



Personuppgifter i vårdregister

DATAINSPEKTIONENS RAPPORT 2003:4

Innehållsförteckning

Innehållsförteckning	1
1. Inledning	2
2. Sammanfattning	3
3. Reglering av vårdregister	4
4. Datainspektionens iakttagelser och synpunkter	5
4.1 Personuppgiftsansvar	5
<i>Datainspektionens iakttagelser</i>	5
<i>Datainspektionens synpunkter</i>	5
4.2 Information till patienter	5
<i>Datainspektionens iakttagelser</i>	5
<i>Datainspektionens synpunkter</i>	6
4.3 Registerutdrag på egen begäran	6
<i>Datainspektionens iakttagelser</i>	6
<i>Datainspektionens synpunkter</i>	7
4.4 IT-säkerhet	8
4.4.1 Trådlösa nät/bedside	8
<i>Inledning</i>	8
<i>Datainspektionens iakttagelser</i>	8
<i>Datainspektionens synpunkter</i>	8
4.4.2 Uppföljning av åtkomst	10
<i>Datainspektionens iakttagelser</i>	10
<i>Datainspektionens synpunkter</i>	10
4.4.3 Rutiner för kontroll av behörighet	10
<i>Datainspektionens iakttagelser</i>	10
<i>Datainspektionens synpunkter</i>	10
4.4.4 Placering av utrustning	11
<i>Datainspektionens iakttagelser</i>	11
<i>Datainspektionens synpunkter</i>	11

Bilaga.

1. Inledning

Datainspektionen har under 2002 gjort 13 inspektioner för att kontrollera hur patientuppgifter behandlas i vårdregister, särskilt vilken information patienterna får om databehandlingen och hur uppgifterna skyddas. Tio sjukhus och vårdcentraler i totalt fem landsting har inspekterats. Även privata vårdgivare har inspekterats: ett sjukhus, en företagshälsovård och en akut-/specialistmottagning. Inspektionsobjekten framgår av rapportens bilaga. Bakgrunden till inspektionsprojektet är följande.

Under hösten 1997 och våren 1998 gjorde Datainspektionen en omfattande kontroll av databehandlingen av patientuppgifter på sjukhus. Resultatet av inspektionerna redovisades i rapporten "Personregistrering vid sjukhus" (december 1998). År 2000 riktade Datainspektionen en enkät till alla landsting med inriktning på IT-säkerheten på sjukhus. Resultaten sammanställdes och sändes till landstingen i februari 2002. Inspektioner inom sjukvården har visat på brister i den obligatoriska informationen som ska lämnas till patienterna och i IT-säkerheten.

Inspektionerna som nu har legat till grund för den här rapporten visar att det finns anledning att fortsätta granskningen av vårdregister.

2. Sammanfattning

Inspektionerna visade att det fortfarande finns stora brister i informationen till de registrerade. Viss information är obligatorisk enligt vårdregisterlagen, men hos sju av de tretton inspektionsobjekten saknades sådan information helt. I tre fall hade man visserligen tagit fram information, men den fanns inte tillgänglig på vårdenheten. I tre andra fall fanns information tillgänglig, men den hade brister i innehållet, t.ex. angavs inte i klartext vem som var personuppgiftsansvarig.

En annan informationsfråga rör registerutdrag som ska lämnas till den registrerade på dennes skriftliga begäran. I ett fall fick de registrerade besked om vilka vårdcentraler de hade besökt med uppmaning att vända sig till respektive vårdcentral för att få ytterligare personuppgifter. I två fall ansågs patienterna ha rätt att få ut uppgifter ur loggregister, dvs. uppgifter som inte rör patienten. Det finns inget stöd för sådana rutiner.

Det fanns vårdcentraler där personalen inte kände till vem som var personuppgiftsansvarig. Den personuppgiftsansvarige har ett skadeståndssanktionerat, och i vissa fall även straffrättsligt, ansvar för behandlingen. Det är därför viktigt att ha klart för sig vem som är ytterst ansvarig för behandlingen av personuppgifter.

Trådlösa nät granskades på två sjukhus. Där finns anledning att noggrant överväga vilka åtgärder som skall vidtas för att uppnå en fullgod IT-säkerhet. Eftersom det finns risk att trådlös information kan avlyssnas, måste informationen skyddas, t.ex. genom tillförlitlig kryptering.

