Datum
2014-11-04

Diarienr
2014-3176-2

Ert datum
2014-06-16

Er referens
S2014/112/FS

Verksamheten för samhällets informations- och cybersäkerhet
Fia Ewald
010-2404493
fia.ewald@msb.se

Regeringskansliet
Socialdepartementet

103 33 Stockholm

Betänkandet SOU 2014:23 Rätt information på rätt plats i rätt tid

Sammanfattning

Myndigheten för samhällskydd och beredskap (MSB) delar utredningens syn att informationssäkerhet är en mycket viktig fråga för den svenska sjukvårdens informationshantering och att det i dag finns stora brister inom området. De framförda konkreta förslagen i utredningen anser MSB dock inte leder i rätt riktning när det gäller informationssäkerhetsfrågan.

Det går inte att undgå intrycket av att den föreliggande utredningens förslag i hög grad sammanfaller med de önskemål som vårdgivare och sjukvårdshuvudmän fört fram i ett antal sammanhang rörande nuvarande reglering. MSB menar dock att syftet med att förändra lagstiftningen inte kan vara att anpassa regleringen till den rådande bristen på efterlevnad av patientdatalagen (2008:355). I fråga om kraven på god informationssäkerhet i patientdatalagen hävdar MSB istället att dessa har en hög grad av giltighet och måste behandlas därefter. Informationssäkerheten inom vård och omsorg kan inte styras av utförarnas intressen. Istället bör den ofta uttalade devisen att sätta patienten i centrum också överföras till att gälla inom informationssäkerhetsområdet. Detta skulle betyda att vårdens aktörer accepterar att patienten har ett antal olika intressen som till exempel god patientsäkerhet och hög integritet samt att dessa intressen inte får ställas emot varandra. Uppgiften är istället att se till att dessa intressen kan tillgodoses samtidigt vilket är fullt möjligt med ett långsiktigt systematisk informationssäkerhetsarbete som en bas i allt arbete, nationellt, regionalt som lokalt. Den föreliggande utredningens förslag skulle, om de förverkligades, vara en tillbakagång och inte det nödvändiga krafttag som behövs för att vårdens informationssäkerhet skulle vara i paritet med de rimliga krav som både den enskilda patienten och samhället kan ställa på vårdens aktörer. Målet bör istället vara att ta fram en gemensam långsiktig styrmodell för informationssäkerhet inom vård och omsorg som kan hantera både normalläge och även situationer då samhället utsätts för större störningar.

Inför de utmaningar som den svenska vården står inför när det gäller den gemensamma informationshanteringen är det inte verkningsfullt att, som i den föreliggande utredningen, inrikta sig på att reglera de enskilda vårdgivarnas ansvar. Ett mer strategiskt perspektiv är nödvändigt där hänsyn tas till att en allt större del av informationsflödet sker mellan organisationer och inte längre inom organisationer. MSB föreslår därför:

- Att innan ställning tas till de nu aktuella lagförslagen ska resultaten från e-hälsokommitténs pågående arbete avvaktas, där informationssäkerhet också kommer att lyftas fram som en prioriterad fråga och som kan förväntas ge underlag för en strategisk inriktning av e-hälsoområdet
- Att en analys genomförs av hur ansvaret bör regleras för att fungera även för den alltmer integrerade nationella informationsinfrastrukturen inom vården
- Att en nulägesanalys genomförs av rådande situation gällande informationssäkerhet inom vården
- Att en grundlig riskanalys genomförs som också kan leda fram till prioriterade förlag på åtgärder för att förbättra informationssäkerheten inom vården
- Att konsekvensanalyser ur ett informationssäkerhetsperspektiv görs då förändringar av patientdatalagen eller andra genomgripande förändringar i reglering som påverkar vårdens informationshantering föreslås

När den nationella strategin för e-hälsa börjar utarbetas är det lämpligt att se över vilka legala förändringar som kan krävas för att förverkliga strategiska vägval. Dessa vägval är då förhoppningsvis förankrade i en omfattande diskussion som inkluderar samtliga aktörer med intresse för en väl fungerande vård, även de utanför sjukvårdshuvudmännens och vårdgivarnas intressesfär.

Bakgrund

Avgränsningar i MSB:s remissvar

Det föreliggande betänkandet innehåller förslag angående reglering av informationshanteringen inom hälso- och sjukvård samt inom socialtjänst. MSB väljer att inte särskilt kommentera förslagen angående socialtjänsten. De generella synpunkter som lämnas angående förslagen rörande hälso- och sjukvårdens informationshantering går dock i huvudsak att överföra till förslagen angående informationshanteringen inom socialtjänsten.

MSB lämnar heller inte synpunkter på det konkreta förslaget på utformning av ny lagstiftning med tanke på de generella invändningar myndigheten har angående konsekvenserna om utredningens förslag skulle genomföras.

