SKaPa

SVENSKT KVALITETSREGISTER FÖR KARIES OCH PARODONTIT

Informationssäkerhet – en fråga om kvalitet

Text: Jörgen Larsson, informationsarkitekt, anlitad av SKaPa vid uppbyggnaden av SKaPas datalager

Artikeln hämtad ur SKaPa Årsrapport 2015

SKaPa satsade redan från början på att finna en användbar struktur för den information som lagras i SKaPas datalager. En begreppsmodell och hierarki utarbetades för den information som levereras från tandvårdsorganisationernas datoriserade patientjournaler, för att kunna ha kontroll på informationskvalitet och möjliggöra insamling, validering och analys av stora datamängder. Har du någon gång funderat över varför datasystem ibland tycks skapa merarbete eller att det är svårt och dyrt att få fram bra och användbar information? Många gånger är det inte helt lätt att se sambanden mellan dubbelarbete, missförstånd och oönskade extrakostnader som kan uppstå i en verksamhet med det IT-arbete som är gjort, kanske flera år tidigare. Är det tekniken som är problemet?

Informationssäkerhet – en kvalitetsfråga
Informationssäkerhet är ett grundläggande begrepp som rör mer än att skydda våra informationstillgångar från obehöriga. Det handlar även om att informationen ska vara korrekt återgiven nu och i framtiden. Definitionen av informationssäkerhet från Lunds Universitet ger en vink om bredden av begreppet och att det inte bara är frågan om teknik.

” … att rätt information är tillgänglig för rätt person när den behövs och på ett spårbart sätt samt att informationen är och förblir riktig över tid”

För att kunna bedriva ett säkerhetsarbete med helhetssyn behöver vi därför förstå de olika egenskaperna inom informationssäkerhet. Vi pratar då om journalsystemets förmåga att hantera information utifrån såväl sekretess, tillgänglighet, riktighet som oavvislighet och spårbarhet.

• **Sekretess** (eg. konfidentialitet) avser systemets förmåga att ge åtkomst till data endast till behöriga. Här menar vi tex. brandväggar eller behörighetssystem men även fysiskt skydd av utrustning som tex. att förhindra stöld av servrar och obehörig åtkomst innanför brandväggarna.

• **Tillgänglighet** avser systemets förmåga att ge åtkomstmöjlighet till funktioner och information när behoven finns. Här pratar vi ofta om SLA (Service Level Agreement) som ett medel för att styra tillgängligheten.

Oftast mäts tillgängligheten i hur stor del av tiden som ett system kan nås av användarna och här gäller det att ha rimliga krav då en överdimensionering kan kosta mer än det smakar.

• **Riktighet** avser systemets förmåga att återge korrekta uppgifter. Ur ett verksamhetsperspektiv är det här mer än systemets förmåga att identifiera enskilda företeelser. Det avser även förmågan att säkerställa en entydig betydelse av olika begrepp. Till exempel att det bara finns data för verkliga patienter i patientregistret eller att filer för åtgärder bara innehåller åtgärder och inte något annat samtidigt.
Viktigt i detta sammanhang är att det även innebär systemets förmåga att återge korrekt information över tid, med andra ord det som täcks in av sista delen i definitionen tidigare.

• **Oavvislighet** avser systemets förmåga att säkerställa att aktiviteter och händelser verkligen har hänt så att de senare inte behöver förkastas. Dvs vi behöver veta att uppgifterna om vad som har hänt stämmer med verkligheten. Att kunna identifiera dessa data innan de tas med i statistiken är inte alltid så lätt.

• **Spårbarhet** avser systemets förmåga att återge vad som har ändrats, av vem och när. Dvs vi behöver kunna se vad som har hänt när något går fel. Innan man väljer kan det därför vara bra att tänka till runt vad verksamheten behöver veta om något avvikande har hänt.

Samtliga aspekter av informationssäkerhet är betydelsefulla
Egenskaperna riktighet och oavvislighet kan inte kontrolleras helt medtekniska lösningar och skiljer sig därmed något från de tre övriga egenskaperna, sekretess, tillgänglighet och spårbarhet. De senare är något som IT-enheter och systemleverantörer ofta har bra koll på och förstår att kravställa på rätt sätt. Egenskaperna riktighet och oavvislighet däremot kräver detaljerat verksamhetskunnande tillsammans med kunskaper inom begreppsanalys och systemering.
Även om ett datasystem inte kan verifiera att en registrerad observation verkligen har inträffat eller att en registrerad klinik verkligen är en fysisk klinik kan man lägga in kontroller och spärrar i systemet mot orimliga värden. Till exempel kan i SKaPa en tandyta inte dokumenteras vara intakt efter att den har observerats med till exempel manifest karies. På samma sätt kan vi validera registrerade kliniker mot en lista med giltiga kliniker. Men sådan inbyggd validering kräver givetvis en detaljerad kunskap och förståelse av verksamheten.
Krav på alla områdena inom informationssäkerhet är alltså viktiga att ställa för att man ska kunna vara rimligt säker på att datasystemet kan hantera information på ett korrekt sätt.