakttagelser och synpunkter

5. 1. Utvecklingstendenser

Sjukhusvården är ännu inte datoriserad

I de landsting som Datainspektionen inspekterade var arbetet med att införa elektroniska patientjournaler inte särskilt långt framskridet. På flertalet sjukhus användes fortfarande till övervägande del pappersjournaler. Datoriserade patientjournaler fanns på ett fåtal avdelningar. Många sjukhus var dock på väg eller hade planer på att införa datoriserade journalsystem i större skala. Det fanns en mängd olika system inom respektive landsting som inte kunde kommunicera med varandra. Labbsvar, remisser och liknande överfördes dock ofta digitalt. När det gäller sammanhållna journaler var det vanligt att beslut om inriktning hade fattats samtidigt som det praktiska genomförandet inte hade kommit så långt. Det var främst inom förlossnings- och mödravården som ett slags sammanhållna journaler redan fanns. I praktiken innebar det att förlossnings- och mödravårdspersonalen hade tillgång till varandras journaler. Inom primärvården hade datoriseringen däremot kommit mycket långt och i flera landsting förekom där ett omfattande utbyte av information.

Takten har ökat när det gäller införandet av trådlösa nät. Hittills har trådlösa nät mest förekommit inom kvinnosjukvården.

Allt större myndigheter

Det är vanligt att landstingen fattar beslut om att landstinget ska ses som ett enda, eller ett fåtal större verksamhetsområden. Landstingen omorganiserar sig till allt större myndigheter i syfte att bland annat underlätta informationsflödet. Utvecklingen går således mot allt större sekretessområden. Flera landsting anser numera att information kan utbytas mellan olika enheter inom landstingen utan föregående sekretessprövning.

Nationella projekt

Det initieras och pågår en mängd olika utvecklingsprojekt när det gäller IT i vården. Här ges några exempel.

Alla landstingsdirektörer har beslutat att ställa sig bakom ett arbete med en nationell samverkande patientöversikt. Ett pilotprojekt kommer att genomföras under 2005 då man ska testa en webbaserad *nationell patientöversikt* i liten skala. Landstingen i Uppsala län, Östergötland, Norrbotten och Jönköping ska ingå och kunna utbyta information med varandra. Projektet Nationell patientöversikt drivs av Carelink.

Regeringen har i början av året tillsatt en arbetsgrupp för att utarbeta en nationell policy för IT inom sjukvården. Arbetsgruppen ska bland annat ta fram riktlinjer för en nationell IT-policy och för kompatibla² system inom vården. Med kompatibla system blir det lättare att utbyta information.

I Dagmaröverenskommelsen för 2005 har regeringen och huvudmännen för sjukvården pekat på IT-områdets betydelse för att utveckla vård och omsorg och på behovet av nationellt koordinerade satsningar på området. Parterna har bland annat enats om att särskilt prioritera utvecklingen av en nationell patientjournal. Medel har delats ut för dessa ändamål.

5.2. Sjukvårdspersonalens tillgång till patientinformation

Datainspektionens iakttagelser

Samtliga landsting uppgav att de uppfyllde kraven i 8 § vårdregisterlagen genom sina rutiner för behörighetstilldelning. Rutinerna för behörighetstilldelning varierade dock över landet. I praktiken hade inte sjukvårdspersonalen tillgång till all journalinformation om varje patient. Eftersom de olika IT-systemen inte kunde kommunicera med varandra var det inte tekniskt möjligt. Synen på hur tillgänglig informationen om patienterna skulle vara varierade dessutom mellan landstingen. Landstingen hade följaktligen valt sinsemellan olika lösningar.

Några exempel:

- I ett fall hade landstingets ledning gjort flera principuttalanden om att alla läkare och sjuksköterskor inom landstinget skulle ha läsbehörighet till all journalinformation om alla patienter i hela landstinget. Det skulle finnas en patientjournal för varje patient som var gemensam för hela landstinget. Huvudprincipen var att all information skulle vara öppen för alla användare (sjuksköterskor och läkare) inom myndighetsgränsen. Största möjliga öppenhet skulle råda. Regler för när det var tillåtet att ta del av journaluppgifter skulle finnas.
- I andra landsting fastställdes behörighet efter vilken typ av tjänst en person hade och var personen var verksam. En analys gjordes även av hur patientinformationen kunde tänkas förflytta sig i ”vårdkedjan”. Enheter som hade ett regelbundet samarbete på grund av att de ingick i samma vårdkedja fick därefter tillgång till varandras information.

² Det vill säga IT-system som kan kommunicera med varandra.

- Det förekom sjukhus där personalen bara hade åtkomst till uppgifter om de patienter som var aktuella vid den egna enheten och där man uppgav att det inte finns några planer på att utvidga behörigheterna.
- I några landsting använde man sig av för flera enheter gemensamma patientöversikter eller portaler där viss basinformation om patienten fanns samlad. Det kunde röra sig om uppgifter om överkänslighet, förskrivna läkemedel och liknande men inte fullständig journalinformation. I vissa landsting avsåg man dock att på sikt låta all journalinformation ingå i översikten. Slutresultatet kan således komma att variera när det gäller hur mycket information en översikt innehåller.
- Ett stort sjukhus hade ett för sjukhuset gemensamt journalsystem som all sjukvårdspersonal hade läsbehörighet till. Där hölls viss information som lokalt bedömdes vara särskilt känslig utanför det gemensamma systemet. Det kunde röra sig om uppgifter från psykiatrin eller om sexuellt överförda sjukdomar.

