

Svar på interpellation 2011:50 av Michel Silvestri (MP) om elektroniska journalsystem, patient(data)säkerhet och patientintegritet

Michel Silvestri (MP) har ställt följande frågor till mig om säkerhet och integritet för patienten i datoriserade journalsystem:

1. Vad gör Du för att säkerställa och skydda patienters säkerhet och integritet utifrån ett medicinskt datalagringsperspektiv?
2. Finns det fortsatt risk för att patienter inom vårdverksamhet som SLL ansvarar för ska drabbas av förlorade digitala patientdata av något slag?
3. Finns det risk för att patientdata har kommit, eller kan komma, på avvägar t ex genom utförsel över Sveriges gränser?
4. Hur ser Du till att vårdpersonalens tillgång till digitala patientdata inte missbrukas ?

Som svar vill jag anföra följande:

Inom Stockholms läns landsting hanteras mycket information och kraven måste vara höga på att informationen hanteras konfidentiellt. Det rör främst patientuppgifter i medicinska journaler. En stor del av informationen bearbetas och hanteras i datasystem. Det skulle vara mycket allvarligt om informationen hamnar i orätta händer. Därför är det av största vikt att gällande regler följs och uppföljningar ständigt görs att regelverket tillämpas på ett korrekt sätt.

Informationssäkerheten måste vara mycket hög inom landstinget. Landstingsfullmäktige fastställde därför år 2003 särskilda riktlinjer för informationssäkerheten i landstinget och dessa riktlinjer har gällt tills nyligen. Den lokala organisationen ska vara väl anpassad för att svara mot uppdraget. Det är viktigt att fortlöpande se över hur informationssäkerhetsarbetet bedrivs inom landstinget och vid behov vidta förändringar. Ett uppdrag finns i budgeten för år 2012 att se över den nuvarande organisationen för informationssäkerhetsarbetet. Landstingsrevisorernas har till uppgift att granska att den interna kontrollen är tillräcklig. Uppföljningen av policyn ska ske regelbundet.

Frågor om informationssäkerhet regleras i patientdatalagen (SFS 2008:355). Närmare bestämmelser om tillämpningen finns i Socialstyrelsens föreskrifter om informationssäkerhet och journalföring (SOSFS 2008:14).

Vårdgivaren ska ge direktiv och säkerställa att det i verksamhetens ledningssystem för kvalitet och patientsäkerhet finns en dokumenterad informationssäkerhetspolicy (SOSFS 2008:14).

Informationssäkerhetspolicyn ska säkerställa att

1. patientuppgifter i vårdgivarens dokumentation är åtkomliga och användbara för den som är behörig (tillgänglighet),
2. patientuppgifterna är oförvanskade (riktighet),
3. obehöriga inte ska kunna ta del av patientuppgifterna (sekretess), och
4. det i sådana informationssystem, som är helt eller delvis automatiserade, är möjligt att i efterhand entydigt kunna härleda åtgärder till en identifierad användare (spårbarhet).

Övergripande informationssäkerhetspolicy kan beslutas av landstinget. Dock är varje enskild vårdgivare skyldig att ha en policy för den säkerhet som är nödvändig i deras verksamhet.

I patientdatalagen finns bestämmelser om vilken behandling av personuppgifter som är tillåten i hälso- och sjukvården. Det finns ett reglerat ansvar för att personalen följer de bestämmelser som finns i lagen och föreskriften om t.ex. behörighet för åtkomst och säkerhet. I lagen och föreskrifterna specificeras även skyldigheterna för t.ex. verksamhetschefen.

Hälso- och sjukvårdspersonalen har också enligt patientsäkerhetslagen ett reglerat ansvar för att patientuppgifter hanteras på rätt sätt.

Jag vill lämna följande svar på interpellantens specifika frågor:

1. Ett ny policy för informationssäkerhet och tillhörande riktlinjer har tagits fram inom landstinget. Landstingsfullmäktige fastställde policyn vid sitt sammanträde i december 2011. De båda dokumenten beskriver de principer som ska gälla och de ger vägledning för verksamheterna, exempelvis till dem som ansvarar för personuppgiftsbehandling. Som en del i samtliga avtal/förfrågningsunderlag d v s regelböcker med vårdgivarna finns en bilaga om Informationsförsörjning. I avtalsbilagan finns krav avseende både informationssäkerhet och informationshantering. I bilagan anges bl a att alla vårdgivare ”skall skydda sin information mot otillbörlig åtkomst och förstörelse i enlighet med gällande lagar, förordningar och föreskrifter. Hur skyddet genomförs skall dokumenteras”. Vidare finns i bilagan ett helt avsnitt som handlar om just ”personuppgiftshantering”. Genom dessa krav säkerställs att den som bedriver vård på landstingets uppdrag följer gällande regelverk om säkerhet och integritet. Inom ramen för ordinarie avtalsuppföljning sker även uppföljning av bilagan kring Informationsförsörjning.

2. Risk för förlust av patientdata finns tyvärr alltid. Risken minimeras genom ett metodiskt informationssäkerhetsarbete. Genom att regelbundet arbeta med exempelvis omvärldsbevakning och riskanalys, omprövas skyddsåtgärderna regelbundet och informationstillgångar som patientdata kan ges erforderlig skyddsnivå.
3. Det finns möjligheter att sända patientdata till andra länder inom EES t.ex. Norge, med rättsligt stöd. En sekretessprövning ska naturligtvis alltid företas och den som skickar handlingarna måste säkerställa att uppgifterna inte kommer på avvägar. Denna rutin ska bara tillämpas i enskilda fall och i enlighet med gällande rutiner.
4. För att nu ytterligare förstärka skyddet kring patientdata byggs många olika IT-system om för att få en säkrare behörighetskontroll. Många administrativa vårdgivartjänster såsom t.ex. elektroniska sjukintyg, apodosförskrivning och WebCare (ett system som används när patienter överförs från slutenvård till primärvård och kommunens omsorgsverksamhet), går inom en snar framtid över till säkrare behörighetskontroll i form av kortinloggning. Arbetet med informations säkerhetspolicyn syftar bl.a. till att säkerställa att det finns övergripande principer för hur behörigheten ska avgränsas så att personalen får tillgång till alla de uppgifter som krävs för en patientsäker vård, men inga patientuppgifter utöver det.

Därmed anser jag interpellationen besvarad.

Birgitta Rydberg