MSB:s roll inom informationssäkerhetsområdet

MSB har uppdraget att stödja och samordna arbetet med samhällets informationssäkerhet. Med informationssäkerhet avses att omge information med rätt nivå av skydd i aspekterna konfidentialitet, riktighet, spårbarhet och tillgänglighet. I de föreskrifter som reglerar vårdens informationshantering är det också dessa aspekter som ska säkerställas med stöd av ett ledningssystem för informationssäkerhet[1].

I den nationella handlingsplan för samhällets informationssäkerhet som MSB tillsammans med de myndigheter som ingår i Samverkansgruppen för informationssäkerhet (de så kallade SAMFI-myndigheterna)[2] tog fram 2012 är det en prioriterad uppgift att ge stöd till vård och omsorg samt till kommuner. Vård och omsorg är att betrakta som en samhällsviktig verksamhet där det yttersta ansvaret ligger hos sjukvårdshuvudmännen, det vill säga kommuner och landsting/regioner. Hälso- och sjukvård och omsorg är också en av de samhällssektorer som omfattas av den nationella strategin och handlingsplanen för skydd av samhällsviktig verksamhet som MSB på regeringens uppdrag tagit fram.[3] Den föreliggande utredningens förslag berör i och med det två av MSB prioriterade områden och av denna anledning har MSB analyserat förslagen utifrån hur de påverkar informationssäkerheten i vård och omsorg.

Övergripande synpunkter på betänkandets förslag

Förutsättningen för ett robust samhälle är att människor ska kunna känna tillit till samhällviktiga funktioner som exempelvis vård och omsorg. Vården är idag beroende av att informationshanteringen fungerar. I och med detta blir informationssäkerhet en fråga av central betydelse för vården. Det finns tydliga indikationer på att informationssäkerheten i vården har brister som innebär risker för patientsäkerhet och patienters rätt till integritet. Eftersom det idag saknas en lägesbild skapad utifrån systematisk insamling av incidenter i informationshanteringen inom vård och omsorg går det inte att med säkerhet bedöma situationen. MSB anser dock att det med stöd från de rapporter som tagits fram av Socialstyrelsen och Datainspektionen samt landstingens egna

---

[1] 2 § Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården, SOSFS 2008:14

[2] Myndigheten för samhällskydd och beredskap (MSB), Post- och telestyrelsen (PTS), Försvarets radioanstalt (FRA), Säkerhetspolisen (Säpo) och Rikskriminalpolisen (RKP) i samverkan, Försvarets materielverk (FMV)/Sveriges certifieringsorgan för IT-säkerhet (CSEC), Försvarsmakten (FM)/Militära underrättelse- och säkerhetstjänsten (MUST)

[3] Myndigheten för samhällsskydd och beredskap, Ett fungerande samhälle i en föränderlig värld - Nationell strategi för skydd av samhällsviktig verksamhet, publnr MSB266, 2011; Myndigheten för samhällsskydd och beredskap, Handlingsplan för skydd av samhällsviktig verksamhet, publnr MSB597, 2013

revisionsrapporter och myndighetens iakttagelser går att säga att nivån på informationssäkerhet inom vården inte motsvarar de krav som är rimliga att ställa utifrån verksamhetens betydelse för individer och samhället i stort.

Det föreliggande betänkandet, Rätt information på rätt plats och i rätt tid, innehåller ett antal förslag som om de förverkligas enligt MSB:s bedömning skulle leda till försämringar för skyddet av vårdens information. Detta innebär ökade risker både när det gäller patientssäkerhet och integritet. Utredningen har också förbigått att analysera den beredskap som vården måste ha för att hantera större och mindre kriser och de krav som detta ställer på informationshanteringen. MSB anser att förutsättningen för att klara allvarliga störningar är en väl fungerande informationssäkerhet i normalläget som kan skalas upp på ett planerat sätt. Detta ställer stora krav på både organisatoriska och tekniska förutsättningar som måste integreras i den utformningen av informationshanteringen både lokalt och nationellt.

Mest radikalt är utredningens förordande av ett paradigmskifte i integritetsfrågan. Om utredningens förslag skulle genomföras skulle det leda till att den som söker hjälp i den offentligt finansierade vården genom detta med automatik avsagt sig rätten att begränsa åtkomsten till den information som skapas i samband med vården. MSB delar experten Maria Bergdahls bedömning, som framförs i ett särskilt yttrande, att det behövs genomarbetad analys av hur utredningens olika förslag sammantaget påverkar patientens integritet innan vidare beslut tas. Det finns ett underliggande tema i utredningen som återkommande framkommer i problembeskrivningen. Utredningen tycks mena att det inte är möjligt att utveckla en informationshantering som samtidigt stödjer god patientsäkerhet och god integritet för patienten. MSB har en annan uppfattning, det är inte bara möjligt att uppnå dessa två mål utan också nödvändigt för att få väl fungerande vård som sätter patientens intressen i centrum.

