



# Nationell Arkitektur – Patientdatalagens konsekvenser

## Sammanfattning

Detta dokument redogör för IT-konsekvenser för *samverkan* mellan olika vård- och omsorgsgivare utgående från förslaget till ny patientdatalag. Dokumentet beskriver *inte* verksamhetsmässiga konsekvenser eller konsekvenser för det *interna* IT-stödet för vård- och omsorgsgivare, om det inte har betydelse för samverkan.

Primära målgrupper för detta dokument är:

- Sveriges vård och omsorg,
- leverantörer samt
- nationella projekt inom ramen för realiserandet av den nationella IT-strategin för vård och omsorg.

Sammantaget kan det sägas att förslaget till ny patientdatalag ställer mycket stora krav på organisation, processer och IT-stöd för vård- och omsorgsgivare i Sverige. Till skillnad mot förut kommer lagen att ställa stora krav på effektiv samverkan och på att medborgare och patienter sätts i fokus.

Ur ett IT-perspektiv kommer säkerhet och personlig integritet att stå i centrum. Avancerade nationella funktioner för loggning, behörighets- och åtkomstkontroll är ett måste. Vidare måste existerande lokala och regionala säkerhetslösningar kunna samverka med framtida nationella lösningar.

Vidare är hantering av samtycken och spärrar av journalinformation på tvärs över vårdgränser en stor utmaning, för att inte tala om de fall där patienten vill kunna ta tillbaka ett tidigare samtycke till delning av journalinformation.

Nya journal- och patientadministrativa system som medger samverkan lokal, regionalt och nationellt måste tas fram parallellt med att existerande IT-stöd måste leva vidare i en övergångsfas, som kan bli utsträckt i tiden beroende på olika lokala förutsättningar.

För att klara av allt detta måste information i journaler och andra system normeras, beskrivas, klassificeras och metamärkas för att överhuvudtaget möjliggöra informationsutbyte och samverkan, med bibehållen integritet och säkerhet för individen.

Dessa är bara några få av de utmaningar som kan målas upp för de organisationer som ska realisera lagens intentioner.

## Utestående frågor och fortsatta aktiviteter

Det finns en del utestående frågor som har identifierats under arbetets gång och som inte har kunnat behandlas inom ramen för projektet Nationell Arkitektur – Regler, Riktlinjer och Rekommendationer (NARRR). För vissa frågor pågår utredningsarbete på bland annat Socialstyrelsen. Nedan redogörs för några av frågorna.

1. Informationsklassificering eller inte? Är informationsklassificering en förutsättning för att sammanhållen journal ska fungera? Om patienten i samtycke ”klassar” informationen, vad är det han eller hon klassar? Hela journalen eller delar av journalen? Är det istället en fråga om metaklassning?
2. Samtycke och spärrar som är begränsat till vårdenhet eller vårdprocess hos samma vårdgivare. Hur skulle detta kunna fungera i praktiken? Innebär detta att en nationell samverkansarkitektur SKA klara av även samverkan *inom* en vårdgivare? Inom NARRR är det samverkan *mellan* vårdgivare som har diskuterats.
3. Fundamentala begrepp i sammanhanget är vårdenhet, vårdprocess, vårdåtagande, vårdrelation m.m. Begreppsstrukturen och definitioner har stor betydelse för konsekvensbeskrivningar av lagen och här bör ett tydligt ansvar finnas för att göra denna begreppsanalys.
4. Nationell befolknings- och ID-tjänst, behövs en sådan tjänst i nationell arkitektur och vems är ansvaret att ta fram sådana tjänster?
5. Kan person spärra information när som helst eller bara i samband med ”vårdepisod”? Kan man spärra för vilken vårdepisod som helst, även historiska vårdepisoder.
6. Vad händer med utlämnat material som sedan spärras inom sammanhållen journal? Ska man spärra denna information på samma sätt som vid rättning och utplåning, för att markera en spärr?
7. När patientdatalagen är beslutat och föreskrifter framtagna så behöver detta dokument omgående omarbetas efter slutliga krav och där bör det klart och tydligt framgå vilka som är odiskutabla åtgärder som måste till och som är tidskritiska.
8. Detta dokument belyser perspektiv av *samverkan* där patientdatalagen kan få konsekvenser. Någon analys specifikt ur ett journalsystemperspektiv och en vårdgivares interna konsekvenser har alltså inte gjorts om det inte påverkar just *samverkan*. Det finns med andra ord ytterligare paragrafer och interna konsekvenser som påverkar vårdgivares egna journalsystem som skulle kunna analyseras.

Denna rapport är en första utgåva, kallad Revision A, (REV A). Vartefter frågor utreds och patientdatalagen och dess föreskrifter utformas, kommer konsekvenserna som beskrivs i denna rapport att behöva ses över. Det är därför lämpligt att en ny version tas fram (REV B) under 2008. Fram till dess kan synpunkter och kommentarer lämnas till Sara Meunier, sara.meunier@carelink.se.

## Förord

Denna rapport är ett resultat av ett deluppdrag inom ramen för projektet Nationell Arkitektur - Regler, Riktlinjer och Rekommendationer (NARRR) Etapp 2 som drivs av Carelink på uppdrag av beställarorganisationen. Deluppdraget var "Beskriv hur patientdatalagens konsekvenser påverkar den nationella arkitekturen". Uppdraget utfördes av Pär Lannerö och Kurt Helenelund på Metamatrix//Interfolio i samarbete med NARRR-projektgrupp på uppdrag av projektledare Sara Meunier, Carelink AB.

Metamatrix//Interfolio gjorde en första genomgång av den föreslagna patientdatalagen, samt de föreslagna förändringarna i fyra andra lagar, som patientdatautredningen publicerat i sitt betänkande "Patientdatalag" (SOU 2006:82). Därefter bearbetades rapporten av följande personer:

Anders Norr, LiÖ

Jan Edquist, SLL

Kurt Helenelund, Metamatrix

Lennart Eriksson, SLL

Per-Arne Lundgren, Region Skåne

Per Torlöf, Region Skåne

Qemajl Imeri, SLL

Sara Meunier, Carelink

Tommy Rigo, VGR

Ulf Palmgren, SLL

Synpunkter har även inlämnats på preliminära utgåvor av rapporten av NARRRs ordinarie projektgrupp, NARRRs styrgrupp, Carelink, NI-projektets (Nationell Informationsstruktur) arbetsgrupp för informationssäkerhet på Socialstyrelsen m.fl. och arbetats in i rapporten.

För varje paragraf som bedöms få konsekvenser för IT-arkitekturen för samverkan inom vård och omsorg, redovisas kortfattat varje sådan konsekvens. För att tydliggöra vilka delar som åsyftas citeras relevanta delar av paragraferna. Dessutom görs en uppräkningslista av centrala begrepp som förekommer i lagförslagets paragrafer, samt begrepp som bedöms behövas finnas med i IT-arkitekturen. De olika begreppen kan med fördel användas som sökbegrepp för den som önskar betrakta konsekvenserna ur olika perspektiv.

Observera att fokus inte har varit på konsekvenser av *förändringarna* av lagstiftningen, utan konsekvenser av de lydelse som redovisas i SOU 2006:82. Det innebär att vissa av de konsekvenser som beskrivs är självklarheter, som sedan länge varit gällande förutsättningar och därmed redan tillämpas inom vården. Vissa andra konsekvenser innebär dock nyheter, och kommer att kräva att IT-system och arkitekturer åtgärdas.

När siduppgift anges utan att publikation nämns är det den tryckta versionen av "Patientdatalag" (SOU 2006:82), från Fritzes förlag 2006, som avses. Den finns tillgänglig som PDF-fil att ladda ner på följande webbadress:

<http://www.regeringen.se/sb/d/6150/a/71234>

Även nya lydelse i sekretesslagen (1980:100), lagen (2005:225) om rättsintyg i anledning av brott, lagen (2002:297) om biobanker i hälso- och sjukvården m.m. och lagen (2001:499) om omskärelse av pojkar som ingick i den tryckta versionen av patientdatalag och har analyserats kort ur ett samverkansperspektiv.

Stockholm 2007-11-30

Sara Meunier, projektledare NARRR

## Innehållsförteckning

Sammanfattning .....	1
Förord.....	4
Läsanvisningar .....	6
Konsekvenser av föreslagen patientdatalag .....	7
Konsekvenser av föreslagna nya lydelse i sekretesslagen (1980:100).....	35
Konsekvenser av föreslagen ny lydelse i lagen (2001:499) om omskärelse av pojkar .....	38
Konsekvenser av föreslagen ny lydelse i lagen (2002:297) om biobanker i hälso- och sjukvården m.m. ....	39
Konsekvenser av föreslagen ny lydelse i lagen (2005:225) om rättsintyg i anledning av brott .....	40

## Läsanvisningar

Dokumentet är strukturerat efter förslaget till ny Patientdatalag (SOU 2006:82) inklusive hänvisning till paragraf och i tillämpliga fall till sidnummer i förarbetet.