I praktiken skiljde sig de olika tekniska systemen åt när det gäller hur pass lätt det var att få åtkomst till patientinformation. I vissa fall var systemen mycket sofistikerade med flera spärrar att passera. Den vårdpersonal som ville ha tillgång till uppgifter om en viss patient var tvungen att göra en rad aktiva val innan uppgifterna blev tillgängliga. I andra fall kom användaren rakt in i en annan vårdgivares journalsystem. Det förekom att gamla behörigheter inte rensades ut. Särskilda svårigheter var förknippade med behörigheten för inhyrda läkare.

Landstingen har tidigare ofta beslutat om behörigheter för tillgång till patientinformation med utgångspunkt från var en anställd är verksam. Nu tilldelas många användare en mer vidsträckt behörighet och får på eget ansvar hålla sig till regelverket.

I vissa av de granskade landstingen hade landstingets ledning gjort generella uttalanden om hur tillgängliga patientuppgifterna skulle vara. Det framgick inte alltid av de beslutsunderlag som fanns tillgängliga, om landstingsledningen grundade sina beslut på en analys av de faktiska behoven när det gäller tillgänglighet för patientuppgifter. Det framgick inte heller i vilken utsträckning företrädare för verksamheten deltog i utvecklingsarbetet. Det förekom att vissa enheter valde att inte följa centrala beslut och inte medge åtkomst till den egna informationen medan andra motsvarande enheter i andra delar av landstinget hade ett annat förhållningssätt. Det gällde framförallt psykiatriska kliniker. Konsekvensen blev att den som fick psykiatrisk vård i en länsdel kunde räkna med att journalinformationen blev åtkomlig över hela landstinget medan

motsvarande information bara blev tillgänglig för den egna enheten i en annan länsdel.

Datainspektionen anser att det är otillfredsställande från integritetssynpunkt att patientuppgifter hanteras så pass olika över landet och till och med inom samma landsting.

Några risker för patienters integritet vid öppna behörighetslösningar

När elektroniska patientjournaler införs och systemen blir kompatibla kan stora mängder känslig patientinformation göras tillgänglig för allt större grupper av sjukvårdsanställda.

Om man väljer öppna behörighetslösningar med bred åtkomst finns risken att känslig patientinformation sprids till en avsevärt större krets än den som har behov av uppgifterna. Risken för obehörigt läsande blir då större. Med en alltför vidsträckt behörighetstilldelning blir det svårt att kontrollera åtkomsten. De rutiner för kontroll som finns idag är enligt Datainspektionens erfarenhet otillräckliga ³.

En annan risk med alltför öppna system är att journalförare avhåller sig från att skriva fullständiga journalanteckningar på grund av att uppgifterna kan läsas av många. Det finns även risk för att patienter avstår från att söka vård av samma skäl. Sådana synpunkter har framförts från patienter och sjukvårdspersonal i anslutning till Datainspektionens tillsyn.

Riskerna ökar för att uppgifter om patienter med sekretessmarkerade personuppgifter kommer i orätta händer, särskilt om uppgiften om var en viss patient har sina sjukvårdskontakter (och därmed är bosatt) skulle bli tillgänglig över hela landet. Det gäller i synnerhet när någon har tvingats flytta och har bosatt sig på en annan ort. Redan idag finns brister i skyddet för dessa utsatta personer. Se vidare nedan.

5.3. Patienters egen åtkomst till journalinformation

Datainspektionen har i ett tillsynsärende⁴ vid sidan av projektet konstaterat att det inte är förenligt med bestämmelserna i vårdregisterlagen att ge enskilda patienter direktåtkomst till uppgifter i vårdregister via Internet. Länsrätten i

³ Se s. 18

⁴ Dnr 1569-2003 Landstinget i Uppsala län, Sustains Sjukvårdskonto

Stockholms län⁵ avslag det aktuella landstingets överklagande av Datainspektionens tillsynsbeslut. Länsrätten fann bland annat att det inte var tillåtet att ge enskilda patienter direktåtkomst till uppgifter som rör dem själva i vårdregister.

Av de landsting som Datainspektionen granskade inom ramen för detta projekt var det endast ett som erbjöd patienter direktåtkomst till sin egen sjukvårdsinformation via Internet. Intresset för att erbjuda patienter sådan direktåtkomst var inte särskilt stort hos övriga granskade landsting, något som endast till viss del uppgavs ha ett samband med Datainspektionens tidigare tillsynsbeslut mot Landstinget i Uppsala län. Däremot var det vanligt att patienterna kunde förnya recept och avboka tider via Internet.

