Journalföring och behandling av personuppgifter i hälso- och sjukvården

Handbok vid tillämpningen av Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården

Socialstyrelsen

Publikationen finns som pdf på Socialstyrelsens webbplats. Publikationen kan också tas fram i alternativt format på begäran. Frågor om alternativa format skickas till alternativaformat@socialstyrelsen.se

ISBN 978-91-7555-414-3
Artikelnummer 2017-3-2

Omslagsfoto iStockphoto
Tryck www.socialstyrelsen.se, mars 2017

Förord

Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården trädde i kraft den 1 mars 2017. De nya föreskrifterna ersätter Socialstyrelsens föreskrifter (SOSFS 2008:14) om informationshantering och journalföring i hälso- och sjukvården. Denna handbok utgör ett stöd vid tillämpningen av föreskrifterna och de allmänna råden och riktar sig i första hand till vårdgivare, verksamhetschefer, medicinskt ansvariga sjuksköterskor och hälso- och sjukvårdspersonal som ska tillämpa föreskrifterna och de allmänna råden.

Handboken är framtagen av Socialstyrelsens jurister Mathias Wallin och Martina Holmström. Under det inledande arbetet med handboken har informationssäkerhetskonsulten Johanna Erlandsson deltagit.

Som ett stöd i arbetet har det funnits en referensgrupp med representanter från Datainspektionen, Inera, Inspektionen för vård och omsorg, Läkarsekreterares och sjukvårdsadministratörers förbund, Läkemedelsverket, Sveriges läkarförbund, Sveriges tandläkarförbund, Myndigheten för samhällsskydd och beredskap, Vårdförbundet och Vårdföretagarna.

Stockholm i mars 2017
Erik Höglund
Avdelningschef
Rättsavdelningen

Innehåll

Läsanvisningar

Denna handbok utgör ett stöd vid tillämpningen av Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården. Handboken följer den struktur som finns i föreskrifterna och de allmänna råden. Efter varje föreskrift och allmänt råd ges en kommentar för att ge läsaren vägledning vid tillämpningen. Det går att läsa varje kapitel för sig men för att förstå den grundläggande systematiken i uppbyggnaden av föreskrifterna rekommenderas att handboken läses i sin helhet.

Definitionerna i 2 kap. 1 § HSLF-FS 2016:40 kommenteras inte särskilt utan här hänvisas i stället till kommentaren till den föreskrift eller det allmänna råd där definitionen förekommer. Inte heller undantagsbestämmelsen i 9 kap. kommenteras särskilt.

Bestämmelserna i HSLF-FS 2016:40 kompletterar och utgår från bestämmelserna i patientdatalagen (2008:355), PDL. För att skapa sig en mer heltäckande bild över den författning som reglerar journalföring och behandling av personuppgifter i hälso- och sjukvården behöver läsaren därför även ha kännedom om bestämmelserna i PDL. Denna handbok kan inte ses som en handbok till PDL. I de fall det är nödvändigt för förståelsen av bestämmelserna i HSLF-FS 2016:40 behandlas dock även relevanta bestämmelser i PDL.

Föreskrifter och allmänna råd

HSLF-FS 2016:40 innehåller både föreskrifter och allmänna råd. Föreskrifter är bindande regler, det vill säga de bestämmer hur enskilda och myndigheter ska handla. En myndighet får inte utfärda föreskrifter om det inte finns stöd för det i lag (8 kap. 11 regeringsformen).

Allmänna råd är inte bindande regler. De är i stället generella rekommendationer om tillämpningen av en författning (lag, förordning eller annan föreskrift) som anger hur någon kan eller bör handla i ett visst hänseende (1 § författningssamlingsförordningen [1976:725]). Allmänna råd utesluter inte andra sätt att uppnå de mål som avses i författningen.

Förkortningar

HSL	Hälso- och sjukvårdslagen (1982:763)
IVO	Inspektionen för vård och omsorg
NI	Nationell informationsstruktur
OSL	Offentlighets- och sekretesslagen (2009:400)
PDL	Patientdatalagen (2008:355)
Prop.	Proposition
PSL	Patientsäkerhetslagen (2010:659)
SKL	Sveriges Kommuner och Landsting

Tillämpningsområde

Föreskrifternas tillämpningsområde

1 kap. 1 § HSLF-FS 2016:40

Dessa föreskrifter ska tillämpas då vårdgivare behandlar patienters personuppgifter i verksamhet som omfattas av 1 kap. 1 § patientdatalagen (2008:355).

HSLF-FS 2016:40 har samma tillämpningsområde som patientdatalagen (2008:355), PDL. Enligt 1 kap. 1 § PDL tillämpas lagen vid vårdgivares behandling av personuppgifter inom hälso- och sjukvården. Hälso- och sjukvård definieras i 1 kap. 3 § PDL som verksamhet som avses i hälso- och sjukvårdslagen (1982:763), tandvårdslagen (1985:125), lagen (1991:1128) om psykiatrisk tvångsvård, lagen (1991:1129) om rättspsykiatrisk vård, smittskyddslagen (2004:168), lagen (1972:119) om fastställande av könstillhörighet i vissa fall, lagen (2006:351) om genetisk integritet m.m. samt den upphävda lagen (1944:133) om kastrering.

Av förarbetena till PDL framgår att i lagens tillämpningsområde ingår även annan närliggande patientverksamhet som insemination, abort, sterilisering, omskärelse, transplantationsingrepp på givare och blodgivning med mera. Till kärnverksamheten räknas vidare bland annat administration och utveckling av verksamheten (2 kap. 4 § och 7 kap. 4 § PDL). Personuppgiftsbehandling för den rent administrativa verksamheten utan direkt koppling till patientverksamheten, till exempel personaladministration, faller dock utanför lagens tillämpningsområde. Detsamma gäller forskning, såvida det inte är fråga om en vårdgivares så kallade patientnära eller kliniska forskning som innefattar journalföring eller annan dokumentation som hör till vården. PDL är inte heller tillämplig vid utbildning av till exempel blivande läkare och sjuksköterskor. I den del dessa deltar i den faktiska patientvården är PDL dock tillämplig (proposition 2007/08:126 Patientdatalag m.m. s. 222).

I PDL finns också bestämmelser om skyldighet att föra patientjournal. Lagen gäller i tillämpliga delar även uppgifter om avlidna personer (1 kap. 1 § PDL).

System som är helt eller delvis automatiserade

1 kap. 2 § HSLF-FS 2016:40

Bestämmelserna i 3 kap. 2 § 4 och 7–20 §§, 4 kap. 2–12 §§, 6 kap. 1–3 §§ samt 7 kap. 1 § 4 ska endast tillämpas av vårdgivare som behandlar patienters personuppgifter i system som är helt eller delvis automatiserade.

Övriga bestämmelser ska tillämpas av de vårdgivare som anges i 1 § oberoende av på vilket sätt personuppgifterna dokumenteras.

Vissa bestämmelser ska endast tillämpas av vårdgivare som behandlar patienters personuppgifter i system som är helt eller delvis automatiserade. Det gäller bestämmelserna i 3 kap. 2 § 4 och 7-20 §§, 4 kap. 2-12 §§, 6 kap. 1-3 §§ samt 7 kap. 1 § 4. De övriga bestämmelserna ska alltid tillämpas oberoende av hur personuppgifterna dokumenteras.

Förhållandet till personuppgiftslagen

1 kap. 3 § HSLF-FS 2016:40

Bestämmelser om hur personuppgiftslagen (1998:204) förhåller sig till patientdatalagen (2008:355) och till sådana föreskrifter som meddelats med stöd av den sistnämnda lagen finns i 1 kap. 4 § patientdatalagen.

Patientdatalagen och personuppgiftslagen

Av 1 kap. 4 § PDL framgår att personuppgiftslagen (1998:204) gäller vid sådan behandling av personuppgifter inom hälso- och sjukvården som är helt eller delvis automatiserad eller där uppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier, om inte annat följer av denna lag eller föreskrifter som meddelats med stöd av denna lag.

Definitioner

2 kap. 1 § HSLF-FS 2016:40

I dessa föreskrifter och allmänna råd avses med

autentisering	kontroll av uppgiven identitet
individanpassad vårdprocess	vårdprocess som är anpassad för en enskild patient
informationssystem	system som insamlar, bearbetar, lagrar eller distribuerar och presenterar information
informationssäkerhetspolicy	policy som anger mål och inriktning för samt styr en organisations informationssäkerhetsarbete
ledningssystem	system för att fastställa principer för ledning av verksamheten
patientjournal	en eller flera journalhandlingar som rör samma patient
process	serie aktiviteter som främjar ett bestämt ändamål eller ett avsett resultat
stark autentisering	kontroll av uppgiven identitet på två olika sätt
vårdgivare	statlig myndighet, landsting och kommun i fråga om sådan hälso- och sjukvård som myndigheten, landstinget eller kommunen har ansvar för samt annan juridisk person eller enskild näringsidkare som bedriver hälso- och sjukvård
vårdprocess	process avseende hälso- och sjukvård som hanterar ett eller flera relaterade hälsoproblem eller hälsotillstånd i syfte att främja ett avsett resultat

Definitionerna i 2 kap. 1 § HSLF-FS 2016:40 kommenteras inte särskilt utan här hänvisas i stället till kommentaren till den föreskrift eller det allmänna råd där definitionen förekommer.

Ledningssystem

3 kap. 1 § HSLF-FS 2016:40

Av Socialstyrelsens föreskrifter och allmänna råd (SOSFS 2011:9) om ledningssystem för systematiskt kvalitetsarbete framgår att varje vårdgivare ansvarar för att det finns sådana processer och rutiner som behövs för att säkerställa att verksamheten uppfyller de krav som ställs i dessa föreskrifter.

Vad är ett ledningssystem?

Ett ledningssystem är ett system för att fastställa principer för ledning av en verksamhet. Ledningssystemet gör det möjligt för ledningen att styra verksamheten så att rätt sak görs vid rätt tillfälle och på rätt sätt. I Socialstyrelsens föreskrifter och allmänna råd (SOSFS 2011:9) om ledningssystem för systematiskt kvalitetsarbete regleras att varje vårdgivare ska ansvara för att det finns ett ledningssystem för verksamheten. Ledningssystemet ska användas för att systematiskt och fortlöpande utveckla och säkra verksamhetens kvalitet (3 kap. 1 § SOSFS 2011:9).

Vårdgivaren ska med stöd av ledningssystemet planera, leda, kontrollera, följa upp, utvärdera och förbättra verksamheten (3 kap. 2 § SOSFS 2011:9). Vårdgivaren ska fastställa de processer och rutiner som behövs för att säkra verksamhetens kvalitet (4 kap. 2-4 §§ SOSFS 2011:9). Kvalitet definieras i SOSFS 2011:9 som att en verksamhet uppfyller de krav och mål som gäller för verksamheten enligt lagar och andra föreskrifter om hälso- och sjukvård och beslut som har meddelats med stöd av sådana föreskrifter. Bestämmelsen i 3 kap. 1 § HSLF-FS 2016:40 beskriver vårdgivarens ansvar för att det finns sådana processer och rutiner som behövs för att verksamheten uppfyller alla de krav som ställs i HSLF-FS 2016:40. Det är alltså genom ledningssystemet för systematiskt kvalitetsarbete som kraven i dessa föreskrifter ska säkerställas.

Ledningssystemet ska anpassas till verksamhetens inriktning och omfattning (4 kap. 1 § SOSFS 2011:9). En verksamhet som är särskilt riskfylld eller komplicerad kan behöva mer styrning i form av fler processer och rutiner än en mindre riskfylld verksamhet. En verksamhet som omfattar många olika delar av hälso- och sjukvård kan behöva arbeta fram fler processer och rutiner än en verksamhet som är av mer begränsad inriktning eller omfattning.

I Socialstyrelsens handbok ”Ledningssystem för systematiskt kvalitetsarbete - Handbok för tillämpningen av föreskrifter och allmänna råd (SOSFS 2011:9) om ledningssystem för systematiskt kvalitetsarbete” finns värdefullt stöd. Handboken kan laddas ner från Socialstyrelsens webbplats.

Informationssäkerhet är en del av ledningssystemet för systematiskt kvalitetsarbete

Ett övergripande ledningssystem i en verksamhet kan innehålla flera delsystem för olika ändamål, exempelvis miljö, kvalitet eller informationssäkerhet. Ledningssystemet för systematiskt kvalitetsarbete ska innehålla de processer och rutiner som krävs för att säkerställa kraven på informationssäkerhet.

Tillgänglighet, riktighet, konfidentialitet och spårbarhet

3 kap. 2 § HSLFS-FS 2016:40

Vårdgivaren ska genom ledningssystemet säkerställa att

1. dokumenterade personuppgifter hos vårdgivaren är åtkomliga och användbara för den som är behörig (tillgänglighet),
2. personuppgifterna är oförvanskade (riktighet),
3. obehöriga inte ska kunna ta del av personuppgifterna (konfidentialitet), och
4. åtgärder kan härledas till en användare (spårbarhet) i informationssystem som är helt eller delvis automatiserade.

Allmänna råd
Vårdgivaren bör använda svenska standarder för informationssäkerhet då ledningssystemet byggs upp. Sådana standarder kan vara standarder i ISO/IEC 27000-serien.

Bestämmelsen tar sikte på vårdgivarens ansvar för att genom processer och rutiner i ledningssystemet för systematiskt kvalitetsarbete säkerställa de grundläggande informationssäkerhetsaspekterna tillgänglighet, riktighet, konfidentialitet och spårbarhet. Begreppen är centrala i arbetet för att nå en god informationssäkerhet.

Tillgänglighet

Tillgång till personuppgifter i hälso- och sjukvården vid rätt tillfälle är en förutsättning för att enskilda patienter ska få en god och säker vård. Uppgifterna behöver vara tillgängliga som underlag för viktiga och i många fall tidskritiska beslut. Tillgängligheten säkerställs bland annat genom att vårdgivaren vid tilldelning av behörigheter ser till att rätt person har tillgång till rätt information (4 kap. 1-3 §§ HSLF-FS 2016:40). Tillgängligheten säkerställs också genom vårdgivarens planering av hur verksamheten ska bedrivas vid en funktionsstörning (3 kap. 11 § HSLF-FS 2016:40) och genom kravet på att de uppgifter som finns dokumenterade i en patientjournal ska finnas tillgängliga på ett överskådligt sätt för behörig hälso- och sjukvårdspersonal (5 kap. 1 § HSLF-FS 2016:40).

Riktighet

Vårdgivaren ska genom ledningssystemet säkerställa att personuppgifterna är oförvanskade, det vill säga hur uppgifternas riktighet ska upprätthållas i verksamheten. Det är nödvändigt att det inom vårdgivarens verksamhet finns en tillit till att dokumentationen är korrekt och användbar. Att innehållet i patientjournalen är korrekt och oförvanskat är en förutsättning för att den ska kunna bidra till en god och säker vård av patienten. Riktigheten säkerställs bland annat genom att rättelse och förstöring av en patientjournal görs enligt 3 kap. 14 § och 8 kap. 3-4 §§ PDL. Riktigheten säkerställs också genom vårdgivarens styrning av behörigheter (4 kap. 1-3 §§ HSLF-FS 2016:40) och genom rutiner för signering av journalanteckningar (6 kap. 4 § HSLF-FS 2016:40).

Konfidentialitet

Vårdgivaren ska genom ledningssystemet säkerställa att obehöriga inte ska kunna ta del av de personuppgifter som behandlas inom den verksamhet som vårdgivaren bedriver. Detta ställer höga krav på att vårdgivaren har de processer och rutiner som behövs för att förhindra obehörig åtkomst, utan att minska uppgifternas tillgänglighet.

Skydd mot obehörig åtkomst säkerställs bland annat genom att vårdgivaren vid kommunicering via öppna nät (exempelvis Internet) ser till att åtkomsten föregås av en så kallad stark autentisering (3 kap. 15 § HSLF-FS 2016:40).

Spårbarhet

Vårdgivaren ska genom ledningssystemet säkerställa att åtgärder kan härledas till en användare (spårbarhet) i informationssystem som är helt eller delvis automatiserade. Bestämmelsen gäller enbart för vårdgivare som använder sig av informationssystem som är helt eller delvis automatiserade.

Svenska standarder för informationssäkerhet

Vårdgivaren bör använda svenska standarder för informationssäkerhet då ledningssystemet byggs upp. Sådana standarder kan vara standarder i ISO/IEC 27000-serien, till exempel SS-ISO/IEC 27001:2014.

3 kap. 3 § HSLF-FS 2016:40

En vårdgivares användning av en svensk standard för informationssäkerhet får inte ersätta dennes skyldighet att uppfylla kraven i dessa föreskrifter.

En vårdgivare kan inte förlita sig på att en standard hanterar alla de krav som ställs i HSLF-FS 2016:40. Samtliga krav gäller således oavsett vilken standard vårdgivaren valt att använda sig av.