Rutiner för uppföljning av loggar saknades i mer än hälften av fallen. Eftersom direktåtkomsten till vårdregister är begränsad till vad som behövs för att utföra arbetet, krävs det att det finns rutiner för hur loggarna ska följas upp. Först då är det möjligt att utreda felaktig eller obehörig användning.

På ett sjukhus fanns två skrivare för utskrift av patientuppgifter i korridorer där patienter vistas. Datautrustning ska hållas under uppsikt och placeras så att inga obehöriga kan få del av personuppgifter.

En positiv iakttagelse är att tre av de inspekterade sjukhusen har infört rutiner för att kontrollera att rätt personer har behörighet till vårdregistren. Tidigare inspektioner inom sjukvården har visat på brister inom det området.

3. Reglering av vårdregister

Den som bedriver vård får utföra automatiserad behandling av personuppgifter i vårdregister. Närmare bestämmelser om vårdregister finns i vårdregisterlagen (1998:544). Vårdregisterlagen omfattar bl.a. datajournaler och patient-administrativa datasystem. Exempel på patientadministration är tidbokning, receptförskrivning, remiss- och hjälpmedelshantering samt sammanställningar av patientens tidigare besök och sjukhusvistelser. Datoriserad ekonomi-administration omfattas också av vårdregisterlagen. En gemensam nämnare är att det måste vara fråga om dokumentation eller administration av vård i enskilda fall.

I de fall som behandlingen av personuppgifter inte regleras närmare av vårdregisterlagen gäller i stället personuppgiftslagen, PuL (1998:204). Exempel på detta är IT-säkerhet, skyldighet att lämna information efter skriftlig begäran från den registrerade (registerutdrag) och Datainspektionens tillsynsbefogenheter.

Datainspektionen har utarbetat en informationsbroschyr om vårdregisterlagen (nr 5, juli 2000, ändringsblad 2002). Där förklaras för vilken behandling av personuppgifter vårdregisterlagen gäller och det finns också exempel på hur lagen ska tillämpas. Datainspektionen har också givit ut allmänna råd om säkerhet för personuppgifter som preciserar PuL:s krav på säkerhet då personuppgifter behandlas (december 1999).

4. Datainspektionens iakttagelser och synpunkter

4.1 Personuppgiftsansvar

Datainspektionens iakttagelser

Vid inspektionerna fann Datainspektionen två vårdcentraler där personalen inte kände till vem som var ansvarig för den behandling av personuppgifter som utfördes, dvs. vem som var personuppgiftsansvarig.

Datainspektionens synpunkter

Med personuppgiftsansvarig avses den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter.

Personuppgiftsansvarig inom ett landsting är den nämnd eller den styrelse som ansvarar för verksamheten där vårdregistret förs. Det är alltså inte förvaltningschefen, verksamhetschefen eller vårdcentralens chef som är personuppgiftsansvarig. Bedrivs vården i ett aktiebolag är det bolaget (den juridiska personen) som är personuppgiftsansvarig. Om däremot en läkare eller en sjukgymnast driver en enskild näringsverksamhet är denne själv personuppgiftsansvarig.

Den personuppgiftsansvarige har ett skadeståndssanktionerat ansvar för att personuppgifter behandlas i enlighet med bestämmelserna i PuL och vårdregisterlagen. Flera av de skyldigheter som PuL lägger på den personuppgiftsansvarige är dessutom straffsanktionerade. Det är därför av stor vikt att alla personuppgifter i vårdregister behandlas i enlighet med vårdregisterlagen och PuL och att man har klart för sig vem som är ytterst ansvarig för behandlingen.

4.2 Information till patienter

Datainspektionens iakttagelser

Datainspektionen har vid inspektionerna kontrollerat att de registrerade får den information de har rätt till enligt vårdregisterlagen.

Hos sju av inspektionsobjekten saknades information om vårdregistren. Vid tre inspektioner hade information utarbetats, men den var inte tillgänglig för de registrerade. I ett av dessa fall var informationen bristfällig.

Den information som fanns tillgänglig för patienterna i de övriga tre fallen hade brister av varierande slag, t.ex. hänvisades enbart till PuL och inte till

vårdregisterlagen, det framgick inte i klartext vem som var personuppgiftsansvarig och information om sökbegrepp och rätten till skadestånd saknades.