Datainspektionen har inga invändningar mot att patienter får information om innehållet i den egna journalen. En stor del av den lagstiftning som finns på sjukvårdsområdet innehåller bestämmelser om patientens rätt till insyn och medinflytande. För närvarande finns dock ingen laglig möjlighet att ge patienter tillgång till sin egen journalinformation genom direktåtkomst, till exempel via Internet. Det krävs således först en lagändring. I ett sådant lagstiftningsarbete behöver särskilda överväganden göras. Hänsyn bör tas till de särskilda risker – exempelvis från säkerhetssynpunkt – som kan vara förknippade med att uppgifterna görs tillgängliga via Internet. Frågan har uppmärksammats av regeringen och Patientdatautredningen (S 2003:03) har fått i uppdrag att se över möjligheten att införa en sådan rätt till direktåtkomst för patienten, med beaktande av möjligheten att utnyttja informationsteknikens fördelar samt möjligheten att utföra nödvändig sekretessprövning (Dir. 2004:95).

5.4. Hantering av recept – läkemedel

E-recept förekom i alla granskade landsting. E-recept innebär att förskrivaren skickar receptet elektroniskt till en e-receptbrevlåda där apotekspersonalen hämtar upp det. Receptet skickas antingen till ett utvalt apotek eller till central receptbrevlåda som inte är bunden till något speciellt apotek. Patienten kan i det senare fallet hämta ut sin medicin var som helst i landet.

E-recept överfördes till övervägande del genom Sjunet som är en nationell infrastruktur för vård och omsorg och förvaltas av Carelink. Sjunet är skyddat genom kryptering i motsats till vad som oftast gäller för landstingens interna nätverk.

⁵ Mål nr 20776-03

I flera landsting använde man sig av *läkemedelslistor* där alla patientens läkemedelsordinationer fanns samlade i en gemensam förteckning.

I enlighet med vad som gäller för alla uppgifter i vårdregister är det bara den som behöver uppgifterna för att kunna utföra sitt arbete som får ha direktåtkomst till dem. Åtkomsten ska begränsas till de uppgifter som behövs för att arbetet ska kunna utföras. Läkemedelslistorna kan innehålla information av mycket ömtåligt slag. Datainspektionen ifrågasätter inte att *förskrivaren*¹ kan behöva ha tillgång till uppgift om vilka andra läkemedel en patient har ordinerats, bland annat för att undvika att olika läkemedel påverkar varandras effekt på ett sätt som inte är önskvärt. Det bör dock observeras att det kan finnas sekretessbestämmelser som begränsar möjligheten att lämna ut uppgifter till eller få tillgång till gemensamma läkemedelslistor.

Den 1 juli trädde den nya lagen (2005:258) om läkemedelsförteckning i kraft. Apoteket AB får nu registrera samtliga de köp av receptförskrivna läkemedel som en patient gör på apotek. Förskrivare kan få tillgång till uppgifterna i förteckningen efter *uttryckligt samtycke* från den registrerade.

5.5. Principer för samtycke

Landstingen hade ingen enhetlig praxis för i vilka situationer patientens samtycke skulle hämtas in om en vårdgivare ville ta del av uppgifter från andra enheter. Vissa landsting hade en omfattande samtyckeshantering. I andra landsting ansåg man att samtycke inte krävdes eftersom det var fråga om vårdregister och uppgifterna dessutom hanterades inom samma myndighet. Praxis varierade också när det gäller patientens möjligheter att påverka uppgifternas tillgänglighet. Det fanns landsting, där patienter tidigare hade kunnat ha visst inflytande över vilka enheter som skulle ha tillgång till informationen, som hade tagit bort den möjligheten. I andra landsting kunde viss information ”spärras” på begäran av patienten.

Den hantering av personuppgifter som är tillåten enligt vårdregisterlagen förutsätter inte patientens samtycke. Personuppgifter får enligt vårdregisterlagen behandlas för dokumentation av vården av patienter, administration som syftar till att bereda vård i enskilda fall och ekonomiadministration som föransleder av vård i enskilda fall. Det är även tillåtet att behandla uppgifter från ett vårdregister för exempelvis statistik, uppföljning och kvalitetssäkring på verksamhetsområdet. När det gäller åtkomsten till personuppgifterna utgår vårdregisterlagen från behovet av uppgifterna. Det ska finnas en vårdrelation *och* uppgifterna ska behövas för arbetets utförande. Det är inte möjligt att kringgå vårdregisterlagens bestämmelser med stöd av patientens samtycke.

Samtycke kan däremot behövas för att bryta *sekretessen* i de fall uppgifterna ska passera en myndighetsgräns. Det är inte Datainspektionens uppgift att pröva dessa sekretessfrågor. Enligt bestämmelser i hälso- och sjukvårdslagen (1982:763), som också faller utanför inspektionens tillsyn, ska vården särskilt bygga på respekt för patientens självbestämmande och integritet (2 a § 3). Justitieombudsmannen har i ett äldre beslut (JO 1986/87 s. 198 ff.) uttalat att det följer av hälso- och sjukvårdslagen att patientens uttryckliga önskemål, om att inte andra vårdenheter ska ta del av journalen, ska respekteras. När journalen är tillgänglig för alla som arbetar inom en viss myndighetsgräns – som kanske består av ett helt landsting – är det svårt att kunna tillgodose sådana önskemål från patienter. Utrymmet för individuellt hänsynstagande blir begränsat.