Strukturen är följande:

**Paragraf:** << paragraf >>

**Lydelse:** << citat >>

**Konsekvenser:** << beskrivning av möjliga konsekvenser för IT-arkitekturen och i vissa fall andra konsekvenser >>

**Kommentarer:** << kommentarer med i tillämpliga fall hänvisning förarbetet eller referenser till andra delar >>

**Begrepp:** << utvalda centrala begrepp ur lagtext och förarbete som inte är allmänna begrepp. Begreppen och dess definitioner kan ha konsekvenser för arkitektur och IT. Vissa begrepp finns redan definierade i Socialstyrelsens termbank, för några kan definitionen behöva förtydligas. >>

**Realisering:** << övergripande lista på befintliga, tänkbara och nödvändiga tjänster som kan behövas för att tillämpa lagtexten och lydelsen i förarbetet. Tjänster kan vara tjänster i en verksamhet eller tjänster som kan realiseras m.h.a. ett IT-stöd. Existerande realiseringar kan refereras. >>

## Konsekvenser av föreslagen patientdatalag

<b>Paragraf:</b>	<b>1kap. §2</b>
<b>Lydelse:</b>	"Personuppgifter skall utformas och i övrigt behandlas så att patienters och övriga registrerades integritet respekteras.  Dokumenterade personuppgifter skall hanteras och förvaras så att obehöriga inte får tillgång till dem."
<b>Konsekvenser:</b>	1.2.1. Arkitekturen bör utformas på ett sådant sätt att det går att överblicka vid vilka situationer personuppgifter blir tillgängliga, och för vem. Det kan vara exempelvis vid skärmvisning på mottagningsrum, vid säkerhetskopiering i driftcentral, vid elektronisk kontakt med andra system, eller vid pappersinsamling i anslutning till skrivare hos vårdgivare.  Nationella regler behövs för åtkomst och skydd av information vid samverkan.
<b>Kommentarer:</b>	1.2.K1. Patientdatakommittén skriver själva, på sidan 516 följande om säkerhetsrutiner mm: ”Det medför att höga krav måste ställas på de säkerhetsåtgärder som skall vidtas för att skydda personuppgifterna och att en sårbarhetsanalys måste göras för att identifiera riskerna. Hög kvalitet på tekniska skyddsåtgärder såsom säkra funktioner för behörighetskontroll, loggning, kommunikation, säkerhetskopiering m.m. måste förutsättas. Minst lika viktigt är administrativa rutiner för hanteringen av personuppgifter och att personalen kontinuerligt utbildas och informeras om säkerhetsfrågor. ”
<b>Begrepp:</b>	patient, övrig registrerad, integritet, obehörig, risker, sårbarhetsanalys, loggning, kommunikation, säkerhetskopiering, rutiner
<b>Realisering:</b>	Journalföring, behörighetskontroll (BIF-åtkomstkontroll), integritetsloggning (BIF-loggning), analys av loggar (BIF-logganalys), utbildning, utveckling av processer och rutiner, säkerhetskopiering, gallring, arkivering.  För BIF-åtkomstkontroll kan det vara nödvändigt att hitta vissa gemensamma nationella modeller för åtkomstregler.

<b>Paragraf:</b>	<b>1kap. §3</b>
<b>Lydelse:</b>	Paragrafen definierar centrala begrepp. Bl.a.: "Journalhandling: Framställning i skrift eller bild samt upptagning som kan läsas, avlyssnas eller på annat sätt uppfattas endast med tekniskt hjälpmedel"
<b>Konsekvenser:</b>	1.3.1. IT-arkitekturen ska innehålla gränssnitt som stödjer olika överenskomna format och protokoll för olika informationsinnehåll i informationssamverkan. Hantering av avvikelser och fel i samverkan ska också slås fast.
<b>Begrepp:</b>	journalhandling, sammanhållen journalföring, direktåtkomst, patientjournal, hälso- och sjukvård, vård, vårdgivare
<b>Realisering:</b>	Standardiserade strukturer för informationsutbyte (RIV). Metaklassning av journalinformation kanske måste finnas.
<b>Paragraf:</b>	<b>2kap. §2</b>
<b>Lydelse:</b>	”Behandling av personuppgifter som är tillåten enligt denna lag får utföras även om den enskilde motsätter sig den. Det gäller dock inte om annat framgår av denna lag, annan lag eller förordning.  I 4 kap. 4 §, 6 kap. och 7 kap. 2 § finns bestämmelser om att en personuppgiftsbehandling inte är tillåten om patienten motsätter sig den eller inte samtycker till den.”
<b>Konsekvenser:</b>	2.2.1. Det måste finnas rutiner för att avgöra om patient motsätter sig personuppgiftsbehandling. Denna konsekvens specificeras närmare i 4 kap. 4 §, 6 kap. och 7 kap. 2 §.
<b>Begrepp:</b>	behandling av personuppgifter, samtycke, motsätter sig, förordning
<b>Realisering:</b>	Kontroll av samtycke och spärrar samt loggning måste finnas (BIF-samtycke, BIF-loggning). Det är det lokala systemet som ska registrera samtycket eller spärr samt att ange att spärr finns.

<b>Paragraf:</b>	<b>2kap. §6</b>
<b>Lydelse:</b>	"En vårdgivare är personuppgiftsansvarig för den behandling av personuppgifter som den utför. I landsting och kommun är varje myndighet som bedriver hälso- och sjukvård personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför.  I 6 och 7 kap. finns särskilda bestämmelser om personuppgiftsansvar."
<b>Konsekvenser:</b>	2.6.1. Regeringen har, enligt s.338, i proposition 2002/03:135) skrivit att "fördelning av personuppgiftsansvar förutsätter naturligtvis att det går att genom loggning spåra vilken myndighet som företagit en viss behandling". I de fall personuppgiftsansvaret är delat måste alltså all behandling loggas.
<b>Kommentarer:</b>	2.6.K1. Att loggning bör ske följer även av konsekvenserna 3.3.1 och 4.3.1.
<b>Begrepp:</b>	personuppgiftsansvar, personuppgiftsansvarig, myndighet
<b>Realisering:</b>	Behörighetskontroll (BIF-åtkomstkontroll), loggning (BIF-loggning), analys av loggar (BIF-logganalys).

<b>Paragraf:</b>	<b>2kap. §7</b>
<b>Lydelse:</b>	"Endast sådana personuppgifter som behövs för ändamål som anges i 4§ får behandlas. Även en vårdgivare som inte är myndighet får behandla sådana uppgifter om lagöverträdelser m.m. som avses i 21 § personuppgiftslagen (1998:204)."
<b>Kommentarer:</b>	<p>2.7.K1. Det är tänkbart att i ett IT-system kräva att ändamål vid all behandling av personuppgifter anges (och loggas), men det är som sagt bara en tänkbar – inte nödvändig konsekvens av lagförslaget. Se s.420. Ändamålet med behandlingen ska också loggas om det går utanför verksamhetsuppdraget (vårdokumentation, administration, verksamhetsutveckling, kvalitetssäkring, uppföljning, utvärdering, tillsyn, kvalitetsregister).</p> <p>2.7.K2 Tjänster och gränssnitt som realiserar informationsutbyte får inte innehålla personuppgifter som inte stämmer överens med ändamålet.</p> <p>2.7.K3. Användandet av fritext i informationsutbytet bör analyseras vidare i arbetet framöver.</p>
<b>Begrepp:</b>	uppgift om lagöverträdelse
<b>Realisering:</b>	Gemensamma nationella informationsstrukturer ska finnas (TIS / RIV). Loggning (BIF-loggning), analys av loggar (BIF-logganalys).

<b>Paragraf:</b>	<b>3kap. §2</b>
<b>Lydelse:</b>	"Skyldig att föra patientjournal är.... 2. Den som, utan att ha legitimation för yrket, utför arbetsuppgifter..."
<b>Konsekvenser:</b>	3.2.1. Journalsystem och liknande kan inte bygga behörighetssystem uteslutande på information om vem som är legitimerad läkare/ssk osv. Enligt s.161 är det inte heller endast anställda som för anteckningar i journal, utan även exempelvis studenter. Detta bör också beaktas vid utformning av behörighetssystem. HSA måste kunna hantera olika yrkeskategorier.
<b>Begrepp:</b>	legitimation
<b>Realisering:</b>	Katalog över vård- och omsorgspersonal, roller, yrkeskategorier, yrkestitlar, vård- och omsorgsgivare (HSA-katalog).  Behörighetstkontroll (BIF-åtkomstkontroll), loggning (BIF-loggning), analys av loggar (BIF-logganalys).
<b>Paragraf:</b>	<b>3kap. §3</b>
<b>Lydelse:</b>	"Den som för patientjournal svarar för sina uppgifter i journalen"
<b>Konsekvenser:</b>	3.3.1. Journalsystem bör registrera information om vem som för patientjournal.  3.3.2 I allt informationsutbyte bör det framgå vem som svarar för uppgifterna i journalen.
<b>Kommentarer:</b>	3.2.K1. Kan synas självklart, men är inte desto mindre viktigt. Kravet specificeras ytterligare i konsekvens 2.6.2.
<b>Realisering:</b>	Informationsstrukturen i informationsutbyte ska innehålla referens till den som svara för uppgifterna (TIS / RIV). Behörighetstkontroll (BIF-åtkomstkontroll), loggning (BIF-loggning), analys av loggar (BIF-logganalys). Historik i HSA nödvändig.