Utredningen framhåller vidare de begränsningar som den nuvarande ”organisationsinriktade” lagstiftningen innebär och förespråkar en starkt vidgad åtkomst av information kring patienter och klienter över huvudmannagränser. MSB menar att utredningen genom detta tar bort en organisatorisk struktur för ansvar utan ersätta den med en annan. Detta blir också problematiskt då utredningen i sitt förslag lägger ansvaret för styrning av informationshantering och informationssäkerhet på den enskilda vårdgivaren. I den komplexa och alltmer gemensamma it- och informationsinfrastruktur som stödjer den svenska vården anser MSB att vårdgivarna de facto inte har möjlighet att ställa verkningsfulla krav och därmed ta det ansvar som utredningen beskriver.

Innan en ny gemensam inriktning för svensk e-hälsa som beskriver hur vårdens informationshantering ska ske och vilka aktörer som ska interagera i denna helhet har tagits fram anser inte MSB att nuvarande lagstiftning bör förändras. Istället bör en analys genomföras som omfattar en beskrivning av nuläget gällande vårdens informationssäkerhet och en riskanalys som grundligt

går igenom och värderar de risker som vården är utsatt för genom sin informationshantering. Först med detta underlag är det möjligt att bedöma vilka organisatoriska och tekniska åtgärder som måste vidtas för att ge förutsättning att reducera aktuella och förutsägbara risker i en nära framtid till en acceptabel nivå. I ett systematiskt informationssäkerhetarbete är alltid de organisatoriska styrmodellerna grunden. MSB anser därför att en analys som också definierar funktionella ansvarsförhållanden för den gemensamma informationshanteringen på nationell nivå i en gemensam infrastruktur måste föregå en ny lagstiftning. I den pågående E-hälsokommittens uppdrag ingår också att föreslå ett antal strategiska ställningstaganden i näraliggande frågor och MSB anser att en lagstiftning måste utformas så att de ligger i linje med den strategiska inriktningen.

Informationssäkerheten i vård och omsorg

Vårdens informationshantering är idag mycket komplex. Komplexiteten finns inte bara i själva informationshanteringen utan också i mängden aktörer som på olika sätt deltar i informationshanteringen samt deras inbördes relationer. Taget i beaktande den roll som hälso- och sjukvård har som samhällsviktig verksamhet och det starka beroende till informationshanteringen blir informationssäkerhet en central fråga. Det är därför oroande att det finns ett flertal större händelser som tyder på att informationssäkerheten inom vården inte når upp till den nivå som verksamhetens typ kräver. Att det finns strukturella brister i säkerheten framgår bland annat i rapporter från Datainspektionen, Socialstyrelsen och IVO [4] men också genom de revisionsrapporter som landstingen själva tagit fram[5]. Dessa rapportet tyder på att vårdgivarna inte bedriver ett systematiskt informationssäkerhetsarbete trots att Socialstyrelsen sedan 2008 tydligt i sina föreskrifter[6] ålagt vårdgivarna att göra detta, något som bland annat patientdatalagen också förutsätter ska fungera. Det inträffar också ett antal större och mindre it-incidenter[7]. Omfattningen och konsekvenser av dessa incidenter är svår att klarlägga eftersom det saknas en systematisk uppföljning i detta hänseende. Intrycket är dock att informationssäkerheten inom vården har stora brister på samma gång

---

[4] Se även det underlag utredningen hänvisar till på sidan 119 f och även till exempel Datainspektionens beslut efter tillsyn – Behörighetsstyrning och loggkontroll inom kommunal hälso- och sjukvård dnr 576-2013

[5] Till exempel Landstinget Västernorrland dnr 12HSN27, Stockholms läns landsting RK 201403-0009

[6] 2 § Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården SOSFS 2008:14

[7] Till exempel Rapport gällande ”skadlig kod” Västra Götalandsregionen Dec 2012 – Jan 2013, Stockholms läns landsting, Analyskommissionens slutrapport avseende driftstoppen som drabbade TakeCare den 11 juni och den 18 juni 2013, http://www.liv.se/Om-landstinget-i-Varmland/Pressrum/Pressmeddelanden/Avvikelse-i-journalsystem-inom-Landstinget-i-Varmland/, http://sverigesradio.se/sida/artikel.aspx?programid=160&artikel=5964329, http://jo.se/PageFiles/4794/3032-2011.pdf

som det finns en generell tendens med ett ökat antal incidenter med stor påverkan. Att påverkan på verksamheten är så stor beror bland annat på den ökande koncentrationen av tjänster, system och drift vilket leder till fler aktörer och funktioner riskerar att slås ut samtidigt[8].

Genom den starka koncentrationen av informationshanteringen eskalerar de risker som redan tidigare funnits när information i huvudsak hanterades inom varje organisation. När en allt mer nationell informationsinfrastruktur skapas får olika typer av incidenter också konsekvenser på nationell nivå. Avbrott, intrång, informationsförluster och bristande riktighet kan då drabba vårdgivare i hela landet samtidigt och en situation med nationella konsekvenser kan därmed uppstå. MSB har analyserat vad den ökade koncentrationen av informationshanteringen innebär i den rapport som skildrar den så kallade Tieto-incidenten[9]. Slutsatserna om risker och konsekvenser av större it-incidenter som beskrivs i rapporten är relevanta även för vård och omsorg och bör därför beaktas när diskussioner förs kring vårdens informationshantering.