Om ett landsting ska låta patienten påverka tillgängligheten till den egna informationen är det nödvändigt att noggrant överväga vad ett eventuellt samtycke från patienten innebär så att detta står klart för alla involverade. Det är viktigt att patienterna inte vilseleds när det gäller i vilken utsträckning de kan hindra informationsutbyte. Ett giltigt samtycke förutsätter att de personer som lämnar sina samtycken verkligen har ett fritt val och inte befinner sig i beroendeställning. Personerna bör även kunna överblicka eventuella konsekvenser av ett lämnat eller avstått samtycke. Landstingen bör ha klara rutiner för att hantera patienternas önskemål *innan* journaluppgifter eventuellt görs tillgängliga för stora grupper av sjukvårdspersonal.

Datainspektionen anser att det finns behov av enhetliga principer och rutiner på nationell nivå. Det är olyckligt att patienternas möjligheter att påverka tillgången till journalinformation skiljer sig över landet.

I uppdraget för patientdatautredningen (Dir. 2004:95) anges att utgångspunkten ska vara att den enskilde ska lämna ett uttryckligt och informerat samtycke till utbyte av information om honom eller henne. Om undantag från denna huvudregel föreslås ska fördelar och nackdelar med ett sådant förslag noggrant belysas. Patientdatautredningen kommer således förmodligen att överväga frågor om samtycke.

5.6. Hantering av skyddade personuppgifter

Skatteverket använder begreppet ”skyddade personuppgifter” som samlingsbegrepp för de olika skyddsåtgärderna sekretessmarkering, kvarskrivning och fingerade personuppgifter. *Sekretessmarkering*, som är den vanligaste skyddsåtgärden, innebär att skattekontoret sätter en markering för särskild sekretessprövning för personen i folkbokföringsdatabasen. En sekretessmarkering kan bli aktuell om skattekontoret bedömer att det kan leda till personföljelse eller annan skada om uppgifter om personen lämnas ut. Det kan exempelvis

röra sig om kvinnor som förföljs av sina före detta män eller personer som hotas på grund av att de tidigare har ställt upp som vittnen i rättegång. Markeringen ska fungera som en varningssignal så att en noggrann prövning görs innan uppgifterna lämnas ut. *Kvarskrivning* innebär att personen får vara folkbokförd på den gamla folkbokföringsadressen. *Fingerade personuppgifter* används vid särskilt allvarliga hot och innebär att personen får använda en helt annan identitet. Uppgifterna registreras på ett sådant sätt att det inte framgår att det rör sig om fingerade personuppgifter. Det är bara ett fåtal personer som använder fingerade personuppgifter. Skatteverket lämnar ut uppgifterna ur folkbokföringsdatabasen till andra myndigheter. Sekretessmarkeringen följer med men de mottagande myndigheterna avgör själva hur de ska hantera uppgifterna.

Datainspektionen har inte gjort någon djupgående granskning av hanteringen av sekretessmarkerade personuppgifter inom sjukvården. Eftersom frågan är av stor vikt anser inspektionen att det ändå finns skäl för att redogöra för vad som framkommit.

De inspekterade landstingen hade egna befolkningsregister med uppgifter som hade hämtats från Skatteverket. Vissa landsting fick inte adressen till personer med sekretessmarkering när uppgifterna hämtades från Skatteverket. Andra fick den fullständiga adressen. Datainspektionen fann exempel på att man använde sig av grupplösenord för åtkomst till befolkningsregistret.

Rutinerna för att hantera patienters skyddade personuppgifter varierade. Även om interna regler fanns förekom det att personalen inte kände till dem. I vårdregistren registrerades vanligtvis namn och personnummer till de personer som hade sekretessmarkerade personuppgifter. Det var således möjligt att se att en namngiven person hade bokat tid på en viss mottagning en viss dag. Det förekom att anställda ansåg att de kunde lämna ut den uppgiften. Vissa landsting valde att hantera uppgifter om personer med sekretessmarkering manuellt.

Landstingens hantering av stora befolkningsregister innebär risker om de innehåller den korrekta adressen till personer med sekretessmarkering. Det är inte godtagbart att använda grupplösenord för inloggning till befolkningsregistret om sådana adresser finns registrerade där.

Enligt Datainspektionens uppfattning är det oroväckande att det finns brister i hanteringen av sekretessmarkerade uppgifter. Det får överhuvudtaget inte förekomma att sådana uppgifter lämnas ut till obehöriga. En vårdbehövande ska inte behöva vara orolig för att sjukvården kan komma att avslöja var personen finns. Landstingen måste ha tydliga rutiner för hur sekretessmarkerade personuppgifter ska hanteras. De rutiner som finns måste vara kända i verksamheten så att *all* personal som kan tänkas komma i kontakt med uppgifterna vet hur de ska hanteras. Landstingen bör överväga om det finns alternativ till nuvarande ordning som innebär att korrekt namn och personnummer finns registrerade i vårdregistren. En komplikation är att patienter måste kunna identifieras på ett säkert sätt.