<b>Paragraf:</b>	<b>3kap. §5</b>
<b>Lydelse:</b>	"En patientjournal skall innehålla de uppgifter som behövs för en god och säker vård av patienten.  Om uppgifterna föreligger, skall en patientjournal alltid innehålla 1. uppgift om patientens identitet, 2. väsentliga uppgifter om bakgrunden till vården, 3. uppgift om ställd diagnos och anledning till mera betydande åtgärder, 4. väsentliga uppgifter om vidtagna och planerade åtgärder, och 5. uppgift om den information som lämnats till patienten och om de ställningstaganden som gjorts om val av behandlingsalternativ och om möjligheten till en förnyad medicinsk bedömning. Patientjournalen skall vidare innehålla uppgift om vem som har gjort en viss anteckning i journalen och när anteckningen gjordes."
<b>Konsekvenser:</b>	3.5.1. Journalsystem måste kunna hantera alla de delar som räknas upp i paragrafen.  3.5.2 I informationsutbytet ska det vara möjligt att utbyta den information som anges
<b>Begrepp:</b>	patientjournal, identitet
<b>Realisering:</b>	Informationsutbytesmodeller (TIS / RIV). Behörighetstkontroll (BIF-åtkomstkontroll), loggning (BIF-loggning), analys av loggar (BIF-logganalys).
<b>Paragraf:</b>	<b>3kap. §10</b>
<b>Lydelse:</b>	"Om en journalhandling eller en avskrift eller kopia av handlingen har lämnats ut till någon, skall det dokumenteras i patientjournalen vem som har fått handlingen, avskriften eller kopian och när denna har lämnats ut. Detta gäller dock inte utlämnande genom direktåtkomst."
<b>Konsekvenser:</b>	3.10.1. Journalsystem ska kunna hantera information om vem som har fått handling/avskrift/kopia och när.  3.10.2 Regler för vad som ska dokumenteras och hur utlämnandet ska ske bör tas fram.
<b>Begrepp:</b>	kopia, journalhandling, direktåtkomst
<b>Realisering:</b>	Loggning (BIF-loggning), analys av loggar (BIF-logganalys), möjliggöra utlämning av information (BIF- utlämnande tjänst), besked om utlämning (BIF-notifiering). Kan BIF-loggning hantera loggning av utskrift på papper?

<b>Paragraf:</b>	<b>3kap. §11</b>
<b>Lydelse:</b>	"Regeringen, eller den myndighet som regeringen bestämmer, får föreskriva undantag från bestämmelsen i 5 § andra stycket 1 såvitt gäller provtagning för viss sjukdom och från bestämmelsen om signeringskrav i 9 §.  Regeringen, eller den myndighet som regeringen bestämmer, får också meddela ytterligare föreskrifter om en journalhandlings innehåll och utformning."
<b>Konsekvenser:</b>	3.11.1. Journalsystem ska (i den utsträckning de används för hantering som berörs av undantag) kunna hantera journalanteckning även i avsaknad av patientens identitet, eller annan avvikelse gällande innehåll. Även ännu icke identifierade patienter måste kunna hanteras (okända eller medvetet anonyma).
<b>Följdkonsekvenser:</b>	3.11.1.F1. Meddelandeformat (schema eller liknande) som används för interoperabilitet mellan olika journalsystem måste kunna utformas för att hantera undantag. Antingen i form av särskilda meddelandeformat eller i form av att generella meddelandeformat är flexibla.  3.1.11.F2 Reservnummer måste kunna hanteras. Det ska vidare vara möjligt att slå samman information som ligger under olika nummer.
<b>Begrepp:</b>	journalhandling, signering
<b>Realisering:</b>	Journalföring och med signering av hela eller delar av informationen. Journalföring med vissa nationella föreskrivna standarder för hantering av identiteter och signeringar. Nationell befolknings- och idtjänst?

<b>Paragraf:</b>	<b>3kap. §12</b>
<b>Lydelse:</b>	"De journalhandlingar som upprättas inom hälso- och sjukvården skall vara skrivna på svenska språket, vara tydligt utformade och så långt möjligt förståeliga för patienten.  Regeringen, eller den myndighet som regeringen bestämmer, får föreskriva att en sådan journalhandling får vara skriven på ett annat språk än svenska."
<b>Konsekvenser:</b>	<ul style="list-style-type: none"><li>3.12.1. Teckenkod lämplig för hantering av svensk text (t.ex. ISO-8859-1 eller UTF-8) måste kunna hanteras av alla journalsystem.</li><li>3.12.2. Presentation (utskriftsmallar, skärmvisningssidor etc.) av journalinnehåll måste anpassas efter patientens förmåga att förstå.</li><li>3.12.3 System får inte vara fullständigt låsta på att endast hantera svensk text. Även norska, danska och engelska kan förekomma.</li><li>3.12.4 Information i journalen eller andra dokument bör undvika att använda koder eller andra förkortning som inte kan förstås av patienten.</li></ul>
<b>Begrepp:</b>	journalhandling
<b>Realisering:</b>	Journalföring och som möjligen ska kunna hantera flera teckenkoder och flera språk. Kan behöva ersättning eller konvertering av vissa medicinska koder eller förkortningar. Kopplingar till medicinskt lexikon kanske skulle vara möjligt.

<b>Paragraf:</b>	<b>3kap. §13</b>
<b>Lydelse:</b>	"Uppgifter i en journalhandling får inte utplånas eller göras oläsliga i andra fall än som avses i 8 kap. 3 §.  Vid rättelse av en felaktighet skall det anges när rättelsen har skett och vem som har gjort den. "
<b>Konsekvenser:</b>	3.13.1. Journalsystem måste ha fullgott skydd mot avsiktlig eller oavsiktlig radering av data. 3.13.2. Journalsystem ska kunna hantera information om att rättelse skett, när den skett och av vem. Se vidare konsekvenser av 8kap. 6§. Nationella anvisningar för hur rättelser visas bör tas fram.
<b>Kommentarer:</b>	3.13.K1 Ett sätt att skydda sig mot oavsiktlig radering är att raderingsfunktion i journalsystem ges en icke framträdande position. Ett sätt att skydda sig mot oavsiktlig radering är att säkerhetskopiering sker regelbundet och enligt väl utarbetade rutiner. Självklarheter, men icke desto mindre viktiga delar av en IT-arkitektur. Från ett verksamhetsperspektiv är det dock ok att ändra i journalanteckningen så länge den ej är signerad. Att ändra i en signerad journal bör istället kunna medföra att originalet sparas och en dubblett skapas där ändringarna införs. 3.13.K2 På s.274 förs ett resonemang om i vilka fall skrivfel kan rättas utan att uppgiften i journalen skall anses upprättad. Socialstyrelsen anser sig ha möjligheter att ta fram föreskrifter och allmänna råd i dessa frågor. Sådana föreskrifter torde få vissa mindre arkitektur-konsekvenser.
<b>Begrepp:</b>	utplånas, rättelse
<b>Realisering:</b>	Journalföring med åtkomstkontroll och skydd för avsiktlig och oavsiktlig felaktig hantering eller handhavande. Säkerhetskopiering och återställning av information. Utveckling av processer och rutiner för drift av system. Journalsystem med journalanteckningar med full spårbarhet.

<b>Paragraf:</b>	<b>3kap. §15</b>
<b>Lydelse:</b>	"Den som enligt 2 § är skyldig att föra patientjournal skall på begäran av patienten utfärda intyg om vården."
<b>Konsekvenser:</b>	3.15.1. Det bör finnas rutiner för utfärdande av intyg. Dessa rutiner kan, men behöver inte nödvändigtvis påverka arkitekturen för informationssystemen.
<b>Kommentarer:</b>	3.15.K1. För att spara tid, t.ex. vid utfärdande av sådana intyg som i Ds 2005:13 (se s.257) föreslås bli ett prioriterat alternativ till journalutdrag till försäkringsbolag, är det sannolikt lämpligt att informationssystem utformas för att enkelt kunna producera intyg.
<b>Begrepp:</b>	intyg, patientjournal, patient
<b>Realisering:</b>	Journalföring med inbyggda tjänster för skapande av intyg.
<b>Paragraf:</b>	<b>3kap. §16</b>
<b>Lydelse:</b>	"En journalhandling skall bevaras minst tre år efter det att den sista uppgiften fördes in i handlingen. Regeringen, eller den myndighet som regeringen bestämmer, får föreskriva att vissa slags journalhandlingar skall bevaras minst tio år.  Om bevarande av journalhandlingar som tagits om hand efter beslut av Socialstyrelsen finns det särskilda föreskrifter i 9 kap. 4 §. I lag finns, för vissa fall, regler om att journalhandlingar skall bevaras under en längre tid än minst tre år."
<b>Konsekvenser:</b>	3.16.1. Journalsystem måste kunna lagra journalhandlingar minst tre år, alternativt överlämna till annat system för lagring. 3.16.2. Journalsystem måste lagra datum för varje införd uppgifts införande, så att det vid gallring och liknande går att kontrollera att alla handlingar bevaras tillräckligt länge.
<b>Kommentarer:</b>	3.16.K1. Från beredningsarbetet har det föreslagits förändring avseende bevaringstiden för journalhandling, den tiden föreslås blir minst 10 år.
<b>Begrepp:</b>	bevarande, gallring, journalhandling, omhändertagande
<b>Realisering:</b>	Journalföring med gallringsmöjligheter som är regelstyrd både på tid och innehåll. Skyddade tids och datumstämplat på registrerade uppgifter. Utveckling av gallringsrutiner. Ett flertal utredningar kring långtidsarkivering av journal finns, dessutom direkt applicerade försök i SLL (e-arkiv)