I detta sammanhang kan inte heller risken för antagonistiska it-attacker med syfte att slå ut tjänster eller få åtkomst till stora mängder personuppgifter negligeras[10]. Personuppgifter, och då särskilt känsliga sådana, är idag mycket användbara i olika illegala syften och den mängd av just denna typ av uppgifter som idag samlas inom vårdsystemen utgör därför ett mycket intressant mål för illasinnade aktörer.

Koncentrationen av information, tjänster och infrastruktur gör också att det är svårt att upprätthålla de ansvarsförhållanden för informationshanteringen som både föreskrivs i lag och föreskrifter. Den enskilde vårdgivaren har liten möjlighet att i realiteten styra informationssäkerheten i den information som är nödvändig för den egna verksamheten då den i allt högre grad sker genom utbyte med andra vårdgivare och i nationella tjänster. Att ställa bilaterala krav mellan ett mycket stort antal aktörer är ett i längden ogenomförbart sätt att styra informationssäkerheten i vården. Ett alternativ är en lösning liknande det nationella regelverk som skapats i Norge, Normen, till vilken olika aktörer måste acceptera för att få ansluta sig till det gemensamma informationsutbytet i vården.

---

[8] Ett intressant exempel på hur nya nationella lösningar förs in i den gemensamma infrastrukturen efter bristfällig kontroll finns beskrivet i Slutrapport Införande av Pascal ordinationsverktyg för dosordinationer i Västra Götaland, 2012-12-05.

[9] Myndigheten för samhällsskydd och beredskap, Reflektioner kring samhällets skydd och beredskap vid allvarliga it-incidenter - En studie av konsekvenserna i samhället efter driftstörningen hos Tieto i november 2011, publikationsnummer MSB367

[10] Ett aktuellt exempel på detta är beskrivet här: http://www.inera.se/OM-OSS/Nyheter/Nyheter/Sarbarhet-i-SSL-v3/

Den ovan beskrivna utvecklingen är oroande. En bristande informationssäkerhet äventyrar både patientssäkerheten, patientens integritet och personalens rättsäkerhet. Brister leder även till stora och onödiga kostnader bland annat genom att ekonomiskt krävande insatser för att reducera konsekvenserna av it-incidenter måste genomföras. Incidenternas konsekvenser och kostnader skulle med all sannolikhet vara betydligt mindre om ett systematiskt, förebyggande arbete bedrivits.

Ytterst kan tilliten till en av samhällets mest centrala funktioner skadas men MSB vill även betona att fungerande informationssäkerhet i ett normalläge är förutsättning för att sjukvården ska kunna upprätthålla sin informationshantering och därmed även verksamhet i ett krisläge.

Generellt angående informationssäkerhet i utredningens förslag

Utredningen tycks i huvudsak dela MSB:s uppfattning både om vikten av informationssäkerhet i sjukvården och om att den nuvarande situationen inte uppfyller rimliga krav på skydd av informationen. Att informationssäkerhet nämns på ett stort antal ställen i utredningen är också positivt. Utredningens konkreta förslag innebär dock paradoxalt nog att kraven på informationssäkerhet skulle sänkas om förslagen genomförs. Utredningens insikt om informationssäkerhetens betydelse har, trots rapportens omfång, endast lett till omnämnande av begreppet men inte till att analysera varför, på vilket sätt, av vem och vad som bör genomföras för att förbättra informationssäkerheten. Inte ens begreppets innebörd anser utredningen klarlagd trots att det som tidigare nämnts finns i föreskrift sedan 2008[11].

Informationssäkerhet beror i hög grad på en systematisk styrning av informationshanteringen inom en organisation. Samverkar flera organisationer kring informationshanteringen behövs organisatoriska former, inklusive gemensamma regler, för att styra informationshanteringen i denna samverkan. Att utredningen bortser från utvecklingen i denna riktning och, med undantag för kravet på riskanalys vid direktåtkomst mellan vårdgivare[12], inriktar sig på styrning av de enskilda vårdgivarna är därför, om målsättningen är att förbättra informationssäkerheten, otillräckligt. Även om utredningen framhåller informationssäkerhet som ett viktigt förbättringsområde är de förslag som ges inte anpassade till att styra informationshanteringen i de former, det vill säga i allt högre grad i samverkan mellan olika organisationer, som den idag sker i den svenska sjukvården.

För att uppnå informationssäkerhetsmålet är det enligt MSB nödvändigt att ta fram en nationell modell för styrning av vårdens informationshantering som ser till helheten. I en sådan modell bör det bland annat ingå att beskriva ansvarsförhållandena för de lösningar för informationshantering som ligger

---

[11] 2§ Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården (SOSFS 2008:14)

[12] 2 kap. 9 § förslaget till hälso- och sjukvårdsdatalagen

utanför det de enskilda vårdgivarna har möjlighet att kontrollera men samtidigt är beroende av för att kunna bedriva sin verksamhet. Modellen ska också ge stöd för den strategiska styrningen och prioriteringen, utveckling och förvaltning samt gemensamma regler för informationshanteringen. Med detta som grund ges möjlighet till styrning av informationssäkerhet inom organisationer såväl som i informationsutbytet mellan organisationer och för de tjänster som tas fram på nationell nivå. MSB anser att det finns anledning att som ett första steg ta del av de norska erfarenheterna kring det för vården gemensamma regelverket Normen. En styrmodell av denna typ skulle också kunna överbrygga de skilda förhållanden som finns hos offentliga respektive privata vårdgivare samt även på ett enhetligt sätt att formulera krav riktat mot de många underleverantörer som ingår i vårdens informationshantering.