Datainspektionens synpunkter

Den som är personuppgiftsansvarig för ett vårdregister ska enligt 11 § vårdregisterlagen se till att den registrerade får information om behandlingen av personuppgifterna.

Informationen ska innehålla upplysningar om:

1. vem som är personuppgiftsansvarig,
2. ändamålet med registret,
3. vilken typ av uppgifter som ingår i registret,
4. den uppgiftsskyldighet som följer av lagen om hälsodataregister,
5. de sekretess- och säkerhetsbestämmelser som gäller för registret,
6. rätten att ta del av uppgifter enligt 26 § PuL,
7. rätten till rättelse av oriktiga eller missvisande uppgifter,
8. rätten till skadestånd vid behandling av personuppgifter i strid med denna lag,
9. vad som gäller i fråga om sökbegrepp, direktåtkomst och utlämnande av uppgifter på medium för automatiserad behandling,
10. vad som gäller i fråga om bevarande och gallring, samt
11. om registreringen är frivillig eller inte.

Informationen ska vara tydligt utformad och bör vara tillgänglig på alla vårdenheter. Det finns däremot inte något krav på att aktivt lämna muntlig eller skriftlig information till varje patient. Informationen kan göras tillgänglig i lokalerna genom anslag och/eller broschyrer i anslutning till kassor, receptioner och/eller väntrum.

När det gäller upplysningen om vem som är personuppgiftsansvarig ska det för landstingsdriven vård framgå i klartext vilken nämnd eller styrelse inom landstinget som är personuppgiftsansvarig. De registrerade kan inte anses känna till exempelvis vilken nämnd eller styrelse vårdenheten tillhör.

4.3 Registerutdrag på patientens begäran

Datainspektionens iakttagelser

När det gäller registerutdrag som den registrerade har begärt, användes i ett fall en rutin som innebär att den registrerade efter sin begäran fick ett skriftligt besked om vilka vårdcentraler han eller hon hade besökt. I beskedet uppmanades den registrerade att vända sig till respektive vårdcentral med sin

begäran om registerutdrag. Motivet för denna rutin var dels att den patient-ansvariga läkaren ansågs vara den enda som kunde göra sekretessprövningen, dels att den registrerade vid utlämnandet fick möjlighet att diskutera innehållet i registerutdraget, vilket inte hade varit möjligt om utdraget hade lämnats på annat sätt.

Vid två inspektioner framkom att patienterna ansågs ha rätt att få ut uppgifter ur loggregister. Ett loggregister visar vilken vårdpersonal som har tagit del av uppgifter i exempelvis en datajournal.

Datainspektionens synpunkter

Den obligatoriska informationen enligt 11 § vårdregisterlagen ska innehålla en upplysning om rätten att ta del av uppgifter enligt 26 § PuL, dvs. rätten att begära ett registerutdrag.

Denna rättighet innebär att en person gratis en gång per kalenderår kan begära information om sig själv hos den personuppgiftsansvarige. Vid en sådan begäran är den personuppgiftsansvarige skyldig att lämna besked om personuppgifter som rör den sökande behandlas eller inte. Om personuppgifter om den sökande behandlas ska den personuppgiftsansvarige ta fram ett registerutdrag samt lämna vissa andra upplysningar. Informationen ska som huvudregel lämnas inom en månad efter ansökan. I vissa fall kan tiden utsträckas till fyra månader efter begäran. Ansökan ska vara skriftlig och egenhändigt undertecknad.

I PuL görs undantag från informationsskyldigheten bl.a. vid sekretess och tystnadsplikt. Undantagsbestämmelsen syftar till att förhindra att uppgifter lämnas ut när det råder sekretess i förhållande till den person som begär information om sig själv. I dessa fall kan de sekretessbelagda personuppgifterna maskeras så att de inte kan utläsas i registerutdraget.

Det finns inget stöd i PuL för den rutin för registerutdrag som beskrivs under *Datainspektionens iakttagelser* ovan. Den registrerade ska bara behöva vända sig till den personuppgiftsansvarige en gång för att få begärd information. Skyldigheten att lämna information i ett registerutdrag omfattar inte en skyldighet att lämna information om logguppgifter. Ett utdrag ur ett loggregister ger normalt inte någon upplysning om den person vars personuppgifter behandlas i t.ex. en patientjournal, utan endast om den som har tagit del av journalen genom att läsa den, skriva in nya uppgifter eller göra en utskrift. Det är alltså fråga om någon annans personuppgifter som inte ska tas med i ett registerutdrag.