<b>Paragraf:</b>	<b>3kap. §17</b>
<b>Lydelse:</b>	"För journalhandlingar som utgör allmän handling gäller, med de undantag som följer av 16 §, arkivlagen (1990:782) samt de bestämmelser som meddelas med stöd av arkivlagen."
<b>Kommentarer:</b>	<p>3.17.K1. Eventuella konsekvenser av arkivlagen. Redovisas inte närmare här.</p> <p>3.17.K2. På s.344 anges att det är ”bra om det framgår genom en uppgift i ett system för sammanhållen journalföring att det finns arkiverade journaler”. Kommentaren förekommer i ett resonemang om vad som händer när en vårdgivare uppgår i en annan eller upphör. Om denna rekommendation ska följas bör journalsystem kunna hantera information om förekomst av arkiverad journal.</p> <p>3.17.K3. På s.348 anges att ”journalhandling eller annan handling bör alltså bara bevaras och bilda arkiv hos en myndighet eller en privat vårdgivare”. Principen är alltså att referera snarare än kopiera. Kopieras handling uppstår nämligen arkivhandling även hos den mottagande vårdgivaren (s.350). För om möjligt undvika kopiering bör system för sammanhållen journalföring utformas på så vis att det är väldigt enkelt att komma åt originalhandlingar lagrade hos andra vårdgivare. Ett förslag på hur detta skulle kunna åstadkommas är att införa klickbara länkar i journalhandlingar. En journalhandling skulle med hjälp av en klickbar länk kunna hänvisa till journalhandling hos annan vårdgivare. Detta torde inte utgöra något problem i förhållande till spärrade handlingar, med tanke på att det får finnas information om att spärrad journalhandling existerar. Dock blir det komplicerat om länkens kontext avslöjar eller antyder vilken information som finns i den länkade journalhandlingen. Även så kallad inline-länkning skulle kunna vara ett sätt att undvika onödig kopiering. Inline-länkning betyder att innehållet i det länkade dokumentet visas i anslutning till länken, dock utan att kopieras till mottagande vårdgivares system.</p>
<b>Begrepp:</b>	-
<b>Realisering:</b>	Journal och dokument bör lagras på format och media som lämpar sig för arkivering. Allra minst måste export (avställning) kunna ske till lämpligt media på föreskrivet format. Journal och med spårbarhet på innehåll. Helst bör gemensamma standarder för elektronisk arkivering användas (OAIS, EAD, etc...). Gemensamma arkivbildningsplaner torde vara en fördel.

<b>Paragraf:</b>	<b>3kap. §18</b>
<b>Lydelse:</b>	"Regeringen får meddela särskilda föreskrifter om patientjournaler i krig, vid krigsfara eller under sådana utomordentliga förhållanden som är föranledda av att det är krig utanför Sveriges gränser eller av att Sverige har varit i krig eller krigsfara."
<b>Kommentarer:</b>	3.18.K1. Det är svårt att förutsäga på vilket sätt en speciell reglering i krig kan se ut, men det är rimligt att kräva att offentlig sektor på något sätt har tillgång till källkod eller gränssnitt för att i händelse av krig kunna anpassa systemen till då rådande omständigheter. Nationell redundans med reservsystem kanske kan bli nödvändigt åtminstone för varningsinformation.
<b>Begrepp:</b>	-
<b>Realisering:</b>	Kan innebära utveckling av reservdrift.
<b>Paragraf:</b>	<b>4kap. §1</b>
<b>Lydelse:</b>	"Den som arbetar hos en vårdgivare får ta del av dokumenterade uppgifter om en patient endast om han eller hon deltar i vården av patienten eller av annat skäl behöver uppgifterna för sitt arbete inom hälso- och sjukvården."
<b>Konsekvenser:</b>	4.1.1. Journalsystem och liknande bör utformas på ett sätt som gör att medarbetare inte kan ta del av journaluppgifter av misstag. 4.1.2. Medarbetare bör kunna identifiera sig vid datorterminaler för att behörighetsregler ska kunna tillämpas. (Se s.364) 4.1.3. "en arbetstagare, som är inloggad på en dator, ska låsa datorn då han eller hon tillfälligt lämnar datorn" (s.366) och därmed behöver system erbjuda funktion för sådan låsning. Går att realisera med ex vis RFID lösningar eller bara med enkel tidstyrning vi inaktivitet. 4.1.4. "Vidare bör uppgifter lagras i olika skikt så att mer känsliga uppgifter kräver aktiva val eller annars inte är lika enkelt åtkomliga för personalen som mindre känsliga uppgifter" (s.369). Ska den skrivningen åtlydas kräver det en nivågradering av känslighet, samt fält för indikering av detta i journalsystem. Gränssnitt behöver också byggas för att ta hänsyn till sådana nivåer.
<b>Kommentarer:</b>	4.1.K1. Rimligtvis kan lydning av denna lagparagraf inte helt åstadkommas med hjälp av tekniska begränsningar. (Det går alltid att se över axeln på en kollega.) Rutiner, utbildning och information till medarbetare måste vara en grundläggande del av efterlevnaden.

- 4.1.K2. På s.360 anges att kollegialt utbyte och konsultationer i stor utsträckning bör kunna ske utan att den enskilde identifieras. Möjligen kan sådant utbyte underlättas genom att journalsystem erbjuder avpersonifierade utdrag. Journalhandlingar som filtreras från personnummer, namn och adresser skulle kunna framställas med en knapptryckning. (Å andra sidan skulle det kunna leda till snabbare och därmed slarvigare sekretessprövning.) Valbar funktion med ”dölj patientinformation” kanske blir nödvändig.
- 4.1.K3. Som påpekas på s.364-365 är det från integritetssynpunkt av stor vikt att patientuppgifter hanteras på liknande sätt över landet. Speciellt vid sammanhållen journalföring. På s. 329 påpekas att behörighet bör tilldelas efter samma principer.

<b>Begrepp:</b>	behörighet, vårdgivare, inre sekretess
<b>Realisering:</b>	Journalföring, behörighets- och åtkomstkontroll – individ / organisation och rollbaserat, loggning, analys av loggar.
<b>Paragraf:</b>	<b>4kap. §2</b>
<b>Lydelse:</b>	"En vårdgivare skall bestämma villkor för tilldelning av behörighet för åtkomst till sådana uppgifter om patienter som förs helt eller delvis automatiserat. Sådan behörighet skall begränsas till vad som behövs för att den enskilde skall kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården."
<b>Konsekvenser:</b>	4.2.1. Journalsystem och andra informationssystem som används för att hantera uppgifter om patienter måste förses med behörighetssystem. 4.2.2. ”Arbetsuppgifter inom hälso- och sjukvården” bör modelleras gemensamt och på ett systematiskt sätt, för att behörigheter ska kunna tilldelas på ett för riket konsekvent sätt. På s. 329 påpekas att behörighet bör tilldelas efter samma principer. Bör modelleras av en verksamhetsutvecklingsgrupp.
<b>Begrepp:</b>	vårdgivare, behörighet, inre sekretess, regeringen får föreskriva
<b>Realisering:</b>	Journalföring, behörighets- och åtkomstkontroll – individ / organisation och rollbaserat, loggning, analys av loggar.

<b>Paragraf:</b>	<b>4kap. §3</b>
<b>Lydelse:</b>	"En vårdgivare skall genomföra åtgärder som innebär att åtkomst till sådana uppgifter om patienter som förs helt eller delvis automatiserat dokumenteras och kan kontrolleras. Vårdgivare skall genomföra systematiska och återkommande kontroller av om obehörig åtkomst till sådana uppgifter förekommer.  Regeringen, eller den myndighet som regeringen bestämmer, får meddela närmare föreskrifter om dokumentation och kontroll enligt första stycket. "
<b>Konsekvenser:</b>	4.3.1. Direktåtkomst och elektronisk åtkomst till uppgifter om patienter måste registreras (loggas). På sidan 341 framgår att loggningen måste vara så detaljerad att ”personuppgiftsbehandling vid behov kan rekonstrueras i efterhand”. Enligt s.370-371 bör Socialstyrelsen i samråd med Datainspektionen kunna föreskriva exakt hur detaljerad loggningen ska vara (t.ex. huruvida utskrifter ska loggas eller ej). 4.3.2. Alltså måste det finnas ett register över åtkomst. 4.3.3. Register över åtkomst måste vara åtkomligt för vårdgivare. 4.3.4. Journalsystem ska erbjuda möjlighet för vårdgivare att följa upp åtkomst.
<b>Följdkonsekvenser:</b>	4.3.2.F1. Former för ansvar, drift, teknik mm för "Register för åtkomst" behöver kartläggas.
<b>Kommentarer:</b>	4.3.K1. Register över åtkomst (logg) ska vara fristående från register som lagrar patientuppgifter (journal). Skall kunna ses av patienten. 4.3.K2. I NARRR slutrapport 2007-04-03 s.24 nämns BIF loggningstjänst i detta sammanhang.
<b>Begrepp:</b>	register över åtkomst, logg, uppföljning, behörighet
<b>Realisering:</b>	Loggning (BIF-loggning) och analys av loggar (BIF-logganalys).