Informationssäkerhetspolicy

3 kap. 4 § HSLF-FS 2016:40

Vårdgivaren ska ansvara för att det finns en informationssäkerhetspolicy. Den ska ange vårdgivarens övergripande mål för och inriktning på verksamhetens arbete med informationssäkerhet i syfte att säkerställa personuppgifternas tillgänglighet, riktighet, konfidentialitet och spårbarhet.

Vad är en informationssäkerhetspolicy?

Informationssäkerhetspolicyn ska ange vårdgivarens övergripande mål och inriktning på verksamhetens arbete med informationssäkerhet i syfte att säkerställa personuppgifternas tillgänglighet, riktighet, konfidentialitet och spårbarhet. Informationssäkerhetspolicyn utgör vårdgivarens gemensamma plattform för detta arbete.

För att kunna säkra informationen behöver varje verksamhet arbeta med att införa de säkerhetsåtgärder som krävs för att nå ledningens specifika säkerhets- och verksamhetsmål. Säkerhetsåtgärderna kan beskrivas i riktlinjer, processer, rutiner, organisationsstrukturer samt hård- och mjukvarufunktioner.

Alla vårdgivare ska ha en informationssäkerhetspolicy, även de som inte dokumenterar patientuppgifter elektroniskt (1 kap. 2 § HSLF-FS 2016:40).

Hur kan en informationssäkerhetspolicy utformas?

De svenska standarderna om informationssäkerhet kan användas som stöd för att utforma en informationssäkerhetspolicy. Exempel på vad en informationssäkerhetspolicy kan innehålla är ett uttryck för ledningens viljeinriktning, det vill säga varför det är viktigt med informationssäkerheten, samt en kort beskrivning av hur viljeinriktningen ska uppnås. Policyn kan även innehålla en kort beskrivning av ansvarsförhållandena inom informationssäkerheten, en förklaring av viktiga begrepp samt en redogörelse för vem som ansvarar för policyn samt hur den ses över och revideras. Exempel på hur en informationssäkerhetspolicy kan utformas finns att hämta på Myndigheten för samhällsskydd och beredskaps webbplats.

Riskanalyser

3 kap. 5 § HSLF-FS 2016:40

Vårdgivaren ska fortlöpande bedöma om det i verksamheten finns risker för händelser som kan medföra att kraven i dessa föreskrifter inte uppfylls.

För varje sådan händelse ska vårdgivaren

1. uppskatta sannolikheten för att händelsen inträffar, och
2. bedöma vilka negativa konsekvenser som skulle kunna bli följden av händelsen.

Riskanalyserna ska dokumenteras.

Riskanalyser av vårdgivarens behandling av personuppgifter

Riskanalyser ger kunskap om vilka åtgärder som behövs för att öka informationssäkerheten och innebär att vårdgivaren arbetar förebyggande. Analyser ska göras för att identifiera händelser som skulle kunna inträffa och som gör att vårdgivaren inte kan leva upp till kraven i HSLF-FS 2016:40. Riskanalyserna innebär att sannolikheten för att en händelse ska inträffa uppskattas och att en bedömning görs av vilka negativa konsekvenser som skulle kunna bli följden av händelsen.

Riskanalyserna ska genomföras fortlöpande. Omständigheter som påverkar vad fortlöpande innebär i det enskilda fallet är till exempel verksamhetens inriktning eller om hela eller delar av verksamheten tidigare bedömts vara särskilt riskfylld. Riskanalyser kan även behöva genomföras innan förändringar av en verksamhet eller inför förändringar av personalens sammansättning och innan nya informationssystem, arbetssätt eller metoder börjar tillämpas och användas.

I handboken ”Riskanalys och händelseanalys – analysmetoder för att öka patientsäkerheten” finns instrument som beskriver hur bland annat riskanalyser kan genomföras. Handboken riktar sig till alla som arbetar med kvalitet och patientsäkerhet i landsting, regioner, kommuner och hos andra vårdgivare. Analysmetoderna som beskrivs i handboken är utvecklade för att identifiera brister i verksamheten som kan riskera patientsäkerheten. Till handboken finns checklistor och mallar som kan ge stöd i det praktiska analysarbetet. Handboken finns att ladda ner och beställa på Sveriges Kommuner och Landstings webbplats.

Ledning och samordning av informationssäkerhetsarbetet

3 kap. 6 § HSLF-FS 2016:40

Vårdgivaren ska utse en eller flera personer som ska leda och samordna informationssäkerhetsarbetet. Den eller de som utses ska minst en gång om året sammanställa information om arbetet till vårdgivaren.

Sammanställningen ska innehålla information om de

1. riskanalyser som har gjorts av informationssäkerheten,
2. incidenter som har påverkat informationssäkerheten och som medfört eller hade kunnat medföra vårdskada,
3. uppföljningar som har gjorts, och
4. förbättringsåtgärder som har vidtagits.

Allmänna råd
Den eller de personer som utses att leda och samordna informationssäkerhetsarbetet bör få en sådan ställning i organisationen att arbetet kan prioriteras och utföras effektivt.

Sammanställa information till vårdgivaren

Det är viktigt att det finns ett tydligt utpekat ansvar för informationssäkerhetsarbetet samt att arbetet är ändamålsenligt och följer bestämmelserna i 28 § hälso- och sjukvårdslagen (1982:763), HSL, om att ledningen ska vara organiserad så att den tillgodoser hög patientsäkerhet, god kvalitet och främjar kostnadseffektivitet. Vårdgivaren ska utse en eller flera personer som ska leda och samordna informationssäkerhetsarbetet. Verksamhetens storlek och inriktning kan vara faktorer som påverkar vid bedömningen av om ansvaret för att leda och samordna informationsarbetet ska läggas på en eller flera personer. Vårdgivaren är alltså fri att antingen utse särskilda personer som enbart arbetar med informationssäkerhet eller lägga ut uppgiften till exempelvis en eller flera verksamhetschefer.

Den eller de som ansvarar för informationssäkerhetsarbetet ska minst en gång om året sammanställa information till vårdgivaren om de riskanalyser som har gjorts av informationssäkerheten, incidenter som har påverkat informationssäkerheten och som medfört eller hade kunnat medföra vårdskada, uppföljningar som har gjorts och förbättringsåtgärder som har vidtagits. Formen för sammanställningen får anpassas till verksamhetens utformning och storlek.

Den eller de personer som utses att leda och samordna informationssäkerhetsarbetet bör få en sådan ställning i organisationen att arbetet kan prioriteras och utföras effektivt. Det innebär att den eller de som utsetts behöver ha möjlighet och befogenhet att fullgöra uppgiften samt att ansvaret är känt och förankrat i verksamheten.

Ta i drift informationssystem

3 kap.7 § HSLF-FS 2016:40

Vårdgivaren ska dokumentera de beslut som har fattats om att ta i drift informationssystem som används för behandling av personuppgifter.

Allmänna råd

Vårdgivaren bör ta fram en process för hantering av idrifttagandet.

Ett beslut om att ta i drift ett informationssystem bör innehålla

– en beskrivning av systemets syfte och hur det ska användas, och
– en validering av att systemet följer informationssäkerhetspolicyn, krav på testning och andra av vårdgivaren angivna säkerhetskrav som kan vara relevanta.

Ett dokumenterat beslut

Ett informationssystem som används i verksamheten kan tillfälligt tas ur drift för att underhållas, uppgraderas eller ändras i något avseende och därefter tas i drift igen. Ett informationssystem kan också tas i drift och vara helt nytt och inte tidigare använt i vårdgivarens verksamhet. Oavsett tidigare situation måste vårdgivaren varje gång ett informationssystem som behandlar personuppgifter tas i drift dokumentera ett beslut om det. När ett informationssystem tas i drift finns risk för att det innehåller fel som leder till störningar eller avbrott i driften. Störningar i driften kan leda till att personuppgifter som informationssystemet behandlar inte blir tillgängliga för hälso- och sjukvårdspersonalen eller att uppgifter blir felaktiga. Genom att dokumentera de beslut om som har fattats om att ta i drift informationssystem som behandlar personuppgifter minskas risken för att fel inte upptäcks.

En process för säkrare beslut

I allmänna råd anges att vårdgivaren bör ta fram en process för hantering av idrifttagandet. I samma allmänna råd anges också att ett beslut om att ta i drift ett informationssystem bör innehålla en beskrivning av systemets syfte och hur det ska användas och en validering av att systemet följer informationssäkerhetspolicyn, krav på testning och andra av vårdgivaren angivna säkerhetskrav som kan vara relevanta. En process kan underlätta arbetet med att skapa en jämn kvalitet i besluten över tiden. Det kan också vara nödvändigt att kontrollera att informationssystemets hård- och mjukvara är kompatibla med andra komponenter i IT-miljön. Informationssystem har ofta beroenden till andra informationssystem i en IT-miljö och därför kan det vara lämpligt att testa förmågan att fungera tillsammans med dessa innan det nya informationssystemet tas i drift. Olika informationssystem ställer olika krav på kapacitet och prestanda för att fungera väl i en IT-miljö. Det kan gälla krav på nyttjande av minnesdiskutrymme eller nätverkskapacitet. Dessa krav kan vårdgivaren behöva förstå och säkra upp resurser för innan informations-

systemet tas i drift. Annars är risken stor att informationssystemet inte fungerar som avsett när det tas i drift.

IT-tjänster som utförs av en extern leverantör

Om driften av ett informationssystem som hanterar personuppgifter utförs av en extern leverantör så är vårdgivaren fortfarande skyldig att dokumentera beslutet om att informationssystemet ska tas i drift. Vårdgivaren kan ställa krav på leverantören att arbeta enligt en process där ett dokumenterat beslut från vårdgivaren alltid krävs innan leverantören kan gå vidare i sitt arbete med att ta i drift ett informationssystem som hanterar personuppgifter.

Driftdokumentation

3 kap. 8 § HSLF-FS 2016:40

Vårdgivaren ska säkerställa att det finns uppdaterad och tillgänglig driftdokumentation för varje informationssystem som används för behandling av personuppgifter.

Vad menas med driftdokumentation?

Driftdokumentation kan omfatta hur olika komponenter av IT-miljön är konfigurerade, exempelvis databaser, servrar och nätverk. Den kan även beskriva hur servrar startas igång igen vid ett driftstopp, var servrar är fysiskt placerade, hur backuper ska hanteras, hur övervakning av aktiviteter ska koordineras, beroenden till andra informationssystem med mera. Dokumentationen säkerställer även att all driftpersonal vet hur man ska göra och att alla gör på samma sätt, samt att personberoendet minskar.

Felaktigheter i eller avsaknad av driftdokumentation kan leda till att IT-miljön hanteras fel, med risk för driftstopp som följd. Det kan också leda till att driftproblem blir onödigt omfattande.

För de informationssystem som behandlar personuppgifter är det viktigt att driften fungerar väl så att uppgifter om patienter går att läsa och skriva i informationssystemet. Störningar i driften kan leda till att personuppgifter som informationssystemet behandlar inte blir tillgängliga för hälso- och sjukvårdspersonalen eller att uppgifter blir felaktiga.

Uppdaterad och tillgänglig driftdokumentation

Vårdgivaren ska säkerställa att det finns uppdaterad och tillgänglig driftdokumentation för varje informationssystem som används för behandling av personuppgifter. Att dokumentera driften för de informationssystem som behandlar personuppgifter är inte en engångsaktivitet. Dokumentationen ska vara uppdaterad, vilket innebär att förändringar i driftmiljön ska återspeglas i driftdokumentationen.

Driftdokumentationen ska även vara tillgänglig för behöriga användare som behöver nå den. Det ställer olika krav på hanteringen av driftdoku-

mentation beroende på om den finns lagrad elektroniskt eller på papper. Oavsett format måste vårdgivaren säkerställa att driftdokumentationen är tillgänglig.

IT-tjänster som utförs av en extern leverantör

Om driften av ett informationssystem som behandlar personuppgifter sker genom en extern leverantör så är vårdgivaren fortfarande skyldig att säkerställa att driften dokumenteras och är uppdaterad, tillförlitlig och tillgänglig. Detta kan ske genom att vårdgivaren ställer krav på leverantören som skrivs in i ett kontrakt. Även om vårdgivaren byter leverantör eller om leverantören upphör med sin verksamhet ska vårdgivaren säkerställa att driftdokumentationen är tillgänglig. Att en extern leverantör kontrakteras för att utföra arbetsuppgifter åt vårdgivaren fråntar inte vårdgivaren något ansvar som följer av denna föreskrift.

Upphandling och utveckling

3 kap. 9 § HSLF-FS 2016:40

Vårdgivaren ska säkerställa att kraven i dessa föreskrifter uppfylls vid upphandling eller egenutveckling av informationssystem som används för behandling av personuppgifter.

Kravställande vid upphandling eller egenutveckling

Vid upphandling eller egenutveckling av informationssystem som behandlar personuppgifter ska vårdgivaren säkerställa att kraven i dessa föreskrifter uppfylls. Syftet är att informationssäkerheten ska vara en integrerad del av de informationssystem som används för behandling av personuppgifter. Vårdgivaren ska säkerställa att informationssystem som används för behandling av personuppgifter får ett tillräckligt skydd i fråga om personuppgifternas tillgänglighet, riktighet, konfidentialitet och spårbarhet. Om vårdgivaren köper ett informationssystem som används för behandling av personuppgifter från en leverantör ska vårdgivaren säkerställa att kraven i HSLF-FS 2016:40 uppfylls i upphandlingskraven.

Om vårdgivaren själv utvecklar ett informationssystem som hanterar patientuppgifter behöver vårdgivaren se till att säkerhetskraven är identifierade och beslutade innan utvecklingen av informationssystemet startar. Vårdgivaren kan säkerställa att verksamheten använder en systemutvecklingsmetod som tar informationssäkerhetskraven i beaktande under utvecklingens gång, exempelvis i kravställandet och testaktiviteter.

Ett informationssystem som behandlar personuppgifter kan vara en medicinteknisk produkt. Vid egentillverkning av medicintekniska produkter ska vårdgivaren leva upp till kraven i 5 kap. Socialstyrelsens föreskrifter och allmänna råd (SOSFS 2008:1) om användning av medicintekniska produkter i hälso- och sjukvården för att få användas i vården av patienter. En medicin-

teknisk produkt används för att förebygga, övervaka, behandla eller lindra en sjukdom, påvisa, övervaka, behandla, lindra eller kompensera en skada eller ett funktionshinder, undersöka, ändra eller ersätta anatomi eller en fysiologisk process, eller kontrollera befruktning (2 § lagen [1993:584] om medicintekniska produkter). Exempel på informationssystem som kan vara en medicinteknisk produkt är journalsystem, medicinska informationssystem eller medicinska instrumentdatasystem.

3 kap.10 § HSLF-FS 2016:40

Vårdgivaren ska vid utveckling, idrifttagande och ändring av informationssystem som används för behandling av personuppgifter säkerställa att personuppgifternas tillgänglighet, riktighet, konfidentialitet och spårbarhet inte riskeras.

Vårdgivaren ska vidare säkerställa att ett informationssystem testas innan det tas i drift.

Allmänna råd

Tester bör göras i miljöer som är åtskilda från produktionsmiljöer.

Informationen i testmiljöerna bör inte innehålla personuppgifter.

Ändringar i informationssystemen bör planeras i förväg. Innan en ändring görs bör vårdgivaren bedöma tänkbara effekter på informationssäkerhet och funktion.

Vårdgivaren bör godkänna ändringar innan de tas i drift i informationssystemen.

Utveckling, idrifttagande och ändring av informationssystem

Risken för fel vid utveckling, idrifttagande och ändring av informationssystem är stor. Vid utveckling, idrifttagande och ändring av ett informationssystem ska vårdgivaren säkerställa att personuppgifternas tillgänglighet, riktighet, konfidentialitet och spårbarhet inte riskeras.

Test innan ett informationssystem tas i drift

Vårdgivaren ska vidare säkerställa att ett informationssystem testas innan det tas i drift. Det är inte alltid möjligt att förutse hur en ändring kommer att fungera när den tas i drift. Det finns många beroenden runt ett informationssystem och dess IT-miljö och även en mindre ändring kan få oöverblickbara konsekvenser.

Test i separat miljö

Tester bör göras i miljöer som är åtskilda från produktionsmiljöer. Informationen i testmiljöerna bör inte innehålla personuppgifter. Ändringar i informationssystemen bör planeras i förväg. Innan en ändring görs bör vårdgivaren bedöma tänkbara effekter på informationssäkerhet och funktion. Vårdgivaren bör godkänna ändringar innan de tas i drift i informationssystemen.

Testaktiviteter kan orsaka förändringar som inte är avsedda i informationssystemets programvara eller dess information. Otillräckligt testade eller felaktiga förändringar i informationssystemet kan få allvarliga konsekvenser vid vård och behandling av patienter. Det kan vara bra att testmiljön liknar driftmiljön så mycket som möjligt, men vårdgivaren måste kunna säkerställa att obehöriga inte kan ta del av personuppgifterna i testmiljön.