Ytterligare en faktor, för att kunna införa ett fungerande arbete med informationssäkerhet, är att identifiera de risker som insatserna inom informationssäkerheten syftar till att reducera. Detta perspektiv saknas genomgående i utredningen och trots upprepningen av begreppet informationssäkerhet går det inte att läsa ut vilka informationssäkerhetsrisker som utredningen avser att hantera med sina förslag. MSB menar att är nödvändigt att göra en grundlig analys av de aktuella risker som finns samt även inkludera de risker som kan förutses i en nära framtid. Utan underlag i form av riskanalyser går det inte att definiera det behov av skydd som bör omge vårdens informationshantering. Är inte detta behov identifierat går det inte att föreslå realistiska lösningar och inte heller få en uppfattning om vilka ekonomiska, organisatoriska och regelmässiga förutsättningar som krävs. Ett systematiskt informationssäkerhetsarbete är riskbaserat både för att åtgärder ska kunna styras dit där de gör mest nytta och för att uppnå kostnadseffektivitet. När utredningen vid enstaka tillfällen föreslår en konkret säkerhetshöjande åtgärd, som skydd för uppgifter då de överförs via internet m.m.[13], blir denna åtgärd tagen ur sitt sammanhang eftersom ingen riskanalys genomförts. Detta väcker ett antal frågor. Är denna för vårdgivarna kostnadskrävande åtgärd för det första den mest prioriterade sett ur ett riskperspektiv, för det andra meningsfull om skyddet mot obehörig åtkomst inte är på samma nivå i övriga delar av informationshanteringsprocessen?

Även om en riskanalys saknas går det att hävda att merparten av vårdens informationshantering måste omges med ett utvecklat skydd som motsvarar höga eller mycket höga krav i samtliga de fyra informationssäkerhetsaspekterna konfidentialitet, riktighet, spårbarhet och tillgänglighet. Det måste därför ses som mycket anmärkningsvärt och allvarligt att utredningen istället genom sitt förslag i praktiken förordar en sänkning av kraven i samtliga aspekter. I det följande presenteras kortfattat hur några av förslagen negativt inverkar på säkerheten i olika delar.

---

[13] SOU 2014:23, kapitel 9.2.3

Förslag i utredningen som påverkar konfidentialitet i vårdens informationshantering och därmed patientens integritet

Konfidentialitet inom vården är ett skydd för patientens integritet. Att individer har rätt till autonomi och integritet även då de är patienter har varit en djupt förankrad etisk princip i den svenska vården sedan länge. I praktiken har det inneburit krav på att endast den sjukvårdspersonal som har en direkt patientrelation har rätt att ta del av uppgifter kring patientens vård och behandling. Det etiska ställningstagandet bygger på att tanken att relationen mellan vårdpersonal och patient ska grundas i förtroende så att patienten ska kunna beskriva även känsliga personliga förhållanden utan riskera att dessa sprids utanför den snäva krets som deltar i patientens vård och behandling. Att ha ett minimalistiskt förhållningssätt till åtkomst av känsliga uppgifter är också en grundprincip i exempel personuppgiftslagen. Det finns ett antal andra perspektiv att lägga på integritetsfrågan som till exempel ett genusperspektiv. För många av de kvinnor som utsätts för misshandel och hot är det livsnödvändigt att de kan uppsöka vård utan risk för att uppgifter om till exempel deras vistelseort eller andra förhållanden blir tillgängliga för obehöriga.

Stark åtkomststyrning är inte bara viktig av etiska skäl utan det finns även ett etablerat orsakssamband mellan en tjänst eller organisations förmåga att upprätthålla användarnas integritet och den tillit som organisationen eller tjänsten möter. Tillit är i sin tur en central faktor för att exempelvis en it-tjänst ska fungera på avsett sätt och accepteras av användarna. I ett vårdsystem kan det konkret innebära att vårdpersonal inte vill dokumentera känslig men viktig information om de inte kan lita på att den förtroenderelation de har med patienten upprätthålls. Om detta inte fungerar riskeras informationskvaliteten och i förlängningen patientssäkerheten.

Med detta i åtanke är det anmärkningsvärt att utredningen föreslår ett radikalt paradigmskifte i integritetsfrågan. Från att huvudregeln tidigare varit att patientens information i identifierbart skick ska vara oåtkomlig för alla som inte är direkt inblandade i patientens vård och behandling menar utredningen istället att den som efterfrågar offentligt finansierad vård därmed med automatik har accepterat att vården får sprida och hantera större delen av patientens vårdinformation utan möjlighet för patienten att påverka spridningen.