Sjukvårdshuvudmännen måste ta hänsyn till hanteringen av sekretessmarkerade uppgifter när nya IT-system ska utvecklas. Skatteverkets vägledning för hantering av sekretessmarkerade uppgifter i offentlig förvaltning finns tillgänglig på Skatteverkets webbplats och kan användas av landstingen.

5.7. Hantering av patientuppgifter i olika IT-system

Känsliga patientuppgifter hanteras i många olika IT-system inom sjukvården; inte bara i patientjournalen. Diagnoser kan finnas registrerade i patientadministrativa system eller i olika kvalitetsregister. Ett område som hittills inte har varit föremål för någon närmare granskning är den rapportering som krävs internt för exempelvis ekonomisk uppföljning.

För integritetsskyddet är det givetvis av vikt att uppgifterna har ett likvärdigt skydd överallt och att det finns lagstöd för hanteringen. Fler uppgifter än nödvändigt får inte registreras. Kravet på att det ska föreligga ett behov av uppgifterna för arbetets utförande gäller även för åtkomsten till patientadministrativa system.

5.8. IT-säkerhet

Allmänt

Inom sjukvården hanteras stora mängder integritetskänslig information vilket medför särskilda krav på det tekniska skyddet för uppgifterna. En svårighet är att de registerlagar som finns, exempelvis vårdregisterlagen, inte innehåller bestämmelser om IT-säkerhet. I förarbetena görs generella uttalanden där det förutsätts att den tekniska säkerheten är tillräcklig. Det kan vara svårt för de personer som arbetar med IT-säkerhet inom sjukvården att utan stöd av ett tydligt regelverk ställa krav på och få gehör för kostsamma säkerhetslösningar.

När särskilda säkerhetsbestämmelser saknas i registerlagarna tillämpas istället personuppgiftslagen. Enligt 31 § personuppgiftslagen ska den personuppgiftsansvarige vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna ska åstadkomma en säkerhetsnivå som är lämplig med beaktande av de tekniska möjligheter som finns, vad det skulle kosta att genomföra åtgärderna, de särskilda risker som finns med behandlingen av personuppgifterna och hur pass känsliga de behandlade personuppgifterna är. Bestämmelsen ger uttryck för en avvägning mellan uppgifternas känslighet, de särskilda risker som finns, vad som är tekniskt möjligt och kostnaderna.

Eftersom ömtålig personlig information hanteras inom sjukvården måste säkerhetsnivån vara hög. Även den medicinska säkerheten är beroende av att IT-stödet fungerar. I takt med att antalet IT-system med personuppgifter ökar och öppnas för allt större grupper blir det lättare för obehöriga (det vill säga personer som inte behöver uppgifterna för sitt arbete) att ta del av patientuppgifter. Ska man införa system som kan göras tillgängliga för i stort sett alla anställda inom sjukvården måste man ställa mycket höga krav på IT-säkerheten. Generellt kan sägas gälla att en vid behörighetstilldelning ställer högre krav på kontrollfunktioner som logganalys och uppföljning. Säkerhetskraven ökar således om vid behörighetstilldelning tillämpas. Landstingen måste redan i samband med upphandlingen ställa krav på de system som levereras så att de legala och säkerhetsmässiga kraven kan uppfyllas.

Det är möjligt att författningsreglera IT-säkerheten. I USA finns ett omfattande regelverk, Health Insurance Portability and Accountability Act (HIPAA), som har till syfte bland annat att skydda patienternas personliga integritet. HIPAA innehåller regler för hantering av data inom hälso- och sjukvården och långtgående konkreta säkerhetsbestämmelser.

Det pågår även arbete med att ta fram en standard för informationssäkerhet som anpassats till sjukvårdssektorn. Standarden heter ISO 27799. Landstingen använder sig ännu inte av någon standard.

Logguppföljning

I samtliga landsting loggades åtkomsten till personuppgifter. Skriftliga rutiner för *regelbunden* uppföljning av loggarna fanns bara i tre landsting. Ansvar för logguppföljningen vilade där på verksamhetscheferna. Det var dock oklart i vilken omfattning kontroller faktiskt utfördes. I två landsting uppgavs att det på sikt skulle finnas bättre verktyg för uppföljning. I tre landsting kontrollerades loggarna bara vid misstanke om oegentligheter, det vill säga vid misstanke om att någon obehörig hade tagit del av patientuppgifter. I ett landsting saknades helt rutiner för uppföljning.

Landstingen kan inte nöja sig med att delegera ansvaret till verksamhetscheferna utan måste i egenskap av personuppgiftsansvariga se till att kontroller faktiskt utförs. Det är den personuppgiftsansvarige som ansvarar för att kontroller utförs på ett sådant sätt att de är meningsfulla.