<b>Paragraf:</b>	<b>4kap. §4</b>
<b>Lydelse:</b>	"...får inte göras tillgängliga genom elektronisk åtkomst för den som arbetar vid en annan vårdenhet eller inom en annan vårdprocess hos samma vårdgivare, om patienten motsätter sig det. I sådana fall skall uppgiften genast spärras."
<b>Konsekvenser:</b>	<p>4.4.1. Journalsystem måste kunna hantera information om spärrning av åtkomst från vårdenhet / vårdprocess. Sådan spärr måste kunna införas "genast".</p> <p>4.4.2. Journalsystem måste hantera information om vilken vårdenhet eller vårdprocess varje journalanteckning hör till.</p> <p>4.4.3. Journalsystem får, även om uppgift är spärrad, visa information för annan vårdenhet eller vårdprocess om att spärrad uppgift finns, samt vilken vårdenhet eller vårdprocess som spärrat informationen (s.27)</p> <p>4.4.4. Vårdenhet och vårdprocess måste definieras för att lagen ska kunna tillämpas. Socialstyrelsens termer ska användas, men dessa ger en stor flexibilitet hur dessa ska införas i praktiken. Kanske HSA måste utformas för att reflektera vårdenheter och vårdprocesser.</p>
<b>Följdnkonsekvenser:</b>	4.4.1.F1. Kravet på att spärr ska kunna införas "genast" medför att alla gränssnitt som kan användas för åtkomst av journalanteckning skall ha realtidstillgång till information om spärrar. En spärr ska inte aktiveras innan journaluppgifterna lagts in. Insynsskydd måste däremot aktiveras på en gång innan journaluppgifterna färdigställts.
<b>Kommentarer:</b>	<p>4.4.K1. Observera att detta gäller så kallad "inre spärr", inom en enskild vårdgivares verksamhet. Ej att förväxla med spärrar inom sammanhållen journalföring.</p> <p>4.4.K2. Förarbetstexten (s. 375) antyder att spärren ska kunna göras med angivande av vilka vårdenhet/vårdprocess som spärren avser. Detta skulle dels kräva att varje vårdenhet/vårdprocess har en entydig identitet, att patienten bereds tillgång till dessa identiteter och att systemet kan hantera spärrar med särskilda destinationer. Modeller av generella vårdprocesser måste tas fram.</p> <p>Arkitekturkonsekvenserna kan vara omfattande. Enligt s.377 bör dessutom informationssystemen kunna utformas på sätt som "minimerar vårdpersonalens arbete".</p>

<b>Begrepp:</b>	inre spärr, identitet, vårdenhet, vårdprocess
<b>Realisering:</b>	Hantering (upprättande och återkallande) av spärrar i journal och system på lokal, regional och nationell nivå. BIF samtyckestjänst och loggning. HSA katalog med vårdenhet och vårdprocess.
<b>Paragraf:</b>	<b>5kap. §4</b>
<b>Lydelse:</b>	"...får en sådan myndighet ha direktåtkomst till personuppgifter som behandlas av annan sådan myndighet i samma landsting eller kommun"
<b>Konsekvenser:</b>	5.4.1. Informationssystem med personuppgifter får göras tillgängliga för direktåtkomst från av andra. 5.4.2. Informationssystem måste hålla reda på geografiska gränser. Måste man dessutom hålla reda på geografiska sammanslagningar?
<b>Kommentarer:</b>	5.4.K1. På sidan 217 och 340 anges att direktåtkomst vanligtvis är skrivskyddad, dvs för att kunna påverka innehållet måste mottagande vårdgivare ladda ner informationen lokalt och modifiera den lokala kopian, som då blir en egen journalanteckning. 5.4.K2. På sidan 245 anges att direktåtkomst inte nödvändigtvis behöver gälla all journalföring hos en vårdgivare, eller alla delar av varje journal. En arkitektur för direktåtkomst av valda delar är alltså fullt tänkbar. 5.4.K3, På sidan 252 anges att "en enhetlig struktur underlättar för den som skall journalföra något att konstatera huruvida en uppgift redan finns antecknad i journalen och alltså inte behöver journalföras på nytt". De vårdgivare som samverkar i en sammanhållen journalföring bör alltså samordna struktur och terminologi.
<b>Följkonsekvenser:</b>	5.4.1.F1. Eftersom direktåtkomst definieras som åtkomst där mottagaren själv söker ut önskad information bör gränssnitt för navigation/sökning erbjudas.
<b>Begrepp:</b>	direktåtkomst, sammanhållen journalföring
<b>Realisering:</b>	Sammanhållen journal eller samverkande journalsystem. Inbyggda restriktioner beroende på organisation / geografisk indelning bör finnas.

<b>Paragraf:</b>	<b>5kap. §5</b>
<b>Lydelse:</b>	"En vårdgivare får medge en enskild direktåtkomst till sådana uppgifter om den enskilde själv som får lämnas ut till honom eller henne...  Regeringen, eller den myndighet som regeringen bestämmer, får föreskriva de krav på säkerhetsåtgärder som skall gälla vid sådan direktåtkomst."
<b>Konsekvenser:</b>	<p>5.5.1. System får förses med gränssnitt för direktåtkomst av patienten själv. Enligt s.387 bör denna möjlighet ges oavsett om vårdgivaren deltar i sammanhållen journalföring eller ej.</p> <p>5.5.2. Tillgänglighet bör endast ges om patienten "på något sätt framfört önskemål till vårdgivaren om att få direktåtkomst" (s.386). Alltså behöver det finnas rutiner och teknik för att hantera sådana önskemål från patienter.</p> <p>5.5.3. Uppgifter som inte får lämnas ut till patienten själv bör, i system där patienten själv bereds tillgång till sina uppgifter, förses med särskild markering, så att systemet kan filtrera bort sådana uppgifter. Observera att även information om vårdpersonalens åtkomst av sådan information bör göras osynlig för patienten, för att inte denne ska få otillbörlig information indirekt genom loggen. Även kallat "insynsskydd".</p> <p>5.5.4. Enligt s.388 har en vårdgivare möjlighet att begränsa direktåtkomsten till vissa uppgifter. Kräver viss modellering /metaklassning i journalsystem för att vara genomförbart.</p> <p>5.5.5. Säkerhetsåtgärder som krävs för enskilds direktåtkomst skall regleras i kommande föreskrifter. Dessa kommer att få betydande konsekvenser för arkitekturen. Medborgare ska ha certifikat med tillräckligt hög säkerhet.</p>
<b>Kommentarer:</b>	<p>5.5.K1. Uppgifterna ska vara "så långt som möjligt förståeliga för patienten" (s.385), något som kan underlättas genom att systemet även erbjuder "möjlighet att få hjälp att tyda dem" (sist på s.385). Kräver någon form av medicinskt (hypertext) lexikon typ Wikipedia för medicin.</p> <p>5.5.K2. Går det att få förhandsbesked om hur föreskrifter för säkerhet kommer att se ut?</p> <p>5.5.K3. Det förefaller lämpligt att sådan direktåtkomst sker via webben, med användande av sådan säkerhetsteknik som används för annan känslig information.</p>
<b>Begrepp:</b>	direktåtkomst, patient, enskilds direktåtkomst, säkerhetsåtgärder

<b>Realisering:</b>	Inbyggda restriktioner beroende på organisation / geografisk indelning bör finnas (vårdgivare, kommun, landsting, nation). Åtkomstregler för att ta del av egen journal ska finnas. BIF-tjänster, där vårdpersonal autentiseras via personliga SITHS-certifikat eller medborgare via medborgarcertifikat. VERVA föreslår i sin handlingsplan åtgärder – där är e-leg enligt bank ID ej anses tillräckligt för journalinformation.
<b>Paragraf:</b>	<b>6kap. §1</b>
<b>Lydelse:</b>	"En vårdgivare får, under de förutsättningar som anges i 2 §, ha direktåtkomst till andra vårdgivares personuppgifter som behandlas för ändamål som anges i 2 kap. 4 § första stycket 1 och 2."
<b>Konsekvenser:</b>	6.1.1. System med personuppgifter (främst syftas på journalsystem) får ha gränssnitt för extern direktåtkomst.
<b>Kommentar:</b>	6.1.K1. Jämför 5kap 4§.
<b>Begrepp:</b>	sammanhållen journalföring, direktåtkomst
<b>Realisering:</b>	Åtkomst av personuppgifter (lokal, region, nationell) för att skapa en sammanhållen journal (referens). Sker med åtkomstkontroll och kontroll av spärrar och samtycket (BIF-åtkomstkontroll och BIF-samtycke).  Inbyggda restriktioner beroende på organisation / geografisk indelning bör finnas (vårdgivare, kommun, landsting, nation).