I kapitel *9.2.5 Ansvar för behörighetstilldelning*[14] förs ett resonemang som inledningsvis tycks syfta till att ha en minimalistisk behörighetssättning men som sedan utmynnar i ett förslag att ta bort de tekniska begränsningarna för åtkomst till patientinformation.

”I verksamheter som hanterar en stor mängd mycket integritetskänsliga uppgifter, som hälso- och sjukvården, ställs stora krav på

[14] SOU 2014:23, s. 184 f

en ändamålsenlig behörighetsstyrning. Även om det vid behörighetsstyrning kan vara svårt att vid varje givet tillfälle uppnå ett exakt förhållande mellan en användares behov och en användares tekniska möjligheter att ta del av uppgifter, måste ambitionen hos den som bedriver verksamheten att komma så nära som möjligt. En del av utmaningen ligger i att det i vissa verksamheter är svårt att förutse vilka individer som en användare kommer att möta i sitt yrke. I vissa delar av hälso- och sjukvården är den osäkerheten ett naturligt inslag som måste vägas in i styrningen av behörigheterna. Det är viktigt att behörigheten inte blir för snäv utan att den är anpassad till de tänkbara behov som finns, så att inte kvaliteten och säkerheten i vården av patienterna riskeras. Dessa svårigheter utgör dock inget skäl för att låta bli att göra de begränsningar av behörigheterna som är motiverade. Sådana uppgifter som en användare inte alls har något behov av ska inte heller vara tekniskt åtkomliga för användaren, dvs. inte ligga inom användarens behörighet.[15]”

Utredningen menar här och i följande resonemang att de normala behörigheterna till vårdinformationssystemen (som i sin tur är kopplade till andra tjänster och system) ska vara mycket vitt satta, i princip ska organisationstillhörighet och roll i vid bemärkelse räcka för att ge åtkomst till helheten. Det innebär att om en läkare eller sjuksköterska är anställd av ett landsting eller annan vårdgivare så kommer hen att få tillgång till samtliga patienter oavsett vårdrelation. Skyddsåtgärderna ska istället för begränsningar i behörigheter bestå i information till personalen samt loggning[16]. Det är här svårt att följa utredningens tankegångar och hur förslaget, som avviker starkt från etablerade metoder för att skydda känslig information, skulle värna patienters integritet. Motsägelsen i att å ena sidan hävda att det inte går att göra fördefinierade begränsningar till vilken information olika typer av roller ska ha åtkomst till och å andra sidan hävda att det skulle vara möjligt att bedriva en systematisk uppföljning av otillåten åtkomst analyseras inte heller i utredningen. Att ha denna öppna tillgång till patienters information inte bara från den egna verksamheten utan även från nationella tjänster och andra vårdgivare men samtidigt hävda att vårdgivaren på ett effektivt sätt ska kunna styra begränsningen enbart via information till personalen förefaller både orealistiskt och ineffektivt. Sammanfört med förslagen på att förändra reglerna för sammanhållen journalföring så att detta kan ske även över huvudmannagränser utan patienten tillfrågas om samtycke[17] och att uppgifter om ordinerade läkemedel samt överkänslighet ”alltid ska finnas tekniskt åtkomliga” leder detta till att mycket litet finns kvar i praktiken av begränsningar. I princip kan stor del av den information som genereras via vårdkontakter vara tillgänglig helt eller i delar för all vårdpersonal i hela landet.

---

[15] SOU 2014:23, s 186

[16] Ibid, s. 187

[17] Ibid, s 371f

Istället för att styra åtkomsten till informationen hyser utredningen alltså en hög tilltro till loggning som säkerhetsåtgärd. Bedömningen att loggning skulle kunna utgöra en begränsning av åtkomst bygger på två logiska felslut. För det första begränsar inte loggning åtkomst utan är en reaktiv åtgärd då en överträdelse redan skett med de skadeverkningar som då kan uppstå. För det andra förutsätter fungerande loggning att det finns mycket tydlig styrning av vem som ska ha åtkomst till vilken information vid vilken tidpunkt. I annat fall ger loggningen inte stöd för att kunna avgöra om åtkomsten varit behörig eller inte. Om en fungerande styrningen finns på plats så finns det ingen anledning att inte tekniskt styra åtkomsten. Ytterligare en central förutsättning för att loggning ska kunna användas på avsett sätt är att det finns rutiner och resurser på plats för att genomföra analys av loggarna. Det är först då loggning blir den efterkontroll som den är avsedd att vara.

De regler som införts i lagförslagets 4 kap. ”en säker och ändamålsenlig hantering av personuppgifter” ger inte stöd för det systematiska arbete med integritetsskydd och informationssäkerhet som är nödvändigt inom hälso- och sjukvården. Det kan istället snarast beskrivas som punktvisa nedslag. Bristande helhetssyn och systematik på detta område skapar, som redogjorts för ovan, brister för både patientsäkerhet och patientintegritet.