Det räcker inte att genomföra riktade kontroller vid misstanke om överträdelse. För att loggkontrollen ska ha en preventiv effekt krävs dessutom en regelbunden och systematisk uppföljning av loggar. Loggar resulterar i enorma mängder data som är svåra att dra några slutsatser av. En systematisk granskning kräver att det finns tekniska verktyg för genomförandet. Det behövs system där det är möjligt att både analysera enskilda användares beteenden och hur personalen bereder sig tillgång till enskilda patienters uppgifter. Om systemet skapar listor över misstänkta beteenden kan den personal som ansvarar för logguppföljningen slutligen göra en bedömning av vilka som har haft rätt att ta del av patientuppgifter. Sådana verktyg går att ta fram. Det är sjukvårdshuvudmännen som måste ställa krav på sina leverantörer att ta fram användbara verktyg. Loggning ska göras av vem som har berett sig tillgång till vårdinformation, vilken information som personen har haft tillgång till, vad som har gjorts och när det har gjorts. För att loggning och uppföljning ska ha en preventiv effekt måste personalen informeras om att loggar kontrolleras.

Det förekom att landstingen lämnade med logglistor i samband med att patienter begärde och fick registerutdrag. I vissa landsting fanns uttalade planer på att patienten själv skulle kunna kontrollera vilka personalkategorier som fått tillgång till hans eller hennes uppgifter.

Bestämmelsen i 26 § personuppgiftslagen om registerutdrag innebär inte att patienten har rätt att få logglistorna utlämnade. Däremot kan ett utlämnande eventuellt vara möjligt med stöd av Tryckfrihetsförordningen (efter sekretessprövning). Den prövningen faller dock utanför Datainspektionens ansvarsområde.

Datainspektionen vill i detta sammanhang understryka att patientens eventuella egenkontroll inte på något sätt kan frånta landstingen ansvaret för att ha verksamma interna rutiner för kontroll.

Om sjukvårdshuvudmännen använder sig av en vidsträckt behörighetstilldelning är, såsom tidigare nämnts, kraven högre på att det finns kontrollfunktioner som logganalys och uppföljning. Det är inte acceptabelt att bygga upp öppna system utan att i praktiken ha någon kontroll över åtkomsten till känslig patientinformation. Landstingen behöver skärpa kontrollen avsevärt.

Säker identifiering

När sjukvårdens journalsystem kan göras tillgängliga för allt fler användare är det inte godtagbart från säkerhetssynpunkt att använda vanliga lösenord vid inloggning. Det är nödvändigt att på sikt gå över till engångslösenord, aktiva behörighetskort, smarta kort eller andra metoder. Det är visserligen förenat med kostnader men det är inte acceptabelt att bygga upp stora kompatibla IT-system för hantering av patientuppgifter utan att samtidigt ha en säker identifiering av användare. En svårighet är att landstingen sinsemellan har olika lösningar. Möjligen kan de samarbetsorgan som finns, exempelvis Carelink, bidra till större enhetlighet. Om landstingen har gemensamma kravspecifikationer blir det lättare att få gehör för kraven.

Trådlösa nät

Med hjälp av bärbara datorer och trådlösa nät (WLAN) kan vårdpersonal komma åt vårdregister från andra platser än där det finns fasta terminaler. Det är möjligt att registrera uppgifter direkt vid patientens säng. Kommunikationen i det trådlösa nätet sker via basstationer som monteras i byggnaden. Basstationerna är ett slags antenner som utgör så kallade accesspunkter, där det trådlösa nätet kommunicerar med det fasta. I den bärbara datorn finns ett radiolankort som möjliggör kommunikation med basstationen via radiosignaler.

Trådlösa nät förekom på de flesta av de inspekterade sjukhusen men oftast på ett fåtal avdelningar. Takten hade dock ökat när det gäller införandet sedan Datainspektionen senast genomförde en bredare granskning av sjukvården⁶. I samband med ombyggnad var det vanligt att sjukhusen förberedde för och installerade trådlösa nät. Det var även vanligt att trådlösa nät hade installerats men ännu inte tagits i drift. Det förekom att de personer som hade varit med och installerat de trådlösa näten hade slutat och att kvarvarande personal saknade kunskaper om hur de skulle hanteras. Landstingen uppgav att informationen i de trådlösa näten krypterades. Vid inspektionerna framkom dock att man använde svag kryptering och ibland glömde att slå på krypteringen. Det fanns även exempel på att trådlösa hade installerats utan att IT-avdelningen medverkat.

Eftersom det är lätt att avlyssna trådlösa nät behöver landstingen vidta särskilda skyddsåtgärder för att skydda personuppgifterna. Datainspektionens rapport 2003:4 Personuppgifter i vårdregister innehåller en uppräknade av sådana skyddsåtgärder⁷. Förutom de åtgärder som finns uppräknade i den tidigare rapporten kan följande åtgärder vara befogade.

- Det är lämpligt att slå av broadcast/utsändning av SSID
- En förteckning över tillåtna MAC-adresser kan finnas i accesspunkterna

Om IT-avdelningen inte medverkar vid installationen kan det vara svårt för informationssäkerhetsorganisationen att hitta de trådlösa näten. Det bör därför finnas en policy för trådlösa nät som reglerar hur införandet ska gå till.