4.4 IT-säkerhet

4.4.1 Trådlösa nät/bedside

Inledning

Med hjälp av bärbara datorer och trådlösa nät (radiolan) finns i dag möjlighet för vårdpersonal att nå ett vårdregister från andra platser än där det finns fasta terminaler. Användningen av bärbara datorer innebär att läkemedel kan delas ut och mätvärden registreras direkt vid patientens säng, därav namnet bedside. Funktionerna i vårdregistret kan därmed vara direkt anpassade till det arbete som utförs bedside. Ronden kan också genomföras utan papper eftersom man kan läsa och anteckna i patientjournalen med hjälp av en bärbar dator. Kommunikationen i det trådlösa nätet sker via basstationer som monteras i byggnaden. Basstationerna är en slags antenner som utgör s.k. accesspunkter, där det trådlösa nätet kommunicerar med det fasta. I den bärbara datorn finns ett radiolankort som möjliggör kommunikation via radiosignaler med basstationen.

Datainspektionens iakttagelser

Datainspektionen kontrollerade trådlösa nät på två sjukhus. Nedan redovisas några iakttagelser som särskilt rör informationssäkerheten kring trådlösa nät.

- För att skydda kommunikationen i nätet användes WEP-kryptering.
- Basstationerna i det trådlösa nätet har normalt en i förväg vald identitet som sänds i klartext. Ett av sjukhusen hade valt en identitet som kunde avslöja att nätet användes för ett vårdregister. Tester utförda av ett sjukhus visade att den identitet som valts kunde uppfattas vid avlyssning utanför sjukhusbyggnaden.
- Basstationerna kontrollerade inte närmare att endast i förväg godkända radiolankort kunde kommunicera i det trådlösa nätet.
- Radiolankortet var ett instickskort i datorn och var därmed lätt att ta bort.
- Det fanns ingen brandvägg eller liknande skydd mellan accesspunkten och sjukhusnätet.

Datainspektionens synpunkter

Den personuppgiftsansvarige ska enligt 31 § PuL 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.

Vårdregistren innehåller känsliga personuppgifter. Detta förhållande ska väga tungt när den personuppgiftsansvarige överväger vilka lämpliga tekniska och organisatoriska åtgärder som behövs för att skydda de personuppgifter som behandlas i ett vårdregister.

Att överföra information i ett vårdregister via ett trådlöst nät får anses kräva särskilda överväganden. Anledningen är bl.a. att kommunikation via radio-signaler kan avlyssnas på ett helt annat sätt än kommunikation i fasta installationer. Det finns också en risk att kommunikationen i det trådlösa systemet sprids utanför den byggnad eller lokal där systemet används.

Information till eller från ett vårdregister som överförs via ett trådlöst system måste därför bl.a. skyddas från obehörig avlyssning, t.ex. genom tillförlitlig kryptering. Kryptering med WEP ger inte ett tillräckligt skydd. Krypteringen får anses vara svag, bl.a. bygger den på gemensamma symmetriska krypteringsnycklar. Med hänsyn till det känsliga innehållet måste informationen skyddas med en kryptering som ger en hög säkerhet. Exempel på en kryptering som i dag anses ge en hög säkerhet är VPN-teknik.

Utöver en kryptering med hög säkerhet bör åtminstone följande säkerhetsåtgärder övervägas för att uppnå fullgod säkerhet för vårdregister i ett trådlöst nät.

- Användarens identitet bör säkerställas genom kryptering, engångslösenord, aktiva behörighetskort eller motsvarande.
- Möjlighet till annan trafik bör blockeras i det trådlösa nätet.
- Det trådlösa nätets identitet bör ändras till en neutral benämning som inte för tanken till hälso- och sjukvård och vårdregister.
- Bärbara datorer som används för kommunikationen måste hållas under uppsikt eller låsas in när de inte används.
- Radiolänkortet bör vara inbyggt i datorn eller skyddas på annat sätt.
- En brandvägg eller annan typ av kontroll bör finnas mellan accesspunkten och sjukhusnätet.

Utöver detta kan även andra åtgärder vara befogade för att uppnå en fullgod säkerhet.

4.4.2 Uppföljning av åtkomst

Datainspektionens iakttagelser

Vid sex av tretton inspektioner framkom att det inte fanns rutiner för uppföljning av hur vårdpersonalen använder vårdregistren.