Sammantaget menar MSB att utredningens förslag kommer i princip att leda till att endast den patient som har tillräckliga ekonomiska resurser för att själv kunna bekosta privat vård kommer att ha praktisk möjlighet att värna sin integritet. Den patient som är hänvisad till offentligt finansierad vård oavsett om den utförs i offentlig eller privat regi har med utredningens förslag accepterat att informationen exempelvis utan patientens samtycke ingår i en journalhantering över huvudmannagränser. MSB delar experten Maria Bergdahls uppfattning i ett särskilt yttrande vars inledande frågeställningar är följande:

”Vart tog patientens integritetsskydd vägen?
Utredningen har föreslagit så många förenklingar, förtydliganden och förändringar i förhållande till hur patientdatalagen ser ut i dag, att utredningen vill införa en ny lag som ersätter patientdatalagen;
Hälso- och sjukvårdsdatalagen.
Inledningsvis anser jag att det saknas en fullödig analys och beskrivning av förslagens konsekvenser för patienternas integritet. Det är inte helt lätt att ta in det omfattande materialet samt att förstå vad de sammantagna effekterna för patienterna kommer att bli totalt sett. Jag anser därför att det behövs en heltäckande analys som tydliggör hur alla dessa förslag sammantaget kommer att inverka på patienternas integritetsskydd. Behovet av en sådan analys följer också av den rätt till integritetsskydd som var och en är tillförsäkrad gentemot det allmänna i 2 kap. 6 § andra stycket regeringsformen.
Det finns flera förslag där jag ifrågasätter om patientens integritetsskydd har tillvaratagits, men på grund av materialets omfång och tidsbrist har jag valt att inte uttala mig i dessa delar. Jag har i huvudsak inriktat mig på nedanstående förslag:

• Förbättrade möjligheter till direktåtkomst mellan vårdgivare nom en huvudmans ansvarsområde.

• En ny sammanhållen journalföring samt en utvidgad direktåtkomst.

• Ändrade spärrmöjligheter för patienterna.[18]”

En så avgörande förändring av den etiska värdegrunden inom den svenska vården bör, förutom av en konsekvensanalys, även föregås av en bred offentlig diskussion. Så är inte fallet nu, i utredningen ges ingen argumentation för varför värdet av den personliga integriteten i praktiken bedöms vara försumbart. Utredningen skapar istället en motsättning mellan å ena sidan patientsäkerhet och å andra sidan integritet, en motsättning som ska motivera varför det senare värdet ska träda åt sidan. Detta rimmar illa med de intentioner som i andra sammanhang förs fram kring patientens autonomi och valfrihet. Som förslaget är skrivet ges ett tydligt intryck av att utredningen menar att vårdgivarnas hittillsvarande oförmåga att organisatoriskt och tekniskt leva upp till befintliga regler rörande skydd av patientens integritet ska leda till att reglerna förändras och skyddet luckras upp. Rimligare är inriktningen att uppföljningen ska skärpas så att vårdgivarna motiveras att hantera sin information så att både patientsäkerhet och integritet säkerställs. Informationshantering som är utformad så att den både håller hög tillgänglighet och god konfidentialitet finns inom andra branscher. Tekniken utgör inte något hinder för att utveckla säkra system och MSB menar därför att ambitionen med nödvändighet måste vara att göra detta även inom vården.

Förslag i utredningen som påverkar riktighet och spårbarhet i vårdens informationshantering

Riktighet och spårbarhet är två andra aspekter av informationssäkerhet som här kommer att behandlas under samma rubrik då de förutsätter likartade typer av säkerhetsåtgärder. Utredningens förslag inverkar negativt även på dessa aspekter. Ett exempel på hur utredningen bortser från behovet av riktighet och spårbarhet är förslaget på att ta bort kravet på signering i vårddokumentationen. Signering är en etablerad metod för att säkerställa riktighet och spårbarhet. Riktighet är också av största betydelse för patientssäkerheten, är inte informationen som föranleder beslut kring vård och behandling korrekt är det en uppenbar risk att patienten felbehandlas vilket innebär en stor risk för liv och hälsa. Att patienter felbehandlas på grund av felaktig information sker redan idag, tyvärr i vissa fall med dödlig utgång, och det är därför befogat att höja kraven på informationskvalitet istället att för som i utredningens förslag – att sänka dem. Utredningen ger också en beskrivning där den administrativa bördan ställs mot signeringens funktion som exempelvis i följande stycke:

”Det nämns att flera landstingsföreträdare tvivlar på om signeringskravet verkligen bidrar till en högre patientsäkerhet eftersom de är tveksamma till om läkare i detalj går igenom sina anteckningar vid signering.[19]”