⁶ Se Personuppgifter i vårdregister Datainspektionens rapport 2003:4

⁷ Sidan 9

6. Avslutande synpunkter

Datainspektionen anser att det är otillfredsställande att patientuppgifter hanteras olika beroende på var i landet en person söker vård. Det är önskvärt att sjukvårdshuvudmännen enas om ett gemensamt förhållningssätt. Regeringens initiativ till arbetsgrupper som bland annat har till uppgift att verka för nationellt koordinerade satsningar på IT-området inom hälso- och sjukvården är därför lovvärt. I Dagmaröverenskommelsen har medel avsatts för Carelinks arbete med att ta fram gemensamma kravspecifikationer på nationell nivå, bland annat när det gäller säkerheten. Datainspektionen välkomnar även detta arbete. Förhoppningsvis ges dataskydds- och integritetsaspekterna utrymme i det arbetet.

Datainspektionen har självfallet inga invändningar mot att den personal som behandlar en viss patient ska ha tillgång till all den information som behövs för att patienten ska få adekvat vård. Datainspektionen är inte heller motståndare till användning av IT i vården. Det finns fördelar – även från integritetsynpunkt – med datoriserade journaler. Med hjälp av IT är det möjligt att begränsa tillgången till patientuppgifter och att kontrollera vilka som tar del av uppgifterna. De integritetsrisker som uppkommer när uppgifterna kan göras tillgängliga för stora grupper av anställda som kanske aldrig kommer att ha behov av uppgifterna får dock inte negligeras. Eventuella integritetsfördelar är således beroende av hur sjukvårdshuvudmännen löser behörighetsfrågor, kontroller och liknande. Patientuppgifter kan hanteras i gemensamma system under förutsättning att uppgifterna hålls åtskilda och hanteras på ett sådant sätt att sekretesslagens och vårdregisterlagens bestämmelser kan iakttas.

Oavsett om man avser att göra patientinformation åtkomlig på regional eller nationell nivå finns en rad överväganden som måste göras. Exempel på frågor som behöver besvaras är hur stort behovet är av att göra uppgifter tillgängliga och vilka uppgifter som i så fall behöver finnas med. Det är också nödvändigt att ta ställning till vilka personalkategorier som ska ha tillgång till uppgifterna. Ska alla sjukvårdsanställda i hela landet ha tillgång till information om alla patienter? Vilket inflytande ska patienterna kunna ha på informationsflödet? Måste framtidens patienter acceptera att deras uppgifter kan läsas av all sjukvårdspersonal över hela landet? Hur ska man garantera att sekretessmarkerade personuppgifter hanteras på ett säkert sätt?

Datainspektionen anser att det kan ifrågasättas om all information måste finnas tillgänglig *på förhand* för *potentiella* vårdgivare. Istället för fullständig journalinformation borde det enligt inspektionens uppfattning vara tillräckligt med någon form av översikt där viktig basinformation – exempelvis överkänslighet och medicinering – samlas, eventuellt tillsammans med uppgift om var ytterligare information finns. Redan en uppgift om var en patient är aktuell kan vara mycket känslig. Behovet av information varierar beroende på vilken yrkesroll

en anställd har och var personen är verksam. En kirurg vid en ortopedakut saknar förmodligen användning för journalanteckningar från landstingets psykoterapienhet. Däremot finns annan information som är viktig att ha tillgång till i en akut situation.

Enligt Datainspektionens uppfattning bör landstingen i första hand satsa på att utveckla system som är kompatibla så att det är möjligt att snabbt överföra information vid behov snarare än att öppna systemen och låta all information bli tillgänglig i förväg. Idag saknas verksamma kontrollrutiner.

När man använder sig av myndighetsövergripande lösningar är det nödvändigt att inblandade parter har klart för sig hur personuppgiftsansvaret är fördelat. Av intresse, men utanför Datainspektionens ansvarsområde, är också om det är möjligt att förena sådana lösningar med gällande sekretesslagstiftning. Den frågan kommer dock att behandlas inom ramen för patientdatautredningen.

Det framförs ofta argument om att de flesta patienter förväntar sig att doktorn ska ha tillgång all information om dem i datorn. Viss information betraktas av många som förhållandevis harmlös. Det gäller dock inte alla patientgrupper och inte heller all information. Det finns patienter som av olika skäl inte vill att deras uppgifter ska vara allmänt tillgängliga. Psykiatrins patienter brukar nämnas som en grupp som typiskt sett inte vill att deras journalinformation sprids till en större krets. Det finns andra exempel och självklart individuella variationer. Enligt Datainspektionens uppfattning måste även sådana synpunkter beaktas.

Det bör också finnas utrymme för att respektera patientens rätt till självbestämmande. En komplikation är att många av de IT-lösningar som finns i sjukvården idag har utformats på ett sådant sätt att det inte är möjligt att begränsa åtkomsten. Hänsyn har inte tagits till exempelvis vårdregisterlagens krav.

Datainspektionen inser värdet av att effektivisera och minska administrationen. Patientens rätt till privatliv är dock av central betydelse och det är viktigt att denna rätt respekteras även när de tekniska möjligheterna att sprida informationen ökar. Det måste därför finnas tekniska och administrativa verktyg för att så långt som möjligt förhindra obehörig åtkomst till patientuppgifter. Enligt Datainspektionens uppfattning är det inte acceptabelt att öppna IT-systemen och hoppas att alla användare självmant håller sig till regelverket. Kontrollfunktioner måste finnas med redan när IT-lösningar utvecklas.