<b>Paragraf:</b>	<b>6kap. §2</b>
<b>Lydelse:</b>	"Om en patient motsätter sig det, får uppgifter om patienten inte göras tillgängliga för andra vårdgivare genom sammanhållen journalföring. Uppgift om att det finns spärrade uppgifter får dock göras tillgänglig. "
<b>Konsekvenser:</b>	<p>6.2.1. Uppgift i journalsystem som används vid sammanhållen journalföring ska kunna föras med ett samtycke som förhindrar annan vårdgivares direktåtkomst via sammanhållen journalföring.</p> <p>6.2.2. Om spärr finns registrerad skall direktåtkomst till de spärrade uppgifterna från annan vårdgivare vara tekniskt omöjlig. (Se s. 296)</p> <p>6.2.3. Om spärr finns registrerad kan uppgift om spärrans existens visas vid direktåtkomst från annan vårdgivare.</p> <p>6.2.4. Enligt s.504 ska patienten vid <i>varje vårdepisod</i> ha möjlighet att spärra sin journalinformation. Därmed behöver begreppet vårdepisod vara entydigt definierat. Patienten har antagligen rätt att kunna spärra journalinformation när som helst.</p>
<b>Kommentarer:</b>	6.2.K1. Kan man förutsätta att samtycket lämnats vid tidigare vårdtillfälle i samma vårdepisod, eller bör system innehålla information om huruvida patienten under vårdepisoden medgivit direktåtkomst?
<b>Begrepp:</b>	vårdepisod
<b>Realisering:</b>	Lokal, regional och nationell hantering (skapa, återkalla, visa) av spärrar. Spärrar ska kunna spåras och kan vara tillfälliga (BIF-samtycke).

<b>Paragraf:</b>	<b>6kap. §2</b>
<b>Lydelse:</b>	<p>" Om en patient motsätter sig det, får uppgifter om patienten inte göras tillgängliga för andra vårdgivare genom sammanhållen journalföring. Uppgift om att det finns spärrade uppgifter får dock göras tillgänglig.</p> <p>Innan uppgifter om en patient görs tillgängliga för andra vårdgivare genom sammanhållen journalföring, skall patienten informeras om vad den sammanhållna journalföringen innebär och om att patienten kan motsätta sig den.</p> <p>Om en patient motsätter sig sammanhållen journalföring, skall uppgifterna genast spärras. En patient kan när som helst begära att den vårdgivare som har spärrat uppgifterna häver spärren."</p>
<b>Konsekvenser:</b>	<p>6.2.5. Uppgift ska kunna spärras "genast".</p> <p>6.2.5. Ska kunna hävas av den vårdgivare som infört spärren.</p> <p>6.2.7. Patientdatakommittén anger på s.294 att personuppgifter tillhörande patienter som motsätter sig deltagande i sammanhållen journalföring inte bör lagras i separata informationssystem. Skall istället regelstyras i samma system utifrån egenskaper på informationen enligt BIF.</p>
<b>Kommentarer:</b>	<p>6.2.K2. Om patienten ber en annan vårdgivare att häva spärren skall denne kontakta den vårdgivare som införde spärren och meddela att patienten bett att få spärren hävd. (Se författningskommentar s.566). Detta förfarande synes aningen omständligt. Kanske kan denna kommunikation ske elektroniskt genom systemet... Troligen är det angeläget att hävningen sker tämligen snart.</p> <p>6.2.K3. Enligt s. 505 ska information inte kunna delges andra vårdgivare via sammanhållen journalföring innan patienten själv kunnat ge samtycke. Dock bör journalföring kunna ske. Därmed behöver system kunna särbehandla information vartill patienten varken givit samtycke till eller spärrat sammanhållen journalföring.'</p>
<b>Begrepp:</b>	hävning, vårdgivare, sammanhållen journalföring
<b>Realisering:</b>	Lokal, regional och nationell hantering (skapa, återkalla, visa) av spärrar. Spärrar ska kunna spåras och kan vara tillfälliga (BIF-samtycke).

<b>Paragraf:</b>	<b>6kap. §3</b>
<b>Lydelse:</b>	"För att en vårdgivare skall få bereda sig tillgång till uppgifter som inte är spärrade enligt 2 § tredje stycket krävs att...patienten samtycker till det...."
<b>Konsekvenser:</b>	<p>6.3.1. Det måste finnas rutiner för att få patientens aktiva samtycke (se s.298) innan direktåtkomst genom sammanhållen journalföring används. Observera att tanken är att patienten ska kunna lämna sådant samtycke i förväg, riktad till en viss eller vissa kommande vårdgivare vid en planerad vårdsituation. Om denna hantering av samtycken ska hanteras genom informationssystemet krävs ganska omfattande arkitekturåtgärder. En spärr skall kunna knytas till vårdprocesser och vårdgivare ungefär på samma sätt som ”inre spärrar” ska kunna knytas till vårdenhet. Men det är också tänkbart att den vårdgivare som tar emot samtycket kontaktar och meddelar alla berörda framtida vårdgivare och meddelar dem detta samtycke. Samtycket kan exempelvis finnas med som kryssruta på konsultremiss</p> <p>6.3.2 På sidan 307 anges att samtycke ska kunna ske i förväg, och riktat mot en viss kategori av vårdgivare. De arkitekturella konsekvenserna av en sådan möjlighet är att landets vårdgivare kategoriseras på lämpligt (enhetligt) sätt och att informationssystem medger att samtycke kopplas till sådan kategorisering.</p>
<b>Begrepp:</b>	samtycke, patientrelation
<b>Realisering:</b>	Lokal, regional och nationell hantering (skapa, återkalla, visa) av spärrar. Spärrar ska kunna spåras och kan vara tillfälliga (BIF samtycke).

<b>Paragraf:</b>	<b>6kap. §4</b>
<b>Lydelse:</b>	”En vårdgivare får bereda sig tillgång till en annan vårdgivares uppgifter om en patient, om patientens samtycke inte kan inhämtas och uppgifterna kan antas ha betydelse för den vård som patienten oundgängligen behöver. Detta gäller endast om uppgifterna inte är spärrade enligt 2 § tredje stycket.”
<b>Konsekvens:</b>	6.4.1 BIF måste utvidgas för att klara nödöppning. Om det inte finns spärr så får man tillgång till informationen.
<b>Kommentarer:</b>	6.4.K1. Vid loggning av åtkomst torde denna typ av åtkomst vara av särskilt intresse med tanke på att patienten inte kunnat ge samtycke.
<b>Begrepp:</b>	samtycke, skede 2
<b>Realisering:</b>	<p>Inbyggda restriktioner beroende på organisation / geografisk indelning bör finnas (vårdgivare, kommun, landsting, region, nation). Möjlighet till att hantera avvikelse i förhållande till den normala åtkomstkontrollen vid speciella förhållanden (bör preciseras) ( BIF samtycke).</p> <p>En alternativ realisering skulle eventuellt kunna vara att detta löses på tillämpningsnivå, dvs. att tjänsten har en blåljusflagga som vid nekad rättighet (spärr och medgivande saknas) från BIF.ÅKT, verifierar mot HSA att frågande organisation är klassad som blåljus-berättigad, helt enkelt släpper igenom frågan. BIF skulle då inte behöva tillföras semantik för blåljus.</p>
<b>Paragraf:</b>	<b>6kap. §7</b>
<b>Lydelse:</b>	"Vad som sägs i 4 kap. 2 och 3 §§ gäller även för behörighetstildelning och åtkomstkontroll vid sammanhållen journalföring."
<b>Kommentarer:</b>	6.7.K1. Innebörden av denna bestämmelse skall enligt författningskommentar (s 572) meddelas närmare i föreskrifter från Socialstyrelsen. Dessa föreskrifter kommer sannolikt att få konsekvenser för IT-arkitekturen.
<b>Begrepp:</b>	behörighet, sammanhållen journalföring
<b>Realisering:</b>	<p>Inbyggda restriktioner beroende på organisation / geografisk indelning bör finnas (vårdgivare, kommun, landsting, nation) (BIF-åtkomstkontroll).</p> <p>Loggning och analys av loggar (BIF-loggtjänst, BIF-logganalys). Möjlighet till att hantera avvikelse i förhållande till den normala åtkomstkontrollen vid speciella förhållanden (bör preciseras). BIF, SITHS och HSA tjänster används.</p>

<b>Paragraf:</b>	<b>6kap. §8</b>
<b>Lydelse:</b>	"gäller skyldigheten enligt 3kap 16§ att bevara en journalhandling den vårdgivare som ansvarar för handlingen"
<b>Konsekvenser:</b>	6.8.1 Regelverk för utskrift och bevarande på papper måste definieras. 6.8.2 Logg över kopiering måste finnas.
<b>Kommentarer:</b>	6.8.K1. Enligt författningskommentaren (s. 573) ska ”nedtankning” av journalhandling från annan vårdgivare via direktåtkomst undvikas. Om detta ändå sker (och det förutsätts vara oundvikligt ibland) skall den kopierade handlingen behandlas som om den härstammade från den egna verksamheten. Därvid uppstår en dubbellagring av handlingen. För att vårdgivare ska kunna veta vad som hänt med journalhandlingen efter kopieringen bedöms att kopieringen som sådan bör noteras i både originalhandlingen och i kopian.
<b>Begrepp:</b>	arkivering, journalhandling, gallring, sammanhållen journalföring
<b>Realisering:</b>	Spårbarhet på journalinformation på tvärs över vårdgränser (vårdgivare, kommun, landsting, nation). Kan innebära dubbel arkivering. Möjligtvis måste tjänst för kopiering av hela eller delar av journal utvecklas. Vidareutveckling av BIF-notifiering, eller utveckla en definierad tjänst som behöver implementeras av de vårdgivare vars journaldata ska tillåtas för utskrift.