Planering av verksamhet vid funktionsstörning

3 kap. 11 § HSLF-FS 2016:40

Vårdgivaren ska planera för hur hälso- och sjukvårdsverksamheten ska bedrivas om informationssystem som används för behandling av personuppgifter inte fungerar.

Vårdgivaren ska vidare planera för hur återstart eller återställande ska göras efter en sådan funktionsstörning.

Vårdgivaren ska dokumentera planeringen.

Allmänna råd

Planeringen bör testas med en periodicitet som har fastställts efter genomförd riskanalys.

Vid förändring i verksamheten eller av riskbilden bör planeringen uppdateras och testas igen.

Planering vid funktionsstörning

I bestämmelsen ställs krav på vårdgivaren att planera för hur hälso- och sjukvårdsverksamheten ska bedrivas om informationssystem som används för behandling av personuppgifter inte fungerar.

En funktionsstörning är en händelse som har en negativ inverkan på möjligheten att bedriva verksamheten. En funktionsstörning kan orsakas av exempelvis virusangrepp (skadlig kod), strömavbrott, översvämning eller brand. Det kan också vara händelser som fel i hård- eller mjukvara i informationssystemet eller IT-miljön som leder till omfattande avbrott i informationssystemets drift. Vid utlokaliserad drift behöver vårdgivaren även planera för motsvarande risker hos driftleverantören.

Oavsett orsak till avbrottet så måste situationen hanteras och hälso- och sjukvårdsverksamheten kunna bedrivas på alternativa sätt för att inte riskera patientsäkerheten. Vid händelse av en funktionsstörning behöver verksamheten veta hur den ska agera för att minska de negativa effekterna på människor och verksamheten.

Ett arbete med förberedelser behöver göras innan en funktionsstörning är ett faktum. En del i planering av verksamhet vid funktionsstörning kan vara att definiera olika händelser eller situationer som ska betecknas som en funktionsstörning och som när de inträffar ska leda till att planen aktiveras.

Syftet med planering av verksamhet vid funktionsstörning

Olika händelser kan leda till att vårdgivarens informationssystem inte fungerar och därmed att personuppgifter inte är tillgängliga. Att ha tillgång till riktiga och rätt personuppgifter är centralt i arbetet med att erbjuda en god och säker vård. Vårdgivaren behöver därför planera för hur hälso- och sjukvårdsverksamheten ska bedrivas om informationssystem som används för behandling av personuppgifter inte fungerar.

Målet med planeringen är att hälso- och sjukvårdsverksamheten ska kunna fortsätta bedrivas trots händelse av en mindre eller större störning i driften av de informationssystem som används för behandling av personuppgifter.

Syftet med planering av verksamhet vid funktionsstörning är att skydda personuppgifternas tillgänglighet, riktighet, konfidentialitet och spårbarhet för att säkerställa hälso- och sjukvårdsverksamhetens kontinuitet och en patientsäker vård. En kombination av förebyggande och återställande skyddsåtgärder kan hjälpa verksamheten att fortsätta bedriva hälso- och sjukvårdsverksamheten trots avsaknad av de informationssystem som används för behandling av personuppgifter.

Planering för återstart eller återställande av informationssystem

Vårdgivaren ska även planera hur återstart eller återställande ska göras efter en funktionsstörning. Rutiner för återställande beskriver de åtgärder som krävs för att återgå till normal verksamhet. Vid händelse av ett större avbrott kan vårdgivaren bli tvungen att prioritera i vilken ordning informationssystem som används för behandling av personuppgifter ska återställas. För att veta vilken prioritering som är lämplig kan en analys göras av de funktioner i verksamheten som är mest kritiska ur ett patientsäkerhetsperspektiv.

Testa planering och uppdatera vid förändring

Planeringen bör testas med en periodicitet som har fastställts efter genomförd riskanalys. Vid förändring i verksamheten eller av riskbilden bör planeringen uppdateras och testas igen. Planeringen kan behöva uppdateras och anpassas till förändringar i omvärlden eller inom verksamheten för att vara aktuell.

Säkerhetskopiering

3 kap. 12 § HSLF-FS 2016:40

Vårdgivaren ska säkerställa att personuppgifter som behandlas i informationssystem säkerhetskopieras med en fastställd periodicitet.

Säkerhetskopiorna ska förvaras på ett säkert sätt, väl åtskilda från originaluppgifterna.

Vad innebär säkerhetskopiering?

Säkerhetskopiering är en metod för att säkerställa att ingen information går förlorad om datorer eller andra informationsbärare går sönder, eller om något annat skulle påverka den lagrade informationen.

Säkerhetskopieringen är ett viktigt moment för att säkerställa personuppgifternas tillgänglighet, vilket är ett av de grundläggande begreppen inom informationssäkerhet. Vårdgivaren ska säkerställa att personuppgifter säkerhetskopieras med en i förväg fastställd periodicitet. Det är viktigt att ingen information kan gå förlorad.

Hur ska säkerhetskopiorna förvaras?

Personuppgifter lagras vanligtvis i databaser och i fysiska servrar som är placerade i datorhallar eller motsvarande, beroende på verksamhetens storlek och omfattning. För mindre vårdgivare kan det röra sig om en vanlig dator som är placerad i anslutning till mottagningen. Säkerhetskopiorna ska förvaras på ett säkert sätt, väl åtskilda från originaluppgifterna. De säkerhetskopior som skapas ska inte förvaras tillsammans med originaluppgifterna, som vanligtvis finns i en server. Hur säkerhetskopiorna hålls väl åtskilda kan variera beroende på vilken typ av information som avses, vilken vårdgivare det rör sig om och vad som framkommer vid en riskanalys.

3 kap. 13 § HSLF-FS 2016:40

Vårdgivaren ska besluta om hur länge säkerhetskopiorna ska sparas och hur ofta återläsningstester av kopiorna ska göras.

Allmänna råd
Hur ofta återläsningstester ska göras bör styras av resultaten av återkommande riskanalyser.

Hur länge ska säkerhetskopiorna sparas?

Säkerhetskopiorna måste bevaras under så lång tid som vårdgivaren bedömer att informationen måste kunna återskapas och så lång tid som olika författningar kräver. Återläsningstest görs för att kontrollera kopiornas kvalitet och för att bedöma hur lång tid det tar att återställa informationen. Tidsfaktorn kan vara viktig beroende på verksamhetens inriktning. Hur ofta återläsningstester ska göras bör styras av resultaten av återkommande riskanalyser enligt 2 kap. 5 § HSLF-FS 2016:40.

Fysiskt skydd av informationssystem

3 kap. 14 § HSLF-FS 2016:40

Vårdgivaren ska säkerställa att informationssystem som används för behandling av personuppgifter skyddas fysiskt mot skada, störning och obehörig åtkomst.

Allmänna råd
Informationssystemen bör förvaras i säkra utrymmen inom avgränsade skalskydd som har lämpliga säkerhetsavspärrningar och tillträdeskontroller.

Fysiska skyddsutrymmen

Målet med att fysiskt skydda informationssystem som behandlar personuppgifter är att förhindra obehörigt fysiskt tillträde, skador eller störningar på vårdgivarens uppgifter om patienter. Begreppet störning beskriver allt som innebär ett avbrott. Enligt SS-ISO/IEC 27002:2014 bör känsliga informationsbehandlingsresurser inrymmas i säkra utrymmen inom ett avgränsat skalskydd med lämpliga säkerhetsavspärrningar och tillträdeskontroller. Skalskydd kan till exempel vara avspärrningar, kortstyrda entréer eller bemannande receptioner. I SS-ISO/IEC 27002:2014 föreslås flera slags skalskydd som en verksamhet kan ta i beaktande i sin analys av lämpligt skalskydd.

Om personuppgifter som lagras i ett informationssystem inte skyddas från fysisk åtkomst eller skada kan det innebära risk för obehörig åtkomst till personuppgifterna eller att tillgängligheten till uppgifterna försämras. Vårdgivaren ska fortlöpande bedöma om det i verksamheten finns risker för händelser som kan medföra att kraven i dessa föreskrifter inte uppfylls (3 kap. 5 § HSLF-FS 2016:40).

Fysisk skada på informationssystem kan vara avsiktlig eller oavsiktlig. Exempel på hot som kan orsaka skada är brand, vattenläckage, elavbrott, explosion eller olika former av skador orsakade av människor såsom inbrott eller skadegörelse.

Det är viktigt att vårdgivaren säkerställer att skyddet även omfattar sådan utrustning som är nödvändig för att informationssystemet ska fungera som avsett, såsom kablar för strömförsörjning eller nätverk.

Ett lämpligt fysiskt skydd kan även behövas för datorer i vårdgivarens lokaler, exempelvis på läkemedelsvagnar och i expeditioner. En dator på vilken en behörig person ur hälso- och sjukvårdspersonalen är inloggad mot ett informationssystem som behandlar personuppgifter, får inte lämnas obevakad för obehöriga att se informationen.

Risk för skador inom skalskyddet

Den fysiska utrustningen i exempelvis en datorhall kan störas om temperatur, fuktförhållanden eller strömförsörjning inte är rätt anpassade till de krav som är nödvändiga för att utrustningen ska fungera. Det kan påverka informationssystem negativt så de störs eller slutar fungera. Servrar genererar mycket värme som kan leda till överhettning och driftstopp om värmen inte leds bort och kyla tillförs på ett effektivt sätt.

En UPS (Uninterruptible Power Supply) förhindrar plötsliga avbrott i strömförsörjningen vid exempelvis strömavbrott och säkerställer en jämn strömförsörjning som är anpassad för utrustningen i fråga.

Ytterligare exempel på skalskydd är dörrar som skyddar från brand. Brand kan bekämpas med olika metoder, exempelvis gas, skum eller vatten som medför olika risker för personer och utrustning som behöver analyseras. Dörrarna kan ha lås och passagesystem där det går att styra vilka som ges tillgång till datorhallen. Vårdgivaren kan även behöva tänka på hur närmiljön runt informationssystemet inom ett skalskydd ser ut, exempelvis om farligt eller brännbart material förvaras på betryggande avstånd.

IT-tjänster som utförs av en extern leverantör

En vårdgivare kan anlita en extern leverantör att fysiskt hantera informationssystemets servrar i sina lokaler. En vårdgivare som anlitar en leverantör kan hos denne ha en egen datorhall för sin IT-utrustning eller dela datorhall med andra verksamheter. Oavsett lösning måste vårdgivaren säkerställa att leverantören lever upp till kraven på fysisk skydd i HSLF-FS 2016:40.

Behandling av personuppgifter i öppna nät

3 kap. 15 § HSLF-FS 2016:40

Om vårdgivaren använder öppna nät vid behandling av personuppgifter, ska denne ansvara för att

1. överföring av uppgifterna görs på ett sådant sätt att inte obehöriga kan ta del av dem, och
2. elektronisk åtkomst eller direktåtkomst till uppgifterna föregås av stark autentisering.

Vad innebär öppna nät?

Öppna nät kan beskrivas som datornätverk som en enskild användare har tillgång till, exempelvis Internet. Genom att utnyttja Internet är det möjligt att enkelt och effektivt kommunicera text, ljud och bild. Om inte vårdgivaren vidtar särskilda skyddsåtgärder kommer dock informationen att överföras

oskyddad. Därför är det nödvändigt med specifika säkerhetslösningar för att minska risken för att obehöriga personer får tillgång till informationen.

Skydd mot obehörig åtkomst

Om en vårdgivare gör uppgifter om patienter tillgängliga över öppna nät, exempelvis för att hälso- och sjukvårdspersonalen ska kunna utföra arbetsuppgifter på distans, måste det göras på ett sådant sätt att ingen obehörig kan nå uppgifterna. I praktiken innebär det bland annat att uppgifter om patienter måste överföras genom en krypterad förbindelse eller genom att kryptera uppgifterna. Teknikutvecklingen medför att krypteringsmetoderna hela tiden kan behöva förbättras för att minimera risken för obehörig åtkomst.

Vad innebär skydd med starkt autentisering?

För att en behörig användare ska få tillgång till personuppgifter via öppna nät måste vårdgivaren se till att åtkomsten föregås av en så kallad stark autentisering. Det innebär att vårdgivaren använder inloggningslösningar som ställer krav på att identiteten kontrolleras på minst två olika sätt, exempelvis:

- med någonting användaren kan − till exempel lösenord eller pinkod
- med någonting användaren har − till exempel kodbox, certifikat, smartkort, engångskoder eller mobiltelefon
- med hjälp av användaren själv – till exempel fingeravtryck eller avläsning av iris.

En etablerad metod för stark autentisering är att använda en e-legitimation. Det är en identitetshandling i elektronisk form som vid elektronisk kommunikation används för legitimering och underskrift. E-legitimationen kan lagras på en dator (certifikat på fil), på ett smartkort eller i en mobiltelefon.

Med hjälp av e-legitimationen och det tillhörande lösenordet (exempelvis en pinkod) skapas förutsättningar för en stark autentisering. Denna metod används bland annat av Skatteverket och Försäkringskassan för att låta kunderna identifiera sig och signera sina handlingar när de använder e-tjänster, till exempel vid deklaration och begäran om föräldraledighet.

Överföra uppgifter om patienter via fax

Telenätet räknas som ett öppet nät. Faxar använder telenätet för sin kommunikation. Därför gäller bestämmelserna om öppna nät också överföring av uppgifter om patienter med hjälp av fax. Detta innebär att det kan vara svårt att överföra uppgifter via fax på ett sätt som uppfyller föreskrifternas krav på säkerhet. Den vårdgivare som använder fax för sådana överföringar måste förvissa sig om att ingen obehörig kan nå uppgifter om patienter. Detta innebär att uppgifter om patienter som faxas ska vara krypterade och att åtkomsten till innehållet i faxet ska föregås av stark autentisering.

Behandling av personuppgifter i öppna nät – undantag

3 kap. 16 § HSLF-FS 2016:40

Vårdgivaren får efter att ha gjort en behovs- och riskanalys besluta om undantag från kraven i 15 § 1 vid överföring av påminnelser och kallelser till vård och behandling som riktar sig till patienter.

Vårdgivaren ska dokumentera beslutet och behovs- och riskanalysen.

Undantag för påminnelser och kallelser

Undantag från kraven om skyddad överföring i 3 kap. 15 § 1 får göras då uppgifter om patienter ingår i påminnelser och kallelser. Det innebär att uppgifter om patienter i elektroniska påminnelser och kallelser som kommuniceras över öppna nätverk, exempelvis via sms eller e-post, inte behöver krypteras. Däremot behöver åtkomsten fortfarande föregås av stark autentisering. Det är inte fråga om ett beslut i varje enskilt fall då en påminnelse eller kallelse ska skickas ut med exempelvis e-post eller sms.

Undantaget från kraven i 3 kap. 15 § 1 har tillkommit eftersom det anses praktiskt och smidigt både för vårdgivare och patienter med kallelser och påminnelser om besök i vården per sms eller e-post.

3 kap. 17 § HSLF-FS 2016:40

En överföring av en påminnelse eller en kallelse får

1. endast göras efter att patienten har gett sitt medgivande, och
2. inte avslöja detaljer om patientens hälsotillstånd eller andra personliga förhållanden.

Allmänna råd

Vårdgivaren bör ha rutiner som säkerställer att patientens kontaktuppgifter är riktiga och aktuella.

En överföring av en påminnelse eller en kallelse får inte avslöja detaljer om en patients hälsotillstånd eller andra personliga förhållanden. En överföring av en påminnelse eller en kallelse får endast göras efter att patienten har gett sitt medgivande. Vårdgivaren bör ha rutiner som säkerställer att patientens kontaktuppgifter är riktiga och aktuella. Ett av de grundläggande kraven vid behandling av personuppgifter är att personuppgifter som behandlas ska vara riktiga, och om nödvändigt, aktuella (prop. 2007/08:126 s. 63).

Utvärdering av skyddet mot olovlig åtkomst

3 kap. 18 § HSLF-FS 2016:40

Vårdgivaren ska årligen utvärdera skyddet mot såväl intern som extern olovlig åtkomst till datornätverk och informationssystem som används för behandling av personuppgifter.

Årlig utvärdering

Vårdgivaren ska årligen utvärdera skyddet mot såväl intern som extern olovlig åtkomst till de datornätverk och informationssystem hos vårdgivaren som används för behandling av personuppgifter.

Aktiviteter i både nätverk och informationssystem kan loggas och övervakas för att upptäcka säkerhetsavvikelser som kan innebära hot mot skyddet av olovlig åtkomst. Personer som administrerar informationssystemet har ofta höga behörigheter som gör det möjligt att kringgå de behörighetskontroller och loggningsfunktioner som är inbyggda i informationssystemet. Det kan därför vara relevant att särskild uppmärksamma att administratörsbehörigheter används restriktivt.