Bilaga

Inspekterade landsting

Landstinget i Östergötland
Universitetssjukhuset i Linköping

Stockholms läns landsting
Södersjukhuset AB

Landstinget Kronoberg
Centrallasarettet Växjö

Landstinget i Jönköpings län
Länssjukhuset Ryhov Jönköping

Landstinget Västernorrland
Sollefteå sjukhus
Skärnsta vårdcentral

Västerbottens läns landsting
Norrlands universitetssjukhus
Lycksele lasarett

Kalmar läns landsting
Stensö vårdcentral
Länssjukhuset i Kalmar

Gotlands kommun
Vårdcentralen Korpen
Visby lasarett



Datainspektionen

Postadress: Box 8114, 104 20 Stockholm

Besöksadress: Fleminggatan 14, plan 9

Beställningar: 08-657 61 42 (telefonsvarare)

E-post: datainspektionen@datainspektionen.se

Telefon: 08-657 61 00 Fax: 08-652 86 52

Webbplats: www.datainspektionen.se

Pris: 50 kr + moms

Accessibility to patients' data

Report 2005:1 Summary in English

During 2004 and 2005 the Data Inspection Board carried out a project in order to investigate the processing of personal data within the medical service. One of the aims of the project was to look closer at the flow of personal data within the medical service and how case book data is shared between different divisions of the hospitals and between different care providers. It was of particular interest to look at how far the potential work with introducing coherent case books had got. The protection of personal data was checked, especially when the data was processed in wireless networks. The focus of the investigation was on hospitals.

During the period March-October, 2004, the Data Inspection Board investigated seven county councils and one municipality without a county council. In addition, the Board participated in network meetings and was in contact with representatives of Carelink, which is an interest association for county councils, regions, municipalities and individual care providers.

Developments within information technology in the medical service are accelerating and comprise many operators. New developing projects are constantly initiated. For a small authority like the Data Inspection Board it is difficult to oversee developments within all parts and be versed in everything that is going on. Therefore, the Data Inspection Board here presents some general points of view on what has appeared regarding supervision and pays special attention to the specific integrity risks that have been observed by the Board. The purpose of this report is partly to provide guidance when it comes to the considerations that have to be taken when new IT-systems are developed within the medical service and partly to constitute a basis for discussion.

It has been difficult to grasp the flow of personal data within the medical service since the county councils have chosen different solutions between themselves. Uniformity is lacking when it comes to the technology as well as the views on how accessible the patients' data should be. The case books of the hospitals are to a great extent still being kept on paper. However, a clear development tendency is that the patient's data gets accessible for more and more users over larger geographical areas as electronic case books are introduced.

Projects that aim at making patients' data more accessible are ongoing, on a regional as well as national level. For example, means have been distributed in order to develop a *national case book*. Experimental work with a *national patient survey* is already ongoing. At the same time the legal issues are under inspection.

The IT-systems are accessible to more and more users. However, working routines to check that unauthorized users do not get access to the data are still lacking to a great extent. The county councils usually expect that the routines will be improved on the long term. In practice this means that the county councils have very little, or no control, of who has got access to information about individual patients.

In certain county councils it is evident that an analysis of the flow of information in the organization has been done. After that, divisions that regularly co-operate are allowed access to one another's information. In other county councils it did not appear what considerations, if any, that had been made regarding principles concerning access to patients' data. With a permitting basis for access control, wishes to separate certain sensitive information from that

to which everyone has access often arise. The difficulty then is to decide which information should be accessible to everybody and which kind of information is too sensitive. The views on which kind of information that should be “blocked” in this way varies within as well as between the county councils. There are county councils that are of the opinion that all information regarding medical care should be processed in the same way and that no information should be blocked, while other county councils choose to limit the access to certain information.

As a summary, the following should be applied:

The guideline is that the patients’ data should not be made accessible to a greater extent than necessary.

An analysis has to be done regarding the need of information within the organization. It should be possible to vary the accessibility in regard to the need of information a certain official may have. The accessibility can be decided with the basis of for example position, medical speciality and established co-operation. Divisions that regularly co-operate because they belong to the same organization normally should be able to get access to one another’s information, assuming that the secrecy issues have been solved. There must also be efficient tools for follow-up and traceability. The identification of the user must comply with security restrictions.

There should be technical “thresholds”, which means that the user must make active choices in order to reach data about a certain patient.

There may be a possibility of a so-called emergency opening in emergency cases. If it appears that an emergency opening has to be used often, it may be necessary to change the principles regarding accessibility.

There should be tools to handle the requests of the patients.

There must be routines to handle secrecy marked personal data so that the risk of sharing such data with an unauthorized person is minimized.

The county councils need to improve their routines regarding follow-ups and check-ups of log files. A regular and systematic follow-up of log files is particularly important at a permitting basis for access control. In order to carry through meaningful analyses the county councils need to have technical tools.

The county councils need to have better control of the installation as well as the management of wireless networks. There should be a specific policy regarding wireless networks.