---

[18] SOU 2014:23, sidan 1219

[19] SOU 2014:23, s 117

Detta är en försåtlig problemformulering där utredningen tycks hämta stöd från sjukvårdshuvudmännen. MSB menar dock att det inte är själva aktiviteten att signera som tar tid utan att gå igenom information och kvalitetssäkra den vilket signeringen är ett intyg på. Utredningen beskriver på ett övergripande sätt att vårdgivaren fortfarande har ansvar för att riktighet upprätthålls i vårddokumentationen men anger inte på något sätt hur detta ska gå till och vilka metoder som bör tillämpas. Det framgår indirekt av förslaget att information ska verifieras enbart genom att vårdpersonal tar del av den på skärmen vilket förefaller som en mycket olämplig metod om avsikten är befrämja krav på riktighet. Krav på riktighet förutsätter om de ska uppfyllas, inom alla etablerade metoder, en aktiv verifiering av en eller flera behöriga användare. Även här argumenterar utredningen för att den enskilde vårdgivaren självständigt ska ta ställning till vilken signering som ska förekomma i den egna verksamheten, det vill säga vilken informationskvalitet som ska finnas i olika informationsmängder. Detta trots att informationen som tidigare framhållits inte används enbart inom den egna verksamheten. MSB menar som tidigare anförts att dessa frågor inte kan lösas på ett så fragmentiserande sätt som föreslås utan att det måste finnas en tydlig nationell styrning.

Kraven på spårbarhet måste ses som en viktig aspekt i vårdens informationshantering generellt och är än mer oundgängligt inom områden som exempelvis läkemedelshantering. Utredningens förslag på att minska kraven på spårbarhet strider inte enbart mot den allmänna utvecklingen inom it-området där denna aspekt blivit allt mer prioriterad utan även mot de initiativ regeringen tagit då även vårdinformationssystem blivit definierade som medicin-teknisk utrustning.

För vårdpersonalen som dokumenterar innebär förslaget att ta bort signering också en avsevärt försämrad rättsäkerhet. De legitimerade yrkesgrupperna har ett starkt personligt ansvar för att vård och behandling genomförs på ett korrekt sätt. Att inte ha hög spårbarhet i dokumentationen kommer att leda till situationer där det inte går att med säkerhet fastställa ansvar och vilken information som legat till grund för en behandling som orsakat patientskador. Ett konkret exempel där vårdpersonal upplever spårbarhetens betydelse är rutinen kring provsvar. Om inte den som är ansvarig för en vårdinsats kan lita på en säker spårbarhet i vilka provsvar som legat till grund för behandlingen hamnar de i en ansvarsmässigt mycket osäker situation. Det finns följaktligen ett mycket starkt gemensamt intresse för patienter och vårdpersonal att spårbarheten kan hållas på en hög nivå.

Förslag i utredningen som påverkar tillgänglighet i vårdens informationshantering

Utredningens intention är att lämna förslag som ska leda till tillgängligheten i vårdens informationshantering ökar. Ovan har redan den bristande kvalitet som MSB menar skulle bli följden av utredningens förslag ifrågasatts men den bristande spårbarheten skulle även leda till svårigheter att identifiera rätt information. Ett problem som är lätt att identifiera är svårigheten att kunna

säkerställa att det är den senaste och därmed korrekta versionen av en viss informationsmängd, exempelvis ett provsvar eller en ordination, som används. Därmed föreligger stora risker för att inte rätt informationen de facto är tillgänglig.

Även bortsett från kvalitetsaspekten anser inte MSB att utredningens förslag gagnar en långsiktigt säker tillgänglighet i vården.

Utredningens huvudförslag för att förbättra tillgängligheten är att reducera åtkomstbegränsningar. MSB anser för det första att det inte finns en ofrånkomlig motsättning mellan bra åtkomstskydd och god tillgänglighet. För det andra krävs organisationsöverskridande insatser för att kunna upprätthålla vårdens informationsflöden eftersom alla vårdgivare dag är knutna till en allt mer gemensam informationsinfrastruktur. Denna frågeställning beaktas inte över huvud taget av utredningen som riktar alla sina regleringsförslag till den enskilda vårdgivaren. I den rådande utvecklingen som gör vårdens informationsinfrastruktur både mer koncentrerad och mer fragmentiserad har den enskilda vårdgivaren små möjligheter säkerställa rätt tillgänglighet till nödvändig information enbart genom åtgärder i den egna informationshanteringen. Beroendet till bland annat nationella tjänster och andra vårdgivares tjänster är helt avgörande för en enskild organisations interna informationshantering. Vidare är det beklagligt att utredningen förutsätter ett ständigt normalläge och inte diskuterar frågan hur rätt information ska finnas på rätt plats i rätt tid även då större och mindre störningar inträffar. I och med vårdens samhällviktiga roll måste informationshanteringen vara utformad även för ett krisläge vilket kräver särskilda insatser som inte går att vidta först när krisen är ett faktum. MSB kan inte se att utredningen beaktat de skyldigheter som sjukvårdshuvudmän och vårdgivare har i ett krishanteringsperspektiv.

I detta ärende har överdirektör Nils Svartz beslutat. Fia Ewald har varit föredragande. I den slutliga handläggningen har också chefsjuristen Key Hedström, avdelningschefen Cecilia Nyström, verksamhetsområdeschefen Richard Oehme och juristen Helena Andersson deltagit.

Nils Svartz

Fia Ewald

Kopia: Justitiedepartementet/SSK