Datainspektionens synpunkter

I 8 § vårdregisterlagen finns en bestämmelse om direktåtkomst till vårdregister. Av bestämmelsen framgår i huvudsak att endast den som behöver tillgång till uppgifterna för att kunna utföra sitt arbete får ha direktåtkomst till uppgifter i ett vårdregister.

För att det ska gå att följa upp åtkomsten till ett vårdregister i enskilda fall krävs en logg. Med loggens hjälp ska det gå att utreda felaktig eller obehörig användning. Det ska finnas rutiner för hur man följer upp loggar, t.ex. genom stickprovskontroller.

4.4.3 Rutiner för kontroll av behörighet

Datainspektionens iakttagelser

Rutiner för att kontrollera att rätt personer har behörighet till vårdregistren har inspekterats på tre sjukhus. En rutin innebar att när någon slutar sin anställning rapporterar avdelningsföreståndaren till en person som handlägger frågor om IT-säkerhet. Handläggaren ser till att behörigheten tas bort och att användarkontot inaktiveras. En gång i kvartalet tar man dessutom ut listor som lämnas till de olika verksamheterna. På listan markeras vilka som har slutat. Listorna ska återlämnas före ett visst datum och saknade listor följs upp.

I ett annat fall gjordes en månatlig kontroll av att användarna är anställda och verksamma vid enheten samt att de har rätt behörighet. Den lokala systemadministratören tar fram en lista över användare som respektive avdelningschef kontrollerar och signerar. Listan arkiveras därefter en viss tid.

I det tredje fallet tillämpades också en rutin med listor som kontrolleras av klinikernas IT-samordnare.

Datainspektionens synpunkter

För att de personuppgiftsansvariga ska kunna följa 8 § i vårdregisterlagen om direktåtkomst till vårdregister måste det finnas rutiner för att ta bort användare som inte längre har rätt att ha direktåtkomst till uppgifterna. Det kan röra sig om anställda som har slutat sin anställning eller bytt arbetsuppgifter.

De rutiner som beskrivs ovan kan ses som exempel på kontroller för att förhindra obehörig användning av vårdregister.

4.4.4 Placering av utrustning

Datainspektionens iakttagelser

På ett sjukhus var två skrivare som användes för utskrifter av patientuppgifter placerade i korridorer där patienter vistades.

Datainspektionens synpunkter

Serverar, skrivare och all annan datautrustning ska förvaras och placeras på ett säkert sätt så att olika risker undanröjs, t.ex. att obehöriga tar del av patientuppgifter. Utrustning som inte används eller hålls under uppsikt ska skyddas. Lämpliga åtgärder kan vara inlåsning (serverar, skrivare, bärbara datorer) och aktivering av skärmläckare med lösenord (terminaler, dataskärmar).

Bilaga

Förteckning över inspektionsobjekt (omorganisationer kan ha ägt rum efter inspektionerna).

Akademiska sjukhuset, Styrelsen för Akademiska sjukhuset i Uppsala läns landsting

Alviva AB, Köping

Cityvården AB, Stockholm

S:t Görans sjukhus AB, Stockholm

Sunderby sjukhus, Landstingsstyrelsen i Norrbottens läns landsting

Landstinget Gävleborg:

Länssjukhuset Gävle-Sandviken i Gävle, Landstingsstyrelsen

Stortorget's Hälsocentral i Gävle, Landstingsstyrelsen

Landstinget Värmland:

Centralsjukhuset i Karlstad, Hälso- och sjukvårdsnämnden

Vårdcentralen Västerstrand i Karlstad, Hälso- och sjukvårdsnämnden

Örebro läns landsting:

Lasarettet i Karlskoga, Styrelsen för Karlskoga lasarett

Brickegårdens vårdcentral i Karlskoga, Styrelsen för primärvård

Universitetssjukhuset i Örebro, Sjukhusstyrelsen för Universitetssjukhuset

Olaus Petri vårdcentral i Örebro, Styrelsen för primärvård



Besöksadress: Fleminggatan 14, plan 9
Postadress: Box 8114, 104 20 Stockholm
Beställningar: 08-657 61 42 (telefonsvarare)
Webbplats: www.datainspektionen.se
E-post: datainspektionen@datainspektionen.se
Fax: 08-652 86 52
Tel: 08-657 61 00

Pris: 50 kr + moms