Skydd av datornätverk

Datornätverk är ofta en nödvändig komponent för att ett informationssystem ska fungera som avsett. Datornätverk hanterar personuppgifter då de används för kommunikation mellan ett informationssystem som hanterar personuppgifter och en användare, eller mellan olika informationssystem. Kommunikation av personuppgifter genom nätverk kan ske inom vårdgivarens verksamhet eller mellan vårdgivaren och externa verksamheter.

Alla nätverk är föremål för regelbundna driftstörningar. Förlust av ett nätverk betyder ofta förlust av åtkomst till journalsystemet för verksamhetens användare.

Vårdgivaren kan på olika sätt skydda de datornätverk som hanterar personuppgifter mot obehörig åtkomst. Exempel på skydd för information som kommuniceras över datornätverk är kryptering samt begränsning av vilka datorer och servrar som kan anslutas till nätverket. En vårdgivares nätverk kan skyddas från andra nätverk, som till exempel Internet, med hjälp av brandväggar och andra skyddsåtgärder.

Trådlös anslutning till nätverk kan behöva särskild hantering för att kunna uppnå en tillräckligt hög säkerhetsnivå för kommunikation av personuppgifter då även de vanligast förekommande krypteringsmetoderna för trådlösa nätverk kan innebära att det är lätt för obehöriga att lyssna av trafiken.

Skydd av informationssystem

Exempel på skydd för informationssystem som behandlar personuppgifter är krav på stark autentisering med användning av e-legitimation vid inloggning

i informationssystemet. För att skyddet ska fungera som avsett är det viktigt att medarbetare hos vårdgivaren är medvetna om vikten av att inte låna ut sin e-legitimation eller sin pinkod till kollegor.

Flyttbart medium för informationslagring

3 kap. 19 § HSLF-FS 2016:40

Den vårdgivare som tillåter flyttbart medium för lagring av personuppgifter ska säkerställa att

1. obehöriga inte kan ta del av dem, och
2. uppgifterna inte går förlorade.

Skydd av flyttbart medium

Hos en vårdgivare kan det finnas behov av att lägga över personuppgifter som hanteras i ett informationssystem till ett flyttbart medium. Exempel på flyttbara medier är USB-minne, disk, minneskort, CD-skiva eller band. Om vårdgivaren tillåter denna hantering ska vårdgivaren säkerställa att det flyttbara mediet skyddas på ett sådant sätt att personuppgifter inte går förlorade eller görs tillgängliga för obehöriga att läsa.

För att skydda personuppgifterna på det flyttbara mediet kan vårdgivaren till exempel ställa krav på att tillstånd ska sökas innan enskilda inom verksamheten får använda flyttbara medier samt krav på att det är klarlagt vilka behörighetskrav som gäller för det flyttbara mediet. En vårdgivare kan därtill behöva ta fram rutiner för att säkerställa att personuppgifterna som lagts över på ett flyttbart medium tas bort från mediet när de inte längre behövs. Där det är tillämpbart kan vårdgivaren kräva kryptering för ett flyttbart medium.

Vad menas med medium?

Ett medium är en enhet som kan lagra information i olika former, exempelvis ljud, bild och text. Personuppgifter kan lagras på en mängd olika medier. Några exempel på lagringsmedier är hårddiskar, USB-minnen, läsplattor, diktafoner, CD-skivor, minneskort, magnetband, papper, videoband och mobiltelefoner. Ett lagringsmedium kan avvecklas av olika orsaker. Det kan gå sönder, bygga på en omodern och därmed oanvändbar teknik eller bli överflödigt på grund av förändrade arbetssätt.

Avveckling av medium för informationslagring

3 kap. 20 § HSLF-FS 2016:40

Medium för informationslagring som innehåller personuppgifter ska avvecklas på ett sådant sätt att uppgifterna inte kan läsas eller återskapas.

Olika metoder för olika medier

Beroende på medium så behöver vårdgivaren använda olika metoder när mediet ska avvecklas på ett sätt som gör informationen på mediet oläsbar och omöjlig att återskapa. En elektronisk lagring av personuppgifter kräver mer djupgående metoder än att informationen i traditionell mening raderas eller att lagringsutrymmet omformateras. Med sådana metoder är informationen fortfarande möjlig att återskapa och läsa med hjälp av rätt teknik.

Enligt SS-ISO/IEC 27002:2014 bör enheter som innehåller känslig information fysiskt förstöras, alternativt att informationen som finns lagrad på enheten förstörs, utplånas eller skrivs över med hjälp av en teknik som omöjliggör rekonstruktion. Tekniker som med full säkerhet omöjliggör rekonstruktion av elektroniskt lagrad information är i det yttersta enbart fysisk förstörelse eller avmagnetisering av mediet.

Vårdgivaren måste även hantera avveckling av pappersmedium, exempelvis pappersjournaler, på ett sätt som omöjliggör läsning eller återskapande. Ett sätt kan vara att alla papper som innehåller personuppgifter avvecklas genom strimling eller bränning.

IT-tjänster som utförs av en extern leverantör

En vårdgivare kan anlita en extern leverantör för att utföra IT-tjänster. I de fall en extern leverantör äger och förvaltar lagringsmedia åt vårdgivaren behöver vårdgivaren säkerställa att leverantören använder metoder som gör personuppgifterna oläsbara och omöjliga att återskapa om leverantören avser att avveckla lagringsmedia. Att vårdgivaren anlitar en extern leverantör fråntar inte denne skyldigheten att uppfylla de krav som anges i HSLF-FS 2016:40.

Åtkomst till uppgifter om patienter

I 4 kap. HSLF-FS 2016:40 finns bestämmelser om vårdgivarens ansvar för styrning av behörigheter och åtkomst till uppgifter om patienter, både inom en vårdgivares verksamhet och vid sammanhållen journalföring. Avsnittet inleds dock med en allmän redogörelse för bestämmelserna om inre sekretess i PDL, för att sedan gå in på bestämmelserna i 4 kap. HSLF-FS 2016:40.

Allmänt om inre sekretess

Med inre sekretess menas vanligen att personalen inom en verksamhet inte får – muntligen eller på något annat sätt – lämna ut uppgifter som omfattas av sekretess till sina arbetskamrater. I förarbetena till PDL ges dock inre sekretess en vidare innebörd som inrymmer flera frågeställningar om hur känsliga uppgifter om enskildas hälsa och andra personliga förhållanden bör hanteras inom en verksamhet för att minska risken för obefogade intrång i den personliga integriteten (prop. 2007/08:126 s. 141).

Bestämmelserna i 2 a § HSL, 3-3 a §§ tandvårdslagen (1985:125) och 5 kap. 1 § patientlagen (2014:821) är av grundläggande betydelse för behandling av personuppgifter. Enligt dessa bestämmelser ska hälso- och sjukvården och tandvården bland annat bygga på respekt för patientens självbestämmande och integritet, och så långt som möjligt utformas och genomföras i samråd med patienten. Bestämmelserna har även betydelse för hanteringen av information om patienten. Justitieombudsmannen (JO) har uttalat att det följer av den angivna bestämmelsen i HSL att en patients uttryckliga önskemål om att journaler inte lämnas till andra kliniker på samma sjukhus ska respekteras (JO 1986/87 s. 199 och prop. 2007/08:126 s. 141).

Personligt ansvar för den inre sekretessen

Bestämmelsen i 4 kap. 1 § PDL om inre sekretessen innebär att den som arbetar hos en vårdgivare bara får ta del av dokumenterade uppgifter om en patient om han eller hon deltar i vården av patienten, eller av något annat skäl behöver uppgifterna för sitt arbete inom hälso- och sjukvården.

Enligt PDL gäller den inre sekretessen för alla dokumenterade personuppgifter om patienter eller andra enskilda registrerade, det vill säga även vårddokumentation, kvalitetsregisteruppgifter med mera som behandlas enligt PDL. Bestämmelsen gäller både manuellt och elektroniskt behandlade uppgifter och även uppgifter om avlidna personer (prop. 2007/08:126 s. 143). Inre sekretess gäller inte bara hälso- och sjukvårdspersonal vid en viss enhet och dess arbete på enheten utan omfattar all personal, oavsett var den tjänstgör och för vilka syften uppgifterna behövs (prop. 2007/08:126 s. 238). Bestämmelsen i 4 kap. 1 § PDL lägger ett ansvar på den som arbetar hos en vårdgivare att inte ta del av mer uppgifter än vad som är nödvändigt för att utföra sitt arbete inom hälso- och sjukvården. Övriga bestämmelser i 4 kap. PDL lägger ett ansvar på vårdgivaren att ha kontroll över och begränsa åtkomsten till uppgifter om patienter.

Studenters möjligheter att ta del av uppgifter

Enligt 1 kap. 1 § PDL ska lagen tillämpas vid vårdgivares behandling av personuppgifter inom hälso- och sjukvården. Utbildningsverksamhet är i allt väsentligt en egen verksamhetsgren också när den bedrivs inom en och samma myndighet som bedriver hälso- och sjukvård. Utbildningsverksamheten som sådan omfattas därför inte av PDL:s tillämpningsområde (prop. 2007/08:126 s. 51). I den utsträckning studenter deltar i den faktiska patientvården såsom praktikanter, ska deras arbete dock omfattas av PDL:s tillämpningsområde. Det innebär bland annat att vårdgivaren i sådana fall ska kunna låta studenterna få ta del av och även kunna föra anteckningar i elektroniska patientjournaler i nödvändig omfattning. Normalt torde detta förutsätta såväl patientens samtycke som att praktikantens åtgärder sker under en handledares uppsikt och ledning (prop. 2007/08:126 s. 51). Studenten behöver i så fall ha en egen personlig inloggning för att kunna ta del av de uppgifter som behövs för att utföra arbetsuppgifterna (6 kap. 1 § HSLF-FS 2016:40), och han eller hon måste kunna dokumentera arbetet. Studenter som deltar i den faktiska vården får därmed också ett ansvar för att bevaka den inre sekretessen.

Vårdgivarens ansvar för inre sekretess

Bestämmelsen om inre sekretess i 4 kap. 1 § PDL uttrycker ett personligt ansvar för den som arbetar hos en vårdgivare. Den bestämmelsen kompletteras av övriga bestämmelserna i kapitlet som beskriver vårdgivarens ansvar för att den inre sekretessen upprätthålls i verksamheten. Av 4 kap. 2 § PDL följer att vårdgivaren ska bestämma villkor för tilldelning av behörighet för åtkomst till sådana uppgifter om patienter som förs helt eller delvis automatiserat på ett sådant sätt att personalen inte har mer behörighet än vad de behöver för att kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården. Dessutom har vårdgivaren enligt 4 kap. 3 § PDL ansvar att se till att åtkomst till sådana uppgifter om patienter som förs helt eller delvis automatiserat dokumenteras (loggas) och kan kontrolleras. I 4 kap. HSLF-FS 2016:40 finns bestämmelser om hur vårdgivaren bland annat ska styra, tilldela och kontrollera åtkomsten till uppgifter om patienter.

Dataintrång

Ett olovligt intrång och olovligt efterforskande i elektroniska informationssystem, till exempel ett journalsystem, kan vara straffbart enligt straffbestämmelsen om dataintrång i 4 kap. 9 c § brottsbalken. Den som olovligen bereder sig tillgång till upptagning för automatisk databehandling eller olovligen ändrar, utplånar, blockerar eller i register för in en sådan uppgift kan enligt 4 kap. 9 c § brottsbalken dömas för dataintrång till böter eller fängelse i högst två år. Bestämmelsen är tillämplig då någon använder sig av sin behörighet till åtkomst till ett elektroniskt journalsystem för att läsa uppgifter om en patient utan att detta behövs från arbetssynpunkt, till exempel på grund av nyfikenhet (prop. 2007/08:126 s. 142-143). Läsning i utbildningssyfte för att eftersöka förebilder på lämpliga formuleringar har i rättspraxis bedömts kunna utgöra dataintrång (RH 2002:36, det så kallade Blommanfallet).

Hovrätten över Skåne och Blekinge har bland annat prövat frågan om inre sekretess då en anhörig uppmanar någon som arbetar inom hälso- och

sjukvården att gå in i dennes patientjournal (dom den 11 mars 2014, mål nr. B 1532-13). Malmö tingsrätt, vars dom hovrätten fastställde utan ändringar, kom fram till att även om den tilltalade hade fått en uppmaning från en anhörig att gå in i dennes journal hade en sådan uppmaning inte gjort inloggningen lovlig, eftersom den tilltalade inte deltog i vården av den anhörige och därmed inte behövt uppgifterna. Se även dom från Hovrätten för Västra Sverige där bland annat frågan om inre sekretess och samtycke från en anhörig att ta del av dennes patientjournal berördes (dom den 30 juni 2015, mål nr. B 3027-14).

Styrning av behörigheter

4 kap. 1 § HSLF-FS 2016:40

Bestämmelser om vårdgivarens ansvar för tilldelning och begränsning av behörigheter för åtkomst till uppgifter om patienter finns i 4 kap. 2 § och 6 kap. 7 § patientdatalagen (2008:355).

Vårdgivarens ansvar för tilldelning och begränsning av behörigheter

Vårdgivaren ska bestämma villkoren för tilldelning av behörighet för åtkomst till uppgifter om patienter som förs helt eller delvis automatiserat. Sådan behörighet ska begränsas till vad som behövs för att den enskilde ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården (4 kap. 2 § PDL). Av 6 kap. 7 § PDL framgår att en vårdgivare har samma skyldigheter när det gäller direktåtkomst till andra vårdgivares uppgifter om patienter genom sammanhållen journalföring. Det ingår alltså i vårdgivarens ansvar att närmare bestämma villkoren för personalens åtkomst till uppgifterna. Detta gäller oavsett om landstinget eller kommunen bedriver hälso- och sjukvård genom en eller flera myndigheter (prop. 2007/08:126 s. 239). Det ingår i varje vårdgivares ansvar att se till att alla anställda får full information om behörighetsreglerna (prop. 2007/08:126 s. 240).

4 kap. 2 § HSLF-FS 2016:40

Vårdgivaren ska ansvara för att varje användare tilldelas en individuell behörighet för åtkomst till personuppgifter. Vårdgivarens beslut om tilldelning av behörighet ska föregås av en behovs- och riskanalys.

Tilldelning av individuell behörighet

Vårdgivaren ansvarar för att alla användare har en individuell behörighet. Det innebär bland annat att endast personliga inloggningar är tillåtna och att

inga så kallade gruppkonton får förekomma. Vårdgivarens ansvar vid tilldelning av behörighet för elektronisk åtkomst innefattar en skyldighet att göra aktiva och individuella behörighetstilldelningar utifrån analyser av vilken närmare information olika personalkategorier och olika slags verksamheter behöver (behovsanalys). Även riskanalyser måste göras där det tas hänsyn till olika slags risker som kan vara förknippade med en alltför vid tillgänglighet avseende vissa slags uppgifter (prop. 2007/08:126 s. 148-149). En användares behörighet behöver vara anpassad till hans eller hennes arbetsuppgifter. Vårdgivaren ansvarar också för att användarna tilldelas rätt behörighet, det vill säga tillräckligt för att de ska kunna utföra sina arbetsuppgifter på ett säkert sätt men samtidigt inte mer omfattande än vad som är nödvändigt.

Av förarbetena till PDL framgår att det generellt sett kan sägas att ju mer omfattande ett informationssystem är, desto större mängd olika behörighetsnivåer måste det finnas. Avgörande för beslut om behörighet för till exempel olika kategorier av hälso- och sjukvårdspersonal till elektronisk åtkomst till uppgifter i patientjournaler bör vara att behörigheten ska begränsas till vad användaren behöver för att kunna ge en god och säker vård. En mer vidsträckt eller grovmaskig behörighetstilldelning bör, även om den skulle ha poänger utifrån effektivitetssynpunkt, anses som en obefogad spridning av journaluppgifter inom en verksamhet och bör som sådan inte accepteras (prop. 2007/08:126 s. 149). När det gäller personal som arbetar med verksamhetsuppföljning, statistikframställning, central ekonomiadministration och liknande verksamhet som inte är individorienterad torde det för flertalet användare räcka med tillgång till uppgifter som endast indirekt kan härledas till enskilda patienter. Elektronisk åtkomst till kodnycklar, personnummer och andra uppgifter som direkt pekar ut enskilda patienter bör på detta område kunna vara starkt begränsad till enstaka personer (prop. 2007/08:126 s. 149).

Behovs- och riskanalys

Vårdgivarens ansvar vid tilldelning av behörighet för elektronisk åtkomst innefattar en skyldighet att göra aktiva och individuella behörighetstilldelningar utifrån analyser av vilken närmare information olika personalkategorier och olika slags verksamheter behöver. Även riskanalyser måste göras där det bland annat kan tas hänsyn till olika slags risker som kan vara förknippade med en alltför vid tillgänglighet avseende vissa slags uppgifter (prop. 2007/08:126 s. 148-149). I förarbetena till PDL anges att skyddade personuppgifter som är sekretessmarkerade, uppgifter om allmänt kända personer, uppgifter från vissa mottagningar eller medicinska specialiteter är exempel på kategorier som kan kräva särskilda riskbedömningar (prop. 2007/08:126 s. 149).

För att varje användare ska få rätt behörighet måste vårdgivaren först ha genomfört behovs- och riskanalyser. Vid behovs- och riskanalyser kan det tas hänsyn till vilka behov av åtkomst en användare har samt vilka risker det kan innebära om personalen har för lite eller för mycket tillgång till olika personuppgifter. Generellt sett kan sägas att ju mer omfattande ett informationssystem är, desto fler olika behörighetsnivåer behöver finnas (prop. 2007/08:126

s. 149). En och samma användare kan också behöva olika behörighetsnivåer vid olika tillfällen, exempelvis om en person ibland har jouransvar för en hel verksamhet men annars ansvarar för en mindre vårdenhet. Ett annat exempel är en student som ibland gör praktikperioder hos en vårdgivare, men vid andra tillfällen arbetar som anställd hos samma vårdgivare. I så fall kan lämpligen vårdgivarens behovs- och riskbedömning ligga till grund för vilka behörigheter som personen ska tilldelas (prop. 2007/08:126 s. 149).

4 kap. 3 § HSLF-FS 2016:40

Vårdgivaren ska ta fram rutiner för ändring, borttagning och regelbunden uppföljning av behörigheterna för att säkerställa att dessa är riktiga och aktuella.

Ändring, borttagning och uppföljning av behörigheterna

Vårdgivaren ansvarar för att det finns rutiner för att ändra, ta bort och regelbundet följa upp behörigheterna. Genom att följa dessa rutiner kan behörigheterna fortsätta att vara riktiga över tiden oavsett om personal börjar, slutar eller får ändrade arbetsuppgifter i verksamheten. Om en användare får nya arbetsuppgifter kan behörigheten behöva följas upp och ändras så att den stämmer överens med de nya arbetsuppgifterna.

Under avsnittet om vårdgivarens ansvar att tilldela och begränsa behörigheter (s. 33) nämns att behörigheterna ska begränsas till vad som behövs för att den enskilde ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården (4 kap. 2 § PDL). Däri ligger bland annat att behörigheter ska följas upp och ändras eller inskränkas efter hand som förändringar i den enskilde användarens arbetsuppgifter ger anledning till det (prop. 2007/08:126 s. 148).

Vårdgivaren skulle exempelvis kunna överväga att samordna administrationen av användarnas behörigheter med personalenhetens (eller motsvarande) personaladministrativa arbete. Behörigheten till informationssystemen kan då jämställas med personaladministrativa frågor som tillgång till telefon, parkering och nycklar. Dessa frågor kan komma vid samma tidpunkt och hanteras i samma rutin, till exempel med hjälp av en checklista med saker som ska göras när en anställning påbörjas, ändras och avslutas. Vårdgivaren kan också fastställa vem eller vilka som har ansvar för att hantera denna process.

Vårdgivaren ansvarar även för att det finns rutiner som inkluderar en regelbunden uppföljning av behörigheterna. Genom att regelbundet följa upp behörigheterna kan felaktiga behörigheter, som av någon anledning inte har hanterats i rutinen, fångas upp.

Rutinen kan innehålla krav på att den ansvarige dokumenterar godkännanden och tilldelningar av behörigheter, exempelvis genom att arkivera beslut om att ändra och ta bort behörigheter. Besluten kan då kontrolleras i efter-

hand om det skulle behövas, men de arkiverade besluten behöver också förvaras så att de är skyddade från olovliga ändringar.

Verksamheter med många användare och ändringar av behörigheter kan behöva komplettera rutinen med något verktyg som underlättar arbetet. Det finns exempelvis kommersiella program för att styra behörigheter och granska ändringar av behörigheterna genom efterkontroller.

Åtkomst till uppgifter inom en vårdgivares verksamhet

4 kap. 4 § HSLF-FS 2016:40

Vårdgivaren ska ansvara för att information om på vilka andra vårdenheter eller i vilka andra vårdprocesser det finns uppgifter om en viss patient inte kan göras tillgänglig utan att den behörige användaren gör ett ställningstagande till om han eller hon har rätt att ta del av denna information (aktivt val). Uppgifterna får sedan inte göras tillgängliga utan att den behörige användaren gör ytterligare ett aktivt val.

Inom en och samma vårdgivares verksamhet ska en användare kunna se i informationssystemet om det finns uppgifter om en patient hos en annan vårdenhet eller i en annan vårdprocess, men inte vilken vårdenhet eller vårdprocess. Användaren ska också kunna se om uppgifterna är spärrade eller inte (4 kap. 4 § PDL). För att kunna se hos vilken vårdenhet eller vårdprocess som uppgifterna finns så måste användaren först göra ett aktivt val. Det aktiva valet fungerar som en tröskel där användaren aktivt väljer åtkomst till uppgifterna genom att gå vidare i informationssystemet. Om vårdenheten eller vårdprocessen har ospärrade uppgifter om patienten måste användaren då göra ytterligare ett aktivt val för att få tillgång till dessa uppgifter. Det krävs alltså två aktiva val för att nå ospärrade uppgifter om en patient.

Aktivt val

En generös behörighetstilldelning kan innebära en obefogad spridning av personuppgifter. Det räcker därför inte att i efterhand kontrollera åtkomstlistor för att konstatera eventuella intrång. I stora, brett tillgängliga system ska normalt olika behörighetsnivåer för personalen finnas (prop. 2007/08:126 s. 240). Enligt förarbetena till PDL bör uppgifter lagras i olika ”skikt” så att mer känsliga uppgifter kräver aktiva val eller inte är lika lätta att nå som mindre känsliga uppgifter (prop. 2007/08:126 s. 149 och 240). Med aktivt val menas att en behörig användare tar ställning till om han eller hon har rätt att ta del av ytterligare uppgifter. Ett aktivt val för åtkomst bekräftar att användaren har tagit ställning till om situationen uppfyller vissa angivna krav i 4 kap. PDL. Om användaren väljer att gå vidare i informationssystemet för att hämta mer uppgifter ska denna åtgärd loggas (4 kap. 3 § PDL och 4 kap. 9 §

HSLF-FS 2016:40). Om kraven är uppfyllda får användaren ta del av uppgifter om en patient på det sätt som beskrivs i 4 kap. PDL.

4 kap. 5 § HSLF-FS 2016:40

Om uppgifter om en patient har spärrats av en annan vårdenhet eller i en annan vårdprocess hos vårdgivaren, får dessa endast göras tillgängliga efter det att den behöriga användaren gjort ett aktivt val. Det aktiva valet ska göras efter en prövning av om de krav som anges i 4 kap. 5 § patientdatalagen (2008:355) för att få häva en spärr är uppfyllda.

Spärrade uppgifter vid annan vårdenhet eller i annan vårdprocess

En patient kan motsätta sig att uppgifter om honom eller henne är tillgängliga genom elektronisk åtkomst för den som arbetar vid en annan vårdenhet eller inom en annan vårdprocess hos samma vårdgivare. I sådana fall ska uppgiften genast spärras. Uppgift om att det finns spärrade uppgifter får vara tillgänglig för andra vårdenheter eller vårdprocesser (4 kap. 4 § PDL). Av 5 kap. 5 § 9 HSLF-FS 2016:40 framgår att patientjournalen ska innehålla uppgift om samtycken och återkallade samtycken.

En spärr får hävas av en behörig befattningshavare hos vårdgivaren om patienten samtycker till det (4 kap. 5 § PDL). Det ska vara ett sådant samtycke som avses i personuppgiftslagen, det vill säga det ska vara frivilligt, särskilt och otvetydigt (prop. 2007/08:126 s. 243).

Spärren kan också hävas av en annan vårdenhet eller vårdprocess, till exempel akutmottagningen, om patientens samtycke inte kan inhämtas och informationen kan antas ha betydelse för den vård eller behandling som patienten oundgängligen behöver (4 kap. 5 § PDL). Det kan exempelvis bero på att patienten är medvetslös eller alltför medtagen för att kunna ta ställning till frågan (prop. 2007/08:126 s. 115 och 243). Vidare kan saken brådska så att det inte finns någon tid att inhämta samtycke. Det ska i princip vara fråga om en allvarlig akutsituation, då patienten på grund av sitt hälsotillstånd eller andra skäl inte kan ta ställning till samtyckesfrågan och då uppgifterna bedöms vara av vital betydelse för de vård- eller behandlingsinsatser som omgående måste sättas in. Det ska alltså av hänsyn till patientsäkerheten inte vara möjligt att avvakta en tid för att patienten ska kunna lämna sitt samtycke (prop. 2007/08:126 s. 243). En patient som i denna situation vidhåller en spärr och alltså motsätter sig att någon utanför vårdenheten eller vårdprocessen tar del av uppgifterna ska respekteras, hur ogrundad eller irrationell patientens inställning än kan tyckas vara (prop. 2007/08:126 s. 243). Då möjligheten att häva en spärr vid en sådan akut nödsituation kan upplevas som känslig för patienten är det viktigt att systemet är utformat så att det både tillgodoser patientens bästa i vårdsituationen men också så långt som möjligt skyddar patientens integritet genom att andra spärrade uppgifter som inte kan antas ha betydelse för den vård som patienten oundgängligen

behöver inte per automatik görs tillgängliga vid en akut nödsituation (prop. 2007/08:126 s. 152).

Om patientens samtycke inte kan inhämtas och informationen kan antas ha betydelse för den vård som patienten oundgängligen behöver, ska uppgift om vårdenheter eller vårdprocesser som spärrat uppgifterna göras tillgängliga (4 kap. 5 § PDL). Vårdgivaren ska ansvara för att information om på vilka andra vårdenheter eller i vilka andra vårdprocesser det finns spärrade uppgifter om en viss patient inte kan göras tillgänglig utan att den behörige användaren gör ett ställningstagande till om han eller hon har rätt att ta del av denna information, det vill säga ett aktivt val (4 kap. 4 § HSLF-FS 2016:40).

Därefter får bara sådana uppgifter som kan antas ha betydelse för vården av patienten göras tillgängliga (4 kap. 5 § andra stycket PDL). Genom att användaren vet vid vilken eller vid vilka vårdenheter eller vårdprocesser som det finns spärrade uppgifter får han eller hon ytterligare underlag för att bedöma om de spärrade uppgifterna kan ha betydelse för den vård som patienten behöver (prop. 2007/08:126 s. 243). De spärrade uppgifterna (som kan antas ha betydelse för vården av patienten) får endast göras tillgängliga efter det att den behöriga användaren gjort ett aktivt val (4 kap. 5 § HSLF-FS 2016:40).

Kortfattat ska alltså systemet vara uppbyggt på så sätt att behörig användare i steg 1 får tillgång till information om vid vilken eller vilka vårdenheter eller vårdprocesser som det finns spärrade uppgifter. Behörig användare kan i detta skede endast se uppgiften vid vilken eller vid vilka vårdenheter eller vårdprocesser som spärrar har gjorts, inte vilken specifik typ av behandling som spärrats. Steg två innebär att behörig användare, genom att denne kan se vid vilken eller vid vilka vårdenheter eller vårdprocesser uppgifter har spärrats, kan bedöma om de spärrade uppgifterna kan antas ha betydelse för vården av patienten. Endast uppgifter som kan antas ha en sådan betydelse får hävas (prop. 2007/08:126 s. 152).

Exempel - häva spärrade uppgifter inom en vårdgivares verksamhet

Med utgångspunkt i vad som beskrivs ovan följer ett exempel på hur en behörig användare kan få åtkomst till spärrade uppgifter inom en vårdgivares verksamhet.

1. En behörig användare kan se i systemet att det finns spärrade uppgifter om en patient men inte vilken eller vid vilka vårdenheter eller vårdprocesser som uppgifterna spärrats.
2. Patienten samtycker till att spärren hävs.
   Patientens samtycke kan inte inhämtas och informationen (om vilken vårdprocess/vårdenhet som har spärrat uppgifterna) kan antas ha betydelse för vården som patienten oundgängligen behöver.
3. Användaren gör ett aktivt val i systemet för att ta del av informationen om vilken eller vilka vårdenheter eller vårdprocesser som spärrat uppgifterna.
4. Användaren gör ett aktivt val (nr. 2) innan han eller hon tar del av uppgifterna som kan antas ha betydelse för vården av patienten.

Om vårdenhet och vårdprocess

Begreppen vårdenhet och vårdprocess definieras inte i PDL. Vårdprocess definieras i 2 kap. 1 § HSLF-FS 2016:40 som process avseende hälso- och sjukvård som hanterar ett eller flera relaterade hälsoproblem eller hälsotillstånd i syfte att främja ett avsett resultat. Vårdenhet definieras i Socialstyrelsens termbank som organisatorisk enhet som tillhandahåller hälso- och sjukvård.

Av förarbetena till PDL framgår att avgränsningen av en vårdprocess är funktionell och inte organisatorisk såsom beträffande vårdenhet. En vårdprocess kan med andra ord inbegripa avgränsbara aktiviteter eller åtgärder hos olika vårdenheter som har ett funktionellt samband. Ofta utgör de privata vårdgivarna en enda enhet (prop. 2007/08:126 s. 241). Inom den offentliga hälso- och sjukvården är det naturligt att se varje vårdcentral som en enhet. Ett sjukhus är däremot normalt inte en enda enhet. Hur gränserna närmare ska dras inom en vårdgivares verksamhet bestäms ytterst av varje vårdgivare (prop. 2007/08:126 s. 241). Enligt förarbetena behöver gränserna dras på ett praktiskt och rimligt sätt för vårdgivaren så att verksamheten inte tyngs med onödig administration. Även inom en vårdenhet eller vårdprocess gäller att en befattningshavare endast ska anses behörig att ta del av uppgifter om en patient om denne deltar i vården av patienten eller av annat skäl behöver uppgifterna för sitt arbete (prop. 2007/08:126 s. 241-242).

Vårdnadshavare får inte spärra barnets uppgifter

Vårdnadshavare till ett barn har inte rätt att spärra barnets uppgifter (4 kap. 4 § andra stycket PDL). Med barn avses den som är under 18 år. Avsikten är att öka hälso- och sjukvårspersonalens möjligheter att upptäcka barn som far illa och att bedöma om anmälan ska göras till socialnämnden för att barnet ska få erforderligt skydd. Detta skäl har ansetts väga över den integritetskränkning som kan uppstå till följd av att vårdnadshavare inte kan spärra sitt barns uppgifter. I takt med barnets stigande ålder och utveckling får barnet själv spärra uppgifterna. Barn och tonåringar bör hanteras på motsvarande sätt som i den övriga verksamheten inom hälso- och sjukvården. I takt med den underåriges stigande ålder och utveckling ska allt större hänsyn tas till barnets önskemål och vilja, jämför 6 kap. 11 § föräldrabalken (prop. 2007/08:126 s. 242).

Allmänt om sammanhållen journalföring

Sammanhållen journalföring innebär att vårdgivare under vissa förutsättningar kan få direktåtkomst till varandras elektroniska journalhandlingar och andra personuppgifter som behandlas för ändamål som rör vårddokumentation. Varje elektronisk journalhandling är knuten till en viss vårdgivare som ansvarar för de handlingar som upprättas eller inkommer i sin verksamhet. Den sammanhållna journalföringen innebär alltså inte att hälso- och sjukvårdspersonal som arbetar hos en vårdgivare ska föra anteckningar i en annan vårdgivares journalhandlingar, utan det är enbart en möjlighet att ta del av andra vårdgivares uppgifter om en patient. Genom att samarbeta via sammanhållen journalföring kan både offentliga och privata vårdgivare på

frivillig väg bygga upp system för elektronisk uppgiftslämning i gemensamma databaser eller andra gränsöverskridande informationssystem för vårddokumentationen (prop. 2007/08:126 s. 105).

Begreppet direktåtkomst används i PDL för att beskriva elektronisk uppgiftslämning där den som är ansvarig för informationen inte har kontroll över vilka uppgifter som mottagaren vid ett visst tillfälle tar del av, så kallad automatiserad tillgång, och där mottagaren inte kan påverka innehållet i det informationssystem eller det register som informationen lämnas ut från. Mottagaren kan alltså ta del av innehållet i till exempel en elektronisk handling men inte ändra i den eller lägga till ny information (prop. 2007/08:126 s. 105-106). Sammanhållen journalföring omfattar inte bara journalhandlingar utan även annan vårddokumentation. I ett system för sammanhållen journalföring kan vårdgivarna alltså upprätta gemensamma patientöversikter med till exempel sammanställningar av viss basinformation, sökregister med mera. Hur systemen ska byggas upp får vårdgivarna själva bestämma. Reglerna för sammanhållen journalföring innebär dock vissa krav på systemen och de måste tekniskt och organisatoriskt utformas och anpassas så att dessa krav kan uppfyllas (prop. 2007/08:126 s. 106 och 248).

Inom den offentliga hälso- och sjukvården gäller sekretess enligt 25 kap. 1 § offentlighets- och sekretesslagen (2009:400), OSL, för uppgifter som kan göras tillgängliga genom sammanhållen journalföring. Enligt den sekretessbrytande bestämmelsen i 25 kap. 11 § 3 OSL hindrar sekretessen enligt 1 § inte att uppgift lämnas till en myndighet som bedriver verksamhet som avses i 1 § eller till en enskild vårdgivare enligt vad som föreskrivs om sammanhållen journalföring i PDL. Det innebär alltså att uppgifter kan lämnas mellan vårdgivare enligt bestämmelserna om sammanhållen journalföring i PDL. För den enskilda (privata) hälso- och sjukvården gäller tystnadspliktsbestämmelser i 6 kap. 12-16 §§ patientsäkerhetslagen (2010:659), PSL. Tystnadsplikten innebär att hälso- och sjukvårdspersonal inte obehörigen får röja vad han eller hon i sin verksamhet har fått veta om en enskilds hälsotillstånd eller andra personliga förhållanden. Vid tolkningen av obehörigt röjande brukar ledning sökas i OSL:s bestämmelser (prop. 1980/81:28 s. 22-23 och prop. 2007/08:126 s. 248). Enligt förarbetena till PDL bör den bestämmelsen därför kunna tolkas på motsvarande sätt som 25 kap. 11 § 3 OSL när det gäller tillgängliggörande av uppgifter i sammanhållen journalföring (prop. 2007/08:126 s. 248). Till detta kommer regleringen i PDL som anger förutsättningarna för den sammanhållna journalföringen. Det innebär att en privat vårdgivare kan göra uppgifter tillgängliga, om förutsättningarna för sammanhållen journalföring är uppfyllda (prop. 2007/08:126 s. 248).

Sammanhållen journalföring innebär alltså utbyte av uppgifter om en patient genom direktåtkomst. Om informationsutbytet går till på något annat sätt gäller bland annat reglerna om tystnadsplikt och sekretess som vanligt vid andra typer av utlämnande av uppgifter om patienter.

Alla uppgifter om en patient behöver inte ingå i den sammanhållna journalföringen, utan kan begränsas till delar av det som dokumenteras i en patientjournal eller andra uppgifter om en patient (prop. 2007/08:126 s. 248). Det innebär att vårdgivarna kan bygga upp ett system där exempelvis bara

vissa medicinska basfakta är tillgängliga. Nationell patientöversikt (NPÖ) är ett exempel på ett sådant system för att utbyta vissa uppgifter om en patient.

Information om sammanhållen journalföring till patienten

Innan uppgifter om en patient görs tillgängliga för andra vårdgivare genom sammanhållen journalföring ska patienten informeras om vad den sammanhållna journalföringen innebär. Patienten ska också informeras om att han eller hon kan motsätta sig att uppgifterna görs tillgängliga på det sättet (6 kap. 2 § tredje stycket PDL). Vid varje vårdepisod ska patienten få en möjlighet att motsätta sig att uppgifterna görs tillgängliga för utomstående vårdgivare. Patienten kan dock inte motsätta sig att uppgifter förs in i journalen eller det elektroniska system som vårdgivaren använder, utan det gäller bara att uppgiften spärras för andra vårdgivare. En sådan spärr får endast hävas av patienten själv eller vid en akut nödsituation (prop. 2007/08:126 s. 112).

Det krävs inget aktivt samtycke från patienten för att uppgifterna ska bli tillgängliga i systemet för sammanhållen journalföring. Informationen måste lämnas innan uppgifter om en patient kan bli tillgängliga för andra. Det finns inga generella regler för hur informationen ska lämnas. Enligt förarbetena förutsätts det att hälso- och sjukvårdens aktörer hittar lämpliga former som är väl avvägda och anpassade till olika verksamhetsområden och till olika slags samarbeten mellan vårdgivare genom sammanhållen journalföring samt till den enskilde patientens förmåga att ta till sig informationen (prop. 2007/08:126 s. 113).

När det gäller till exempel patienter som inte talar svenska bör den personuppgiftsansvarige se till att någon översätter informationen eller att det finns skriftliga informationsblanketter på flera språk (prop. 2007/08:126 s. 250).

Datainspektionen konstaterade i ett tillsynsbeslut den 29 juni 2010 (dnr 1390-2009), som avsåg NPÖ, att vårdgivaren får avgöra utifrån omständigheterna i det enskilda fallet hur informationen ska lämnas till patienten. Datainspektionen uppgav att det ankommer på vårdgivaren att visa att samtliga patienter som omfattas av den sammanhållna journalföringen har fått information innan tillgängliggörandet. Enligt Datainspektionen innebär informationskravet bland annat att en vårdgivare behöver lämna ny, kompletterande, information till patienterna för det fall den sammanhållna journalföringen förändrats sedan den ursprungliga informationen lämnades. Som exempel nämndes att nya vårdgivare anslutit sig till den sammanhållna journalföringen och därmed fått möjlighet att ta del av uppgifter om patienter.

Vårdnadshavare får inte spärra barnets uppgifter

Vårdnadshavare till ett barn kan inte spärra uppgifter om barnet (6 kap. 2 § fjärde stycket PDL). Med barn avses den som är under 18 år. Skälet till detta är att öka vårdpersonalens möjligheter att upptäcka barn som far illa och att bedöma om anmälan ska göras till socialnämnden för att barnet ska få erforderligt skydd. Dessa skäl har ansetts överväga den integritetskränkning som kan uppstå till följd av att vårdnadshavare inte kan spärra sitt barns

uppgifter (prop. 2007/08:126 s. 250-251). I takt med barnets stigande ålder och utveckling får barnet själv spärra uppgifterna. Barn och tonåringar bör hanteras på motsvarande sätt som i den övriga verksamheten inom hälso- och sjukvården. I takt med den underåriges stigande ålder och utveckling ska allt större hänsyn tas till barnets önskemål och vilja, jämför 6 kap. 11 § föräldrabalken (prop. 2007/08:126 s. 251).

Ospärrade uppgifter vid sammanhållen journalföring

4 kap. 6 § HSLF-FS 2016:40

Vårdgivaren ska ansvara för att en behörig användares åtkomst till ospärrade uppgifter om en patient hos en annan vårdgivare föregås av att användaren kontrollerar att förutsättningarna för behandling av personuppgifter enligt 6 kap. 3 § eller 3 a § patientdatalagen (2008:355) är uppfyllda och därefter gör ett aktivt val för att ta del av uppgifterna.

Åtkomst till ospärrade uppgifter vid sammanhållen journalföring

Om patienten inte har motsatt sig att uppgifter om patienten görs tillgängliga för andra vårdgivare i ett system för sammanhållen journalföring, får alltså dessa uppgifter göras tillgängliga. Det ska då anges i systemet att det finns ospärrade uppgifter om patienten, vilket andra vårdgivare ska kunna se utan att veta vilken vårdgivare uppgiften kommer ifrån (6 kap. 2 § femte stycket PDL). Vårdgivaren ansvarar för att information om på vilka andra vårdenheter eller i vilka andra vårdprocesser (hos en annan vårdgivare) det finns uppgifter om en patient inte kan göras tillgänglig utan att den behörige användaren gör ett aktivt val (4 kap. 4 § HSLF-FS 2016:40). Vidare ansvarar vårdgivaren för att en behörig användares åtkomst till ospärrade uppgifter om en patient (hos en annan vårdgivare) föregås av att användaren kontrollerar att förutsättningarna i 6 kap. 3 § eller 3 a § PDL är uppfyllda. Användaren måste sedan göra ytterligare ett aktivt val för att ta del av uppgifterna om patienten (4 kap. 6 § HSLF-FS 2016:40).

Förutsättningar i 6 kap. 3 § patientdatalagen

För att andra vårdgivare ska få ta del av ospärrade uppgifter krävs att uppgifterna rör en patient som det finns en aktuell patientrelation med och att uppgifterna kan antas ha betydelse för att förebygga, utreda eller behandla sjukdomar eller skador hos patienten. Patienten måste också samtycka till det (6 kap. 3 § första stycket PDL). Vårdgivaren får även behandla sådana uppgifter om uppgifterna rör en patient som det finns eller har funnits en patientrelation med, om uppgifterna kan antas ha betydelse för att utfärda

intyg om vården och patienten samtycker till det (6 kap. 3 § andra stycket PDL). Bestämmelsen är inte en regel om så kallad inre sekretess, utan anger under vilka förutsättningar vårdgivaren som sådan får använda direktåtkomst till annan vårdgivares information som vårdgivaren medgetts genom den sammanhållna journalföringen (prop. 2007/08:126 s. 117 och 252). Det gör att den faktiska tillgången till andra vårdgivares information begränsas till de patienter som vårdas eller behandlas inom den egna verksamheten (prop. 2007/08:126 s. 117).

I förarbetena till PDL anges att huruvida en patientrelation över huvud taget föreligger med en enskild person är normalt enkelt att konstatera (prop. 2007/08:126 s. 252). En patientrelation anses vanligen som avslutad då en intagen sjukhuspatient skrivs ut såsom färdigbehandlad och det inte finns några inplanerade återbesök, efterkontroller eller liknande. Detsamma bör gälla om patienten skrivs ut för fortsatt vård eller uppföljning hos öppen primärvård i annan vårdgivares regi. Mer tveksamt kan det vara huruvida en husläkare, och därmed den vårdgivare som husläkaren hör till, ska anses ha en ständig aktuell patientrelation med alla de personer som tecknat sig hos läkaren. Så bör normalt inte bedömas vara fallet, men beträffande sådana patienter som regelbundet och relativt frekvent besöker eller har kontakt med sin husläkare kan en annan bedömning göras (prop. 2007/08:126 s. 252). Av kravet på att det ska finnas en aktuell patientrelation följer att det inte är tillåtet att i en behandlingssituation med en patient söka efter och ta fram vårddokumentation om någon annan patient som vårdas hos en annan vårdgivare, exempelvis en nära släkting med samma sjukdomsdiagnos (prop. 2007/08:126 s. 252).

Det krävs ett aktivt samtycke från patienten för att en annan vårdgivare ska få behandla ospärrade uppgifter om en patient som finns tillgängliga genom sammanhållen journalföring (6 kap. 3 § första stycket PDL). Det ska vara ett sådant samtycke som avses i personuppgiftslagen, det vill säga vara frivilligt, särskilt och otvetydigt. Kravet på att samtycket ska vara frivilligt ger uttryck för att den enskilde verkligen ska ha ett val (prop. 2007/08:126 s. 252). Personuppgiftslagen anger vidare att samtycket ska vara särskilt, vilket betyder att en patient inte kan lämna ett generellt samtycke till personuppgiftsbehandling som inte är preciserad till något eller några ändamål (prop. 2007/08:126 s. 252). Slutligen ska samtycket vara otvetydigt, vilket innebär att det inte får råda någon tvekan om att patienten godtar personuppgiftsbehandlingen. Inget hindrar att ett samtycke lämnas i förväg innan den aktuella patientrelationen har uppstått, till exempel i samband med att uppgifter om honom eller henne görs tillgängliga i ett sammanhållet journalsystem. Patienten kan då samtycka till att en annan vårdgivare senare får ta del av uppgifterna (prop. 2007/08:126 s. 253). Detta är möjligt under förutsättning att samtycket är särskilt och otvetydigt. Exempelvis kan samtycket lämnas i förväg om en patient befinner sig i en vårdprocess som inbegriper flera olika vårdgivare och där patienten skickas mellan dessa i ett remissförfarande (prop. 2007/08:126 s. 253).

Förutsättningar i 6 kap. 3 a § patientdatalagen

I PDL finns en särskild bestämmelse gällande personer som inte endast tillfälligt saknar förmåga att lämna samtycke till behandling av uppgifter i ett system med sammanhållen journalföring (6 kap. 3 a § PDL).

I 6 kap. 3 a § första stycket PDL regleras under vilka förutsättningar en vårdgivare får ta del av uppgift om vilken vårdgivare som gjort uppgifter tillgängliga. I bestämmelsens andra stycke anges under vilka förutsättningar som vårdgivaren även får behandla personuppgifter som gjorts tillgängliga av en annan vårdgivare.

En bedömning ska göras om patienten saknar förmåga att lämna det samtycke som i normalfallet krävs för åtkomst till uppgifter i system för sammanhållen journalföring. Vidare är det fråga om uppgifter som rör en patient för vilken det finns en aktuell patientrelation och att uppgifterna kan antas ha betydelse för att förebygga, utreda eller behandla sjukdomar och skador hos patienten inom hälso- och sjukvården (proposition 2013/14:202 Förbättrad informationshantering avseende vissa patienter inom hälso- och sjukvården s. 43). Bedömning av patientens förmåga till att samtycka har inte någon räckvidd utanför den konkreta situationen då bedömningen görs. Med hänsyn till hur patientens hälsotillstånd utvecklas eller förändras kan patientens förmåga variera över tid och även variera beroende på vilken fråga som patienten behöver ta ställning till (6 kap. 3 § första stycket PDL och prop. 2013/14:202 s. 43).

I 6 kap. 3 a § andra stycket PDL regleras under vilka förutsättningar vårdgivaren även får behandla personuppgifter som gjorts tillgängliga av en annan vårdgivare. Om vårdgivaren med ledning av uppgifterna om vilken vårdgivare som gjort uppgifter tillgängliga bedömer att uppgifterna som avses i 2 eller 2 a §§ (det vill säga som är ospärrade) kan antas ha betydelse för den vård som är nödvändig med hänsyn till patientens hälsotillstånd, får vårdgivaren även behandla uppgifterna (prop. 2013/14:202 s. 43). Det krävs också att patientens inställning till vårdgivarens möjlighet att även få behandla uppgifter - som en annan vårdgivare gjort tillgängliga i systemet med sammanhållen journalföring - så långt som möjligt ska ha klarlagts samt att det inte finns anledning att anta att patienten skulle ha motsatt sig personuppgiftsbehandlingen. Detta tar särskilt sikte på de fall då patienten tidigare haft förmåga att ta ställning till tillgängliggörande av personuppgifter i sammanhållen journalföring (6 kap. 2 § PDL), men vid tiden för direktåtkomst av en annan vårdgivares patientuppgifter saknar förmåga att lämna samtycke (prop. 2013/14:202 s. 43). Hur omfattande åtgärder vårdgivaren behöver vidta för att klarlägga inställningen får avgöras av förhållandena i det enskilda fallet. Med att ”det inte finns anledning att anta” menas att det inte ska föreligga konkreta omständigheter som visar att patienten skulle motsätta sig personuppgiftsbehandlingen (prop. 2013/14:202 s. 43).

Det är den vårdgivare som behöver ta del av uppgifter hos en annan vårdgivare som ska göra bedömningen av om patienten har förmåga att ge sitt samtycke till personuppgiftsbehandlingen eller inte, respektive göra bedömningen om uppgifterna kan antas ha betydelse för vården. Det kan vara den eller de behöriga användarna hos vårdgivaren som ges denna åtkomst respektive får behandla uppgifterna. Vem eller vilka som är behöriga befatt-

ningshavare bestäms av vårdgivaren (prop. 2013/14:202 s. 44 och prop. 2007/08:126 s. 253).

Bestämmelserna i 6 kap. 3 a § PDL ska inte tillämpas i akuta situationer där det är fara för den enskildes liv eller annars föreligger allvarlig fara för den enskildes hälsa. I sådana akuta situationer kan bestämmelsen i 6 kap. 4 § andra stycket PDL tillämpas (prop. 2013/14:202 s. 44).

Aktivt val

Förutom att behörig användare ska kontrollera att förutsättningarna enligt 6 kap. 3 § eller 3 a § PDL är uppfyllda, ansvarar vårdgivaren för att behörig användare därefter gör ett aktivt val för att ta del av uppgifterna (4 kap. 6 § HSLF-FS 2016:40).

Det aktiva valet fungerar som en tröskel i systemet där användaren aktivt måste ta ställning till om han eller hon har rätt att ta del av ytterligare uppgifter om en patient, innan användaren går vidare i systemet och får tillgång till uppgifterna. Enligt förarbetena till PDL bör uppgifter lagras i olika skikt så att mer känsliga uppgifter kräver aktiva val eller inte är lika lätta att nå som mindre känsliga uppgifter (prop. 2007/08:126 s. 149). Med aktivt val menas att en behörig användare tar ställning till om han eller hon har rätt att ta del av ytterligare uppgifter. Om användaren då går vidare i informationssystemet för att hämta mer uppgifter ska denna åtgärd loggas enligt 4 kap. 9 § HSLF-FS 2016:40. Ett aktivt val för åtkomst bekräftar att användaren har tagit ställning till om situationen uppfyller vissa angivna krav i 6 kap. PDL. Om kraven är uppfyllda får användaren ta del av uppgifter i ett journalsystem på det sätt som också beskrivs i 6 kap. PDL.