<b>Paragraf:</b>	<b>7kap. §2</b>
<b>Lydelse:</b>	"Personuppgifter får inte behandlas i ett nationellt eller regionalt kvalitetsregister, om den enskilde motsätter sig det.  Om den enskilde motsätter sig personuppgiftsbehandlingen sedan den påbörjats, skall uppgifterna utplånas ur registret så snart det kan ske. "
<b>Konsekvenser:</b>	7.2.1. I de fall där den elektroniska journalföringen är integrerad med kvalitetsregisterrapporteringen (se s.435) måste patientens motsättande av personuppgiftsbehandling på något sätt kunna hanteras. Eftersom personuppgiftsbehandling för journalföringen inte är frivillig så kommer uppgifter att behandlas i systemet, men om dessa inte ska anses behandlas i kvalitetsregistret måste uppgifterna på något sätt markeras så att de kan undantas i all behandling som är kopplad till kvalitetsregister. Patienten kan medge användning för syfte Hälso- och Sjukvård men inte medge användning syfte Forskning och uppföljning. Detta gör att medgivandet kanske måste kopplas till syftet vilket komplicerar men är hanterbart. 7.2.2 Spårbarhet på samtycke på individnivå och vårdgivare måste finnas. All information i kvalitetsregister måste kunna kopplas till enskild individ.
<b>Kommentarer:</b>	7.2.K1. Enligt s.450 bör kostnadseffektivitet kunna behandlas parallellt med behandlingsresultat mm. För att kunna beräkna kostnadseffektivitet förefaller det naturligt att koppla samman vårddokumentation med administrativ dokumentation i t.ex. lönesystem. Sådan samkörning kan alltså eventuellt bli aktuell, vilket IT-arkitekter bör vara kunniga om. Se även s.413 om verksamhetsuppföljning.
<b>Begrepp:</b>	kvalitetsregister, personuppgifter, motsätter sig, utplånas
<b>Realisering:</b>	Spärrar för lokala, regionala och nationella kvalitetsregister ska kunna hanteras. Radering av uppgifter i kvalitetsregister, kan behöva tjänsteinteraktion av typen uppdrag/svar (asynkron tvåvägskommunikation). OBS detta gäller även då information delats ut via sammanhållen journal till annan vårdgivare (BIF-åtkomstkontroll). Logg för spårbarhet på individ och information måste implementeras i kvalitetsregister (BIF-loggning, BIF-logganalys).

<b>Paragraf:</b>	<b>7kap. §8</b>
<b>Lydelse:</b>	"...enskilds personnummer eller namn får behandlas i ett nationellt eller regionalt kvalitetsregister endast om det inte är tillräckligt för ändamål som anges i 4 § att använda kodade personuppgifter eller personuppgifter som endast indirekt kan hänföras till den enskilde...."
<b>Konsekvenser:</b>	7.8.1. Kvalitetsregister ska i normala fall hantera kodade personuppgifter istället för pnr..
<b>Följdkonsekvenser:</b>	7.8.1.F1. Rutiner för kodning och hantering av kodnycklar mm måste finnas för de flesta kvalitetsregister. Ett arbete för InfoSäk gruppen?
<b>Kommentarer:</b>	7.8.K1. Se även s.418 om verksamhetsuppföljning.
<b>Begrepp:</b>	avidentifiering, personnummer, kodad, känsliga personuppgifter,
<b>Realisering:</b>	Avkodning av patientuppgifter. Behöver ny tjänst för pseudonymisering <sup>1</sup> .
<b>Paragraf:</b>	<b>7kap. §9</b>
<b>Lydelse:</b>	"En vårdgivare får ha direktåtkomst till de uppgifter i ett nationellt eller regionalt kvalitetsregister som vårdgivaren lämnat till registret."
<b>Konsekvenser:</b>	7.9.1. Uppgifter ska, i den mån vårdgivare ska kunna få direktåtkomst, vara försedda med uppgiftslämnande vårdgivares identitet. 7.9.2. I den mån vårdgivare ska kunna få direktåtkomst till kvalitetsregister skall detta kunna filtrera ut uppgifter baserat på uppgiftslämnande vårdgivares identitet (och endast ge möjlighet till åtkomst av uppgifter från den egna vårdgivaren).
<b>Kommentarer:</b>	7.9.K1. Vårdgivares identitet bör företrädesvis kopplas till en beständig katalogpost, så att eventuella organisatoriska förändringar inte gör det omöjligt att kontakta en vårdgivare som ärvt ansvaret för uppgiften. HSA-katalogen (se s.115) kanske kan användas(?). Observera att en vårdgivare kan delas upp och bli flera. Ska då alla dessa vårdgivare anses vara behöriga att få direktåtkomst till information som lagrades innan delningen?
<b>Begrepp:</b>	vårdgivare, kvalitetsregister, direktåtkomst
<b>Realisering:</b>	Åtkomstkontroll och loggning av åtkomst till kvalitetsregister.

---

<sup>1</sup> Pseudonymisering: avidentifiering av individinformation

<b>Paragraf:</b>	<b>8kap. §3</b>
<b>Lydelse:</b>	"På ansökan av patienten eller någon annan som omnämns i en patientjournal får Socialstyrelsen förordna att journalen helt eller delvis skall förstöras..."
<b>Konsekvenser:</b>	8.3.1. Patientjournal ska kunna förstöras. 8.3.2. Regelverk för hantering av kopierad information bör finnas. 8.3.3. Säkerhetskopior på permanent media går inte att selektivt radera.
<b>Kommentarer:</b>	8.3.K1. Enligt patientdatakommittén (s.281) är det av vikt att det finns rutiner för att säkerställa att förstöringen även omfattar eventuella uppgifter i säkerhetskopior. Vår bedömning är att det kan visa sig vara svårt att söka upp och utplåna utvalda data från stora mängder säkerhetskopior. Ska hela eller delar av journal förstöras?
<b>Begrepp:</b>	förstöras, utplånas
<b>Realisering:</b>	Permanent radering av hela eller delar av journal. OBS detta gäller även då information delats ut via sammanhållen journal till annan vårdgivare. Genom BIF utlämnandetjänst o/e loggning kan kopior spåras.
<b>Paragraf:</b>	<b>8kap. §4</b>
<b>Lydelse:</b>	"En vårdgivare skall på begäran av en patient lämna information om den direktåtkomst och elektroniska åtkomst som förekommit till uppgifter om patienten...."
<b>Konsekvenser:</b>	8.4.1 Påverkar hur loggar utformas. 8.4.2. Ska vara på ett sådan media och format så att patienten kan läsa och förstå informationen. Det behövs en åtkomstlogg som patienten ska kunna titta på.
<b>Kommentarer:</b>	8.4.K1. De föreskrifter som nämns i slutet av 8kap. §4 kan få konsekvenser för utformning av registret.
<b>Begrepp:</b>	åtkomst, vårdgivare, patient
<b>Realisering:</b>	Export av information från integritetslogg. BIF loggtjänst och BIF-logganslys. Förutsätter historik i HSA-katalogen.

<b>Paragraf:</b>	<b>8kap. §6</b>
<b>Lydelse:</b>	Den personuppgiftsansvarige skall ha möjlighet att korrigera journalanteckningar. Sker rättelse skall den personuppgiftsansvarige också underrätta tredje man, till vilken uppgifterna har lämnats ut. (Enligt patientdatakommittens betänkande, avsnitt 18.2.1, s 506).
<b>Konsekvenser:</b>	<p>8.6.1 Journalsystem ska kunna hantera information om att rättelse skett, när den skett och av vem. Nationella riktlinjer för hur rättelser ska visas måste tas fram.</p> <p>8.6.2. Personuppgiftsansvarig ska ha möjlighet att införa rättelser – även efter att journalanteckning blivit signerad. I och med att journalanteckning inte får utplånas utan att Socialstyrelsen så beslutat bör dock rättelser hanteras i form av tilläggs-/ändringsinformation, och inte helt ersätta tidigare data. Se även s.273. En aviseringsfunktion om vem som tagit del av felaktiga uppgifter kanske måste finnas!</p> <p>8.6.3. Identitet på alla som tagit del av de okorrigerade uppgiften bör finnas tillgänglig, och att det även finns möjlighet att kontakta dessa.</p> <p>8.6.4 Historisk information om organisationer, personer och roller måste finnas (HSA).</p>
<b>Kommentarer:</b>	8.6.K1. Om det visar sig att rättelser ofta förekommer bör system utformas så att de underlättar för personalen att underrätta tredje man (den som tagit del av icke korrigerad information). Kanske kan systemet till och med underrätta tredje man automatiskt? Journalsystemet måste hantera spårbarhet av kommunicerat journalmaterial (rättelser, radering).
<b>Begrepp:</b>	rättelse, korrigering, personuppgiftsansvarig
<b>Realisering:</b>	Möjlighet att korrigera uppgifter och spåra korrigeringar av uppgifter. OBS detta gäller även då information delats ut via sammanhållen journal till annan vårdgivare. BIF-loggtjänst och BIF-logganalys för att kunna spåra uppgifter. Påverkar HSA katalogens struktur.

<b>Paragraf:</b>	<b>9kap. §1</b>
<b>Lydelse:</b>	" Om det på sannolika skäl kan antas att patientjournaler inom enskild hälso- och sjukvård inte kommer att handhas enligt föreskrifterna i denna lag eller enligt föreskrifter som meddelats med stöd av lagen, får Socialstyrelsen besluta att de skall tas om hand.  Socialstyrelsen får också besluta om omhändertagande av patientjournaler inom enskild hälso- och sjukvård, om – den som ansvarar för hanteringen av journalerna ansöker om det, och – det finns ett påtagligt behov av att journalerna tas om hand. "
<b>Konsekvenser:</b>	9.1.1. Socialstyrelsen måste ha rutiner för att ta emot ansökningar om omhändertagande av patientjournaler. 9.1.2. Patientjournaler måste hanteras på ett sådant sätt att det är tekniskt möjligt för annan att överta hanteringen.
<b>Realisering:</b>	Export av hela journaler på media och format om Socialstyrelsen kan läsa och hantera. Bör vara nationell standard och kanske helst på arkivbeständigt format.
<b>Paragraf:</b>	<b>Övergångsbestämmelser</b>
<b>Lydelse:</b>	"Denna lag träder i kraft den 1 januari 2008, då patientjournallagen (1985:562) och lagen (1998:544) om vårdregister upphör att gälla.  2. Bestämmelserna i 7 kap. skall inte börja tillämpas förrän den 1 januari 2009 i fråga om nationella och regionala kvalitetsregister som börjat föras före denna lags ikraftträdande. 3. Bestämmelserna i 7 kap. 2 och 3 §§ gäller inte för personuppgifter som behandlats i nationella och regionala kvalitetsregister före den 1 januari 2009. "
<b>Konsekvenser:</b>	Ö.1. Det är bråttom! Vårdgivare som redan idag hanterar information som berörs av patientdatalagen behöver anpassa sina system på ganska få månader.
<b>Kommentarer:</b>	Ö.K1. Nytt datum är satt till den 1 juli 2008 då denna lag beräknas träda i kraft.
<b>Begrepp:</b>	övergångsbestämmelser, ikraftträdande
<b>Realisering:</b>	-

## Konsekvenser av föreslagna nya lydelse i sekretesslagen (1980:100)

<b>Paragraf:</b>	<b>SL 7kap. §1c</b>
<b>Lydelse:</b>	"Sekretess gäller....  Sekretess enligt första stycket gäller också i sådan verksamhet hos myndighet som innefattar omprövning av beslut i eller särskild tillsyn över allmän eller enskild hälso- och sjukvård."
<b>Konsekvenser:</b>	SL7.1.1. Behandling av personuppgifter inom hälso- och sjukvården måste ske med iakttagande av tillfredsställande säkerhetsrutiner, hantering av behörighet, tekniskt skydd mot avlyssning och så vidare. Detta gäller inte bara i den dagliga informationshanteringen utan också i de fall då myndighet omprövar beslut eller utövar särskild tillsyn.
<b>Begrepp:</b>	sekretess, säkerhet
<b>Realisering:</b>	Omfattande tjänster för säker hantering av journalinformation inklusive loggning och analys av loggar (BIF loggning och logganalys). Hantering av sekretesskyddade uppgifter. Utveckling av processer och rutiner för hantering av journalinformation och administration av behörighet och åtkomst (BIF åtkomst och autenticering).
<b>Paragraf:</b>	<b>SL 7kap. §1d</b>
<b>Lydelse:</b>	"Sekretess enligt 1 c § första stycket hindrar inte att en uppgift lämnas..."
<b>Konsekvenser:</b>	SL7.1.2. Undantag från sekretess för sammanhållen journalföring innebär att journalsystem kan ha gränssnitt mot externa aktörer som enligt lagen får ha tillgång till uppgifterna.
<b>Begrepp:</b>	sammanhållen journalföring, sekretess
<b>Realisering:</b>	Omfattande tjänster för säker hantering av journalinformation inklusive loggning och analys av loggar (BIF loggning och logganalys). Hantering av sekretesskyddade uppgifter. Utveckling av processer och rutiner för hantering av journalinformation och administration av behörighet och åtkomst (BIF åtkomst och autenticering).

<b>Paragraf:</b>	<b>SL 7kap. §3</b>
<b>Lydelse:</b>	"Sekretessen enligt 1 c eller 1 e § gäller också i förhållande till den vård- eller behandlingsbehövande själv i fråga om uppgift om hans eller hennes hälsotillstånd, om det med hänsyn till ändamålet med vården eller behandlingen är av synnerlig vikt att uppgiften inte lämnas till honom eller henne."
<b>Konsekvenser:</b>	5.5.3. Uppgifter som inte får lämnas ut till patienten själv bör, i system där patienten själv bereds tillgång till sina uppgifter, förses med särskild markering, så att systemet kan hindra visning av sådana uppgifter. SL7.3.1. "Om den som ansvarade för journalen vid behandlingstillfället inte längre tjänstgör, får hans eller hennes efterträdare i verksamheten anses ha övertagit ansvaret". Det bör finnas möjligheter att identifiera befattningshavares efterträdare, för att kunna hänvisa frågor om patients behörig att ta del av information från sin egen journal till rätt person.
<b>Realisering:</b>	Omfattande tjänster för säker hantering av journalinformation inklusive loggning och analys av loggar (BIF loggning och logganalys). Hantering av sekretesskyddade uppgifter. Utveckling av processer och rutiner för hantering av journalinformation och administration av behörighet och åtkomst (BIF åtkomst och autenticering).
<b>Paragraf:</b>	<b>SL 9kap. §4</b>
<b>Lydelse:</b>	"Sekretess gäller i sådan särskild verksamhet hos myndighet som avser framställning av statistik för uppgift som avser enskilda personliga eller ekonomiska förhållanden och som kan hänföras till den enskilde."
<b>Kommentarer:</b>	SL9.4.K1. Om fält för namn eller personnummer hanteras är det uppenbart att uppgift som kan hänföras till den enskilde. Men hur är det med löpande text, bilder eller annat material. Där torde en manuell bedömning behöva ske vid varje enskilt tillfälle då uppgiften kommuniceras. Konsekvensen blir att det nog inte går att göra några IT-system som automatiskt markerar sekretessbelagda uppgifter.
<b>Realisering:</b>	Omfattande tjänster för säker hantering av journalinformation inklusive loggning och analys av loggar (BIF loggning och logganalys). Hantering av sekretesskyddade uppgifter. Utveckling av processer och rutiner för hantering av journalinformation och administration av behörighet och åtkomst (BIF åtkomst och autenticering).

<b>Paragraf:</b>	<b>SL 9kap. §4</b>
<b>Lydelse:</b>	"Uppgift ... får dock lämnas ut, om det står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till den enskilde lider skada eller men. Detsamma gäller en uppgift som avser en avliden och som rör dödsorsak eller dödsdatum, om uppgiften behövs i ett nationellt eller regionalt kvalitetsregister enligt patientdatalagen."
<b>Kommentarer:</b>	SL9.4.K2. Uppgift om dödsorsak och dödsdatum får alltså kommuniceras med kvalitetsregister. Detta skulle kunna få arkitekturkonsekvenser, t.ex. vid systemdesign där uppgifter om avlidna hanteras på särskilt sätt. Vad gäller för spärrar efter patient avlidit?
<b>Begrepp:</b>	dödsorsak, utlämnande, kvalitetsregister
<b>Realisering:</b>	Tjänster för export av valda delar av journaler.

## **Konsekvenser av föreslagen ny lydelse i lagen (2001:499) om omskärelse av pojkar**

Förändringen är en rent lagteknisk korrigeringsmed anledning av att patientjournalagen ersätts av patientdatalagen. Bedömningen är att ändringen i sig medför några IT-arkitekturkonsekvenser.

## Konsekvenser av föreslagen ny lydelse i lagen (2002:297) om biobanker i hälso- och sjukvården m.m.

<b>Paragraf:</b>	<b>BL 3kap. §7</b>
<b>Lydelse:</b>	"Uppgifter om information och samtycke m.m. enligt 1–6 §§ skall dokumenteras på lämpligt sätt i anslutning till biobanken samt i provgivarens patientjournal."
<b>Konsekvenser:</b>	BL3.7.1. I anslutning till biobanker skall uppgifter om information och samtycke kunna dokumenteras.
<b>Begrepp:</b>	biobank, samtycke
<b>Realisering:</b>	Registrering och hantering av samtycke i både journalsystem och system för administration av biobank. Inkluderar även spårbarhet vid export. Ska det finnas möjlighet till att återkalla samtycke?
<b>Paragraf:</b>	<b>BL 4kap. §6a</b>
<b>Lydelse:</b>	"Anser denne att journalhandlingen eller någon del av den inte bör lämnas ut, skall han eller hon genast med eget yttrande överlämna frågan till Socialstyrelsen för prövning."
<b>Kommentarer:</b>	8.2.K1. Inte nödvändigtvis en IT-arkitekturkonsekvens, men en konsekvens torde vara att rutiner behöver finnas för överlämnande av utlämnandeärenden till Socialstyrelsen.
<b>Begrepp:</b>	utlämnande

## **Konsekvenser av föreslagen ny lydelse i lagen (2005:225) om rättsintyg i anledning av brott**

Ändringarna utgör endast följdändringar till bestämmelserna i sekretesslagen, och medför i sig enligt bedömning inte några konsekvenser för IT-arkitekturen.