Exempel - åtkomst till ospärrade uppgifter vid sammanhållen journalföring

Med utgångspunkt i vad som beskrivs i avsnitten ovan, följer ett exempel på hur en behörig användare kan få åtkomst till ospärrade uppgifter vid sammanhållen journalföring.

1. En användare kan se att någon annan vårdgivare har ospärrade uppgifter om en viss patient, men inte vilken vårdgivare.
2. Användaren gör ett aktivt val (nr. 1) för att ta del av uppgiften om vilken eller vilka vårdgivare som har de ospärrade uppgifterna.
3. Användaren kontrollerar att förutsättningarna i 6 kap. 3 § eller 3 a § PDL är uppfyllda.
4. Användaren gör ett aktivt val (nr. 2) innan han eller hon får ta del av uppgifterna om patienten.

Uppgift om spärrade uppgifter vid sammanhållen journalföring

4 kap. 7 § HSLF-FS 2016:40

Vårdgivaren ska ansvara för att det framgår av systemet med sammanhållen journalföring att det finns spärrade uppgifter om en patient hos någon annan vårdgivare.

Vårdgivaren ska även ansvara för att information om vilken eller vilka vårdgivare som har spärrade uppgifter om en patient endast görs tillgängliga efter att en behörig användare har gjort ett aktivt val.

Uppgift om spärrade uppgifter

Av 6 kap. 2 § andra stycket PDL framgår att uppgift om att det finns spärrade uppgifter om en patient samt uppgift om vilken vårdgivare som har spärrat uppgifterna får göras tillgängliga för andra vårdgivare genom sammanhållen journalföring. En annan vårdgivare får bara ta del av uppgift om vilken vårdgivare som har spärrat uppgifterna under de förutsättningar som anges i 6 kap. 4 § PDL.

Patientens möjlighet att spärra uppgifter omfattar alltså inte uppgift om att det finns spärrade uppgifter om patienten och uppgift om vilken vårdgivare som har spärrat uppgifterna (prop. 2007/08:126 s. 248). Systemet ska därför vara uppbyggt på så sätt att andra vårdgivare ska kunna ta del av uppgift om att det finns spärrade uppgifter utan att ta del av uppgiften om vilken vårdgivare som har spärrat uppgifterna (prop. 2007/08:126 s. 249). Syftet är enligt förarbetena att kännedomen om att det finns spärrade uppgifter kan initiera en önskvärd dialog mellan en patient och hälso- och sjukvårdspersonal i en enskild vårdsituation (prop. 2007/08:126 s. 249).

Vårdgivaren ansvarar enligt 4 kap. 7 § första stycket HSLF-FS 2016:40 för att en användare ska kunna se i systemet med sammanhållen journalföring att det finns spärrade uppgifter om en patient hos någon annan vårdgivare, men inte hos vilken.

En patient kan när som helst begära att den vårdgivare som har spärrat uppgifterna häver spärren (6 kap. 2 § fjärde stycket PDL). Annars får en annan vårdgivare ta del av uppgift om vilken eller vilka vårdgivare som har spärrat uppgifterna endast under de förutsättningar som anges i 6 kap. 4 § PDL. Om det finns spärrade uppgifter om en patient och det föreligger fara för patientens liv eller det annars föreligger allvarlig risk för dennes hälsa får vårdgivaren, om inte patienten själv kan häva spärren, ta del av uppgift om vilken eller vilka vårdgivare som har spärrat uppgifterna (6 kap. 4 § första stycket PDL).

Vårdgivaren ansvarar för att behörig användare gör ett aktivt val innan han eller hon tar del av information om vilken eller vilka vårdgivare som har spärrade uppgifter om en patient (4 kap. 7 § andra stycket HSLF-FS 2016:40). För att sedan få tillgång till de spärrade uppgifterna måste förut-

sättningarna enligt 6 kap. 4 § PDL och 4 kap. 8 § HSLF-FS 2016:40 vara uppfyllda, som behandlas i nästa avsnitt.

Nödöppning vid sammanhållen journalföring

4 kap. 8 § HSLF-FS 2016:40

En vårdgivare som är ansluten till systemet med sammanhållen journalföring ska säkerställa att behöriga användare får tillgång till de uppgifter om en patient som kan antas ha betydelse för den vård patienten oundgängligen behöver när det föreligger fara för hans eller hennes liv eller allvarlig risk för hans eller hennes hälsa.

Vid en sådan situation som avses i 6 kap. 4 § patientdatalagen (2008:355) ska vårdgivaren ansvara för att åtkomst till information om vilken eller vilka vårdgivare som har uppgifter om en patient föregås av att den behörige användaren gör ett aktivt val.

Vidare ska vid en sådan situation åtkomsten till ospärrade uppgifter om en patient hos en annan vårdgivare föregås av ytterligare ett aktivt val. Om uppgifterna är spärrade, ska en begäran om åtkomst göras hos den vårdgivare som har spärrat uppgifterna.

Vårdgivaren ska säkerställa att behöriga användare får tillgång till de uppgifter om en patient som kan antas ha betydelse för den vård patienten oundgängligen behöver när det föreligger fara för patientens liv eller allvarlig risk för patientens hälsa (4 kap. 8 § första stycket HSLF 2016:40). Det gäller oavsett om uppgifterna finns hos en annan vårdenhet (exempelvis inom samma landsting) eller en annan vårdgivare (exempelvis ett annat landsting) och oavsett om uppgifterna är spärrade eller ospärrade. Även i en sådan situation är det viktigt att så långt som möjligt respektera patientens spärrar.

Nödöppning av spärrade uppgifter vid sammanhållen journalföring

Om vårdgivaren med ledning av uppgiften om vilken eller vilka vårdgivare som har spärrat uppgifterna (som beskrivs under förgående avsnitt till 4 kap. 7 § HSLF-FS 2016:40) bedömer att de spärrade uppgifterna kan antas ha betydelse för den vård som patienten oundgängligen behöver, ska en begäran om åtkomst göras hos den vårdgivare som har spärrat uppgifterna (4 kap. 8 § tredje stycket HSLF-FS 2016:40 och 6 kap. 4 § första stycket PDL). Uppgift om vilken eller vilka vårdgivare som har de spärrade uppgifterna ska alltså ligga till grund för vårdgivarens bedömning om spärren för uppgifterna om patienten ska hävas eller inte. Genom att vårdgivaren kan se hos vilken eller vilka vårdgivare som det finns spärrade uppgifter, kan vårdgivaren bedöma om uppgifterna kan antas ha betydelse för den vård som patienten oundgängligen behöver. Endast en spärr för uppgifter som kan antas ha sådan bety-

delse får hävas (prop. 2007/08:126 s. 253). Kravet ”kan antas ha betydelse” förutsätter att den som avser bereda sig tillgång till uppgifterna gör något aktivt ställningstagande till vilken betydelse uppgifterna kan ha (prop. 2007/08:126 s. 253). Det bör vara den eller de behöriga befattningshavarna hos vårdgivaren som ges denna åtkomst respektive får behandla uppgifterna. Vem som är behörig befattningshavare bestäms av vårdgivaren (prop. 2007/08:126 s. 253).

En vårdgivare som är ansluten till systemet med sammanhållen journalföring ska säkerställa att behörig användare får tillgång till de uppgifter om en patient som kan antas ha betydelse för den vård patienten oundgängligen behöver när det föreligger fara för hans eller hennes liv eller allvarlig risk för hans eller hennes hälsa (4 kap. 8 § första stycket HSLF-FS 2016:40).

Exempel – nödöppning av spärrade uppgifter vid sammanhållen journalföring

Med utgångspunkt i vad som beskrivs i avsnitten ovan, följer ett exempel på hur en behörig användare kan få åtkomst till spärrade uppgifter genom nödöppning.

1. Användaren kan se att någon annan vårdgivare har spärrade uppgifter om en viss patient, dock inte vilka eller vilken vårdgivare. Det föreligger fara för patientens liv eller allvarlig risk för patientens hälsa.
2. Användaren gör ett aktivt val i systemet för att därefter kunna se vilken eller vilka vårdgivare som har gjort de spärrade uppgifterna om patienten tillgängliga.
3. Med ledning av uppgiften (om vilken eller vilka vårdgivare som gjort uppgifterna tillgängliga) bedömer användaren att de spärrade uppgifterna kan antas ha betydelse för den vård som patienten oundgängligen behöver.
4. Begäran om åtkomst ska göras hos den vårdgivare som har spärrat uppgifterna.

Nödöppning av ospärrade uppgifter vid sammanhållen journalföring

I avsnittet om åtkomst till ospärrade uppgifter vid sammanhållen journalföring (s. 42) beskrivs att det i systemet för sammanhållen journalföring ska framgå att det finns ospärrade uppgifter om patienten, men inte hos vilken eller vilka vårdgivare (6 kap. 2 § femte stycket PDL).

Om patientens samtycke inte kan inhämtas enligt 6 kap. 3 § PDL, får en vårdgivare ta del av uppgift om vilken eller vilka vårdgivare som har gjort uppgifterna tillgängliga om det föreligger fara för patientens liv eller det annars föreligger allvarlig risk för dennes hälsa (6 kap. 4 § andra stycket PDL).

För att få åtkomst till information om vilken eller vilka vårdgivare som har de ospärrade uppgifterna om patienten, ska behörig användare först göra ett aktivt val i systemet (4 kap. 8 § andra stycket HSLF-FS 2016:40).

Om vårdgivaren med ledning av denna uppgift (det vill säga vilken eller vilka vårdgivare som har gjort uppgifterna tillgängliga) bedömer att de ospärrade uppgifterna kan antas ha betydelse för den vård som patienten

oundgängligen behöver, får vårdgivaren behandla de ospärrade uppgifterna. Innan användaren får åtkomst till de ospärrade uppgifterna ska användaren göra ytterligare ett aktivt val (4 kap. 8 § tredje stycket HSLF-FS 2016:40).

Exempel - nödöppning av ospärrade uppgifter vid sammanhållen journalföring

Nedan följer ett exempel på hur en behörig användare kan få åtkomst till ospärrade uppgifter som gjorts tillgängliga i ett system för sammanhållen journalföring genom nödöppning.

1. En användare kan se att någon annan vårdgivare har ospärrade uppgifter om en viss patient, dock inte vilken eller vilka vårdgivare. Det föreligger fara för patientens liv eller allvarlig risk för patientens hälsa.
2. Användaren gör ett aktivt val (nr. 1) i systemet för att därefter kunna se vilken eller vilka vårdgivare som har gjort de ospärrade uppgifterna tillgängliga.
3. Med ledning av informationen (om vilken eller vilka vårdgivare som har gjort de ospärrade uppgifterna tillgängliga) bedömer användaren att de ospärrade uppgifterna kan antas ha betydelse för den vård som patienten oundgängligen behöver.
4. Användaren gör ytterligare ett aktivt val (nr. 2) i systemet för att ta del av de ospärrade uppgifterna.

Schematisk bild hur åtkomst till uppgifter om en patient kan se ut

	Inom en vårdgivare	Mellan olika vårdgivare
Utgångspunkt	Det framgår av systemet att det finns ospärrade eller spärrade uppgifter vid någon annan vårdenhet eller i en annan vårdprocess, men inte vilken.	Det framgår av systemet att det finns ospärrade eller spärrade uppgifter hos någon annan vårdgivare, men inte vilken.
Ospärrade uppgifter	Användaren vill se vilken vårdenhet/vårdprocess som har uppgifter om en patient, alltså gör användaren ett aktivt val (nr. 1). Användaren vill se uppgifterna vid annan vårdenhet/vårdprocess, alltså gör användaren ytterligare ett aktivt val (nr. 2).	Användaren gör aktivt val (nr. 1) för att ta del av uppgift om vilken/vilka vårdgivare som har de ospärrade uppgifterna. Användaren vill se uppgifterna hos vårdgivaren, alltså kontrolleras att förutsättningarna enligt 6 kap. 3 § eller 3 a § PDL är uppfyllda. Användaren gör sedan ett aktivt val (nr. 2) för att ta del av uppgifterna. **Nödöppning** Fara föreligger för patientens liv eller allvarlig risk för hälsa, så användaren gör ett aktivt val (nr. 1) för att se vilken eller vilka vårdgivare som har uppgifterna. Användaren bedömer att uppgifterna kan antas ha betydelse för den vård som patienten oundgängligen behöver. Användaren gör ytterligare ett aktivt val (nr. 2) för att ta del av de ospärrade uppgifterna.
Spärrade uppgifter	Patienten samtycker till att spärren hävs. Patientens samtycke kan inte inhämtas. Uppgift om vårdenheter eller vårdprocesser som spärrat uppgifterna kan antas ha betydelse för vården som patienten oundgängligen behöver. Användaren gör ett aktivt val (nr. 1) för att se vilken vårdenhet eller vårdprocess som spärrat uppgifterna. Användaren gör ett aktivt val (nr. 2) innan han eller hon tar del av uppgifterna som kan antas ha betydelse för vården av patienten.	Patienten häver spärren själv. **Nödöppning** Fara föreligger för patientens liv eller allvarlig risk för hälsa, så användaren gör ett aktivt val för att se vilken eller vilka vårdgivare som har uppgifterna. Användaren bedömer att de spärrade uppgifterna kan antas ha betydelse för den vård som patienten oundgängligen behöver. Begäran om åtkomst ska göras hos den vårdgivare som har spärrat uppgifterna.

Kontroll av åtkomst till uppgifter

4 kap. 9 § HSLF-FS 2016:40

Vårdgivaren ska ansvara för att

1. det av dokumentationen av åtkomsten (loggar) framgår vilka åtgärder som har vidtagits med uppgifter om en patient,
2. det av loggarna framgår vid vilken vårdenhet eller vårdprocess åtgärderna vidtagits,
3. det av loggarna framgår vid vilken tidpunkt åtgärderna vidtagits,
4. användarens och patientens identitet framgår av loggarna,
5. systematiska och återkommande stickprovskontroller av loggarna görs,
6. kontroller av loggarna dokumenteras, och
7. loggarna sparas minst fem år för att möjliggöra kontroll av åtkomsten till uppgifter om en patient.

Bestämmelsen i 4 kap. 9 § HSLF-FS 2016:40 anger närmare hur kontroll av elektronisk åtkomst enligt 4 kap. 3 § PDL ska ske. Vårdgivaren ska, enligt 4 kap. 3 § PDL, se till att åtkomst till sådana uppgifter om patienter som förs helt eller delvis automatiserat dokumenteras och kan kontrolleras. Vårdgivaren ska göra systematiska och återkommande kontroller av om någon obehörigen kommer åt sådana uppgifter. Bestämmelsen i 4 kap. 2 § PDL gäller även för åtkomstkontroll vid sammanhållen journalföring (6 kap. 7 § PDL).

Vårdgivaren ansvarar bland annat för att det av dokumentationen av åtkomsten (loggar) framgår vilka åtgärder som har vidtagits med uppgifter om en patient. Ett aktivt val för att få tillgång till uppgifter om en patient är ett exempel på en åtgärd som ska loggas. Genom sitt aktiva val bekräftar användaren att förutsättningarna för åtkomst är uppfyllda. Vårdgivaren ansvarar också för att loggarna sparas minst fem år för att möjliggöra kontroll av åtkomsten till uppgifter om en patient.

Syftet med åtkomstkontroll

Åtkomstkontroller ska göras för att säkerställa att användare inte använder sina behörigheter på fel sätt genom att läsa, ändra eller ta bort information som de inte ska behandla. Exempel på en felaktig åtkomst kan vara att någon tittar i en patientjournal trots att han eller hon inte deltar i vården av patienten eller av annat skäl behöver uppgiften för sitt arbete inom hälso- och sjukvården (4 kap. 1 § PDL). För att vårdgivaren ska kunna kontrollera att behörigheterna används på ett korrekt sätt måste denne dokumentera (logga) åtkomsten till de uppgifter som har använts.

I förarbetena till PDL betonas vikten av uppföljningskontroller, inte bara för att utreda åtkomst som faktiskt har skett utan även som en preventiv åtgärd. Med en väl fungerande åtkomstkontroll kan ett intrång upptäckas i efterhand och användaren kan tänka sig för innan han eller hon gör något

intrång. Det räcker dock inte att bara göra åtkomstkontroller i särskilda fall när ett obehörigt intrång misstänks. Vårdgivaren måste göra systematiska och återkommande kontroller av om det förekommer någon obehörig åtkomst till uppgifter om patienterna. I förarbetena till PDL angavs som skäl till införandet av bestämmelsen i 4 kap. 3 § PDL att det skulle bli lättare att identifiera faktiska dataintrång och vidta åtgärder mot dem, men att kontrollerna troligen också skulle ha avhållande effekt på personal som annars skulle frestas att olovligen läsa uppgifter (prop. 2007/08:126 s. 150 och 282).

Systematiska och återkommande kontroller

Åtkomstkontrollerna ska göras systematisk och återkommande (4 kap. 3 § PDL). Hur ofta det behöver göras kan exempelvis bero på verksamhetens omfattning, antalet personer med åtkomst, hur behörigheterna delas ut och hur omfattande kontrollerna är. Det är nödvändigt att kontrollerna görs regelbundet och omfattar en så hög andel av logghändelserna att det blir en effektiv kontroll. Målet med kontrollen är enligt förarbetena att både upptäcka och att verka avhållande från intrång (prop. 2007/08:126 s. 150). När det gäller vissa kategorier av uppgifter kan det behövas särskilda riskanalyser för att bestämma vilken nivå av kontroll som är rimlig. Det kan exempelvis gälla skyddade personuppgifter som är sekretessmarkerade, uppgifter om barn eller allmänt kända personer samt uppgifter från vissa mottagningar eller medicinska specialiteter. Det finns automatiserade stöd för logghantering och efterkontroll som kan underlätta arbetet för vårdgivare som hanterar stora mängder loggar.

4 kap. 10 § HSLF-FS 2016:40

Av informationen som vårdgivaren enligt 8 kap. 5 § patientdatalagen (2008:355) på begäran ska lämna till en patient om åtkomsten till hans eller hennes uppgifter ska det framgå från vilken vårdenhet samt vid vilken tidpunkt någon har tagit del av uppgifterna. Informationen ska vara utformad så att patienten kan bedöma om åtkomsten har varit befogad eller inte.

Information till patienten om åtkomst till uppgifter

Vårdgivaren ska enligt 8 kap. 5 § PDL på begäran av en patient lämna information om den direktåtkomst och den elektroniska åtkomst till uppgifter om patienten som förekommit. Bestämmelsen är tillämplig inom både den offentliga och privata hälso- och sjukvården. Av informationen som lämnas till patienten ska det framgå från vilken vårdenhet och vid vilken tidpunkt någon har tagit del av uppgifterna. Informationen ska vara utformad så att patienten kan bedöma om åtkomsten har varit befogad eller inte.

Enligt förarbetena till PDL förstärks allmänhetens förtroende för hälso- och sjukvårdens informationshantering om den enskilde får klar och tydlig information om vilken åtkomst som förekommit. För den patient som oroar sig för att någon obehörig läst patientjournalen är bearbetade logglistor med

förklaringar ett verktyg att själv kunna konstatera om oron varit befogad eller inte. Liksom när det gäller systematiska och återkommande åtkomstkontroller, torde vetskapen om patientens rätt att själv kontrollera åtkomsten ha en starkt avhållande verkan (prop. 2007/08:126 s. 150).

Avsikten med bestämmelsen i PDL är att informationen ska vara anpassad och klargörande för den enskilde i syfte att han eller hon enkelt ska kunna tillgodogöra sig den (prop. 2007/08:126 s. 265). Informationen som lämnas måste alltså vara begriplig och vägledande för patienten när han eller hon själv ska bilda sig en uppfattning om åtkomsten varit befogad eller inte (prop. 2007/08:126 s. 265). Enligt förarbetena bör det till exempel tydligt framgå när och från vilken enhet inom hälso- och sjukvården en slagning har skett. Vid sammanhållen journalföring bör vidare varje vårdgivare kunna redovisa vilken åtkomst till den egna verksamhetens journaluppgifter som har förekommit från andra vårdgivare. Även andra mottagande vårdgivare bör kunna redovisa när direktåtkomst har använts. Hur informationen närmare ska utformas framgår dock inte av lagen (prop. 2007/08:126 s. 265).

Av förarbetena till PDL följer att det inte finns något behov av att namnge hälso- och sjukvårdspersonalen eller att ge andra uppgifter som indirekt kan hänföras till en fysisk person. För detta ändamål är det tillräckligt att ange från vilken avdelning, klinik eller motsvarande enhet som åtkomsten härrör (prop. 2007/08:126 s. 150).

Inom den offentliga hälso- och sjukvården utgör logglistorna allmänna handlingar som patienten också kan begära ut med stöd av 2 kap. tryckfrihetsförordningen. Någon sekretess torde normalt inte kunna anföras som skäl mot att lämna ut sådana listor (prop. 2007/08:126 s. 150).

Patientens rätt att få logginformation minskar inte vårdgivarens ansvar att följa upp hur behörighetssystemet fungerar och om det förekommer några obehöriga intrång (4 kap. 3 § och 6 kap. 7 § PDL).

Direktåtkomst till uppgifter om den enskilde själv

4 kap. 11 § HSLF-FS 2016:40

Vårdgivaren ska ansvara för att en enskilds direktåtkomst till uppgifter om sig själv och till dokumentation om åtkomst tillåts endast efter att den enskildes identitet har säkerställts genom stark autentisering.

4 kap. 12 § HSLF-FS 2016:40

Om vårdgivaren endast medger en begränsad direktåtkomst, ska denne informera den enskilde om detta.

Vårdgivaren ska även informera den enskilde om vart han eller hon kan vända sig för att få hjälp med att förstå dokumentationen.

Av 5 kap. 5 § PDL framgår att vårdgivaren får medge en enskild direktåtkomst till delar av eller hela sin patientjournal. Genom direktåtkomst kan vårdgivaren få bättre kommunikation och dialog med sina patienter. För direktåtkomst används vanligen öppna nät, se 3 kap. 15-17 §§ HSLF-FS 2016:40. För att nå ut till en bred patientskara kan Internet vara användbart som kommunikationskanal men då ska vårdgivaren kunna identifiera patienten på ett säkert sätt och även ha ett skydd mot att obehöriga tar del av uppgifterna när de förs över.

Identifiering med stark autentisering

För att en patient ska få direktåtkomst till uppgifter om sig själv och till dokumentation om åtkomst måste vårdgivaren säkerställa den enskildes identitet genom stark autentisering. Det innebär bland annat att vårdgivaren använder inloggningslösningar som ställer krav på att identiteten kontrolleras på minst två olika sätt (se definition av stark autentisering i 2 kap. 1 § HSLF-FS 2016:40), exempelvis

- med någonting användaren kan – till exempel lösenord
- med någonting användaren har – till exempel kodbox, certifikat, smartkort, engångskoder eller mobiltelefon
- med hjälp av användaren själv – till exempel fingeravtryck eller avläsning av iris

En etablerad metod för stark autentisering är att använda en e-legitimation. Det är en identitetshandling i elektronisk form som vid elektronisk kommunikation används för legitimering och underskrift. E-legitimationen kan lagras på en dator (certifikat på fil), på ett smartkort eller i en mobiltelefon.

Med hjälp av e-legitimationen och det tillhörande lösenordet (exempelvis en pinkod) skapas förutsättningar för en stark autentisering. Denna metod används bland annat av Skatteverket och Försäkringskassan för att låta kunderna identifiera sig och signera sina handlingar när de använder e-tjänster, till exempel vid deklaration och begäran om föräldraledighet.

Information till patienten om begränsad direktåtkomst

Om vårdgivaren endast medger en begränsad direktåtkomst, ska vårdgivaren informera den enskilde om detta. Tillgången till information kan till exempel vara begränsad genom beslut om sekretess. När och hur en begränsad direktåtkomst ska göras får bedömas i varje enskilt fall. För att kunna avgöra om uppgifter om en patient kan lämnas ut genom direktåtkomst eller inte behöver först en sekretessprövning göras. Utan en sådan prövning kan inga uppgifter lämnas direkt till patienten. Vissa uppgifter kan vara lämpligare att lämna i direktkontakt mellan patienten och den som ansvarar för patientens vård, till exempel vissa diagnoser, provsvar och undersökningsresultat. Efter sekretessprövningen måste det även tas ställning till om hela patientjournalen ska lämnas ut, om endast vissa delar av den görs tillgänglig eller enbart uppgifter från vissa vårdenheter.

I samband med att uppgifter om en patient lämnas ut genom direktåtkomst ska vårdgivaren även informera den enskilde om vart han eller hon kan

vända sig för att få hjälp med att förstå dokumentationen. Det kan exempelvis gälla att ge kontaktuppgifter till patientens behandlande läkare.

Direktåtkomst till ett ombud

Kammarrätten i Stockholm prövade frågan om en vårdgivare som behandlar personuppgifter med stöd av PDL får ge ombud direktåtkomst till vårdgivarens uppgifter om en enskild under samma förutsättningar som till den enskilde själv (dom den 10 juni 2016, mål nr. 5402-15). Kammarrätten bedömde att den enskildes samtycke enligt 2 kap. 3 § PDL ger rättsligt stöd åt att vårdgivare får ge direktåtkomst till ombud under samma förutsättningar som till den enskilde själv. Domen har överklagats till Högsta förvaltningsdomstolen, som har meddelat prövningstillstånd (mål nr. 3716-16).

Patientjournalens struktur och innehåll

Vårdgivaren ska säkerställa att de uppgifter som finns dokumenterade i en patientjournal finns tillgängliga på ett överskådligt sätt för den hälso- och sjukvårdspersonal som är behörig att ta del av uppgifterna (5 kap. 1 § HSLF-FS 2016:40). Vårdgivaren ska även säkerställa att uppgifterna i en patientjournal är entydiga (5 kap. 2 § HSLF-FS 2016:40).

Vid sammanhållen journalföring blir det än viktigare att journalspråket är enhetligt, det vill säga att de begrepp och termer som används är gemensamma. Journalföringen får inte leda till något onödigt administrativt arbete för hälso- och sjukvårdspersonalen. Varje journaluppgift bör om möjligt bara noteras en gång eftersom dubbeldokumentation tynger journalerna och gör dem svårtillgängliga (prop. 2007/08:126 s. 89).

Socialstyrelsen har regeringens uppdrag att utveckla och förvalta en nationell informationsstruktur (NI) och nationellt fackspråk. NI beskriver hur information som skapas för och om en patient ska struktureras i journalsystemen för att bli återanvändbar både nu och i framtiden. Nationellt fackspråk utgör ett stöd för att skapa innehållet i dokumentationen och omfattar begreppssystemet Snomed CT, hälsorelaterade klassifikationer och Socialstyrelsens termbank.

Information som dokumenteras om en patient måste kunna återanvändas i olika delar av patientens vårdprocess. NI och nationellt fackspråk möjliggör detta genom att de utgör grunden för att strukturera och koda information som ska dokumenteras i journalsystemen. Arbetet med strukturering och kodning av dokumentationen möjliggör utveckling av journalsystemen så att de stödjer effektiv dokumentation.

Tillämpningen av NI och nationellt fackspråk är en förutsättning för att säkerställa semantisk interoperabilitet, vilket innebär att information kan delas utan att innebörd och sammanhang går förlorat.

Allmänt om krav på journalföring

I 3 kap. PDL finns bestämmelser om vad skyldigheten att föra patientjournal innebär. Grundläggande bestämmelser om vad en patientjournal ska innehålla finns i 3 kap. 5-8 och 11 §§ PDL. En patientjournal ska bland annat innehålla de uppgifter som behövs för en god och säker vård av patienten (3 kap. 6 § PDL). I 5 kap. HSLF-FS 2016:40 finns föreskrifter som kompletterar PDL:s bestämmelser om vilka uppgifter en patientjournal i förekommande fall ska innehålla.

När ska patientjournal föras?

I 3 kap. 1 § PDL anges att vid vård av patienter ska det föras patientjournal, det vill säga vid åtgärder för att medicinskt förebygga, utreda och behandla sjukdomar och skador (1 § HSL). Av samma bestämmelse följer att en

patientjournal ska föras för varje patient och får inte vara gemensam för flera patienter. Skyldigheten att journalföra är densamma inom såväl offentlig som privat bedriven vård.

Vem är skyldig att föra patientjournal?

I 3 kap. 3 § PDL anges vilka som är skyldiga att föra patientjournal. Skyldigheten gäller främst den som har legitimation eller ett särskilt förordnande att utöva ett visst yrke inom hälso- och sjukvården eller tandvården. I vissa fall måste även icke-legitimerad personal föra patientjournaler, exempelvis personal inom hälso- och sjukvården som biträder en legitimerad yrkesutövare. Den som för patientjournal ansvarar enligt 3 kap. 4 § PDL för sina uppgifter i journalen.

Vid vård av patienter ska det föras patientjournal (3 kap. 1 § PDL). En verksamhet kan vara skyldig att se till att patientjournaler förs enligt 3 kap. 1 § PDL utan att ha anställda som är skyldiga att föra patientjournal enligt 3 kap. 3 § PDL. Då måste vårdgivaren ha de processer och rutiner som behövs för att säkerställa att skyldigheten fullgörs. Det kan innebära att även icke-legitimerad personal ska föra journal i enlighet med verksamhetens rutiner. Den som deltar i vården av en patient kan alltså behöva dokumentera uppgifter som har betydelse för patienters vård och behandling, även om den anställde inte är journalföringspliktig enligt lag.

Varför ska det föras patientjournal?

Syftet med att föra patientjournal är i första hand att bidra till en god och säker vård av patienten (3 kap. 2 § första stycket PDL). En patientjournal är även en informationskälla för patienten, uppföljning och utveckling av verksamheten, tillsyn och rättsliga krav, uppgiftsskyldighet enligt lag samt forskning (3 kap. 2 § andra stycket PDL).

Patientjournalen är av grundläggande betydelse för vård- och behandlingsarbetet inom hälso- och sjukvården. För patientsäkerheten kan det vara helt avgörande att olika åtgärder dokumenteras. Om olika vårdgivare har elektronisk åtkomst till varandras journaler får dokumentationen rimligen ännu större betydelse (prop. 2007/08:126 s. 89).

Patientjournalen är främst ett arbetsinstrument för den som ansvarar för patientens vård (prop. 2007/08:126 s. 89). En väl förd patientjournal har stor betydelse för patientsäkerheten och ökar tryggheten för personalen inom hälso- och sjukvården och tandvården. En bra journalföring minskar även risken för onödiga missförstånd om vården ifrågasätts eller om någon annan tar över ansvaret för en behandling. En gemensam struktur i patientjournalen möjliggör återanvändning av information och minskar dubbeldokumentation.

Hur snabbt ska uppgifter som ska dokumenteras föras in i patientjournalen?

Uppgifter som ska antecknas i en patientjournal ska enligt 3 kap. 9 § PDL föras in i journalen så snart som möjligt. Vårdgivarens ska också genom sitt ledningssystem säkerställa att dokumenterade personuppgifter hos vårdgivaren är åtkomliga och användbara för den som är behörig (3 kap. 2 § HSLF-FS 2016:40).

För att kunna tillgodose patienterna en god och säker vård är det viktigt att väsentliga uppgifter om vården finns tillgängliga så fort som möjligt efter ett besök i vården. Samtidigt är det förståeligt att det kan gå en kort tid innan en uppgift blir införd i journalen. Mot bakgrund av PDL:s krav på att uppgiften ska föras in i journalen så snart som möjligt kan det dock inte vara fråga om någon längre fördröjning.

I ett tillsynsbeslut den 24 november 2008 (dnr 44-9129/08) meddelade Socialstyrelsen att en viss vårdgivare bland annat måste se till att samtliga journaldiktat vid en akutklinik i fortsättningen ska journalföras fortlöpande och senast inom två dygn från den aktuella medicinska åtgärden. Socialstyrelsens bedömning gjordes mot bakgrund av att tillsynen gällde verksamheten vid en akutklinik.

Det är lämpligt att vårdgivaren anpassar sina processer och rutiner för hur snabbt en journalanteckning ska föras in i patientjournalen utifrån vilken typ av verksamhet som bedrivs och vilka särskilda behov som finns.

Vad är en patientjournal?

Patientjournalen består av en eller flera journalhandlingar som rör samma patient. En journalhandling definieras i 1 kap. 3 § PDL som en framställning i skrift eller bild samt upptagning som kan läsas, avlyssnas eller på annat sätt uppfattas endast med tekniskt hjälpmedel och som upprättas eller inkommer i samband med vården av en patient och som innehåller uppgifter om patientens hälsotillstånd eller andra personliga förhållanden eller om vidtagna eller planerade vårdåtgärder.

Patientjournalens struktur

5 kap. 1 § HSLF-FS 2016:40

Vårdgivaren ska säkerställa att de uppgifter som finns dokumenterade i en patientjournal finns tillgängliga på ett överskådligt sätt för den hälso- och sjukvårdspersonal som är behörig att ta del av uppgifterna.

Allmänna råd
De delar av en patients journal som hör till en och samma individanpassade vårdprocess bör hållas samman.

Uppgifterna ska finnas tillgängliga på ett överskådligt sätt

Syftet med att föra patientjournal är i första hand att bidra till en god och säker vård av patienten (3 kap. 2 § PDL). Tillgängligheten till uppgifterna i patientjournalen är av central betydelse för att kunna uppnå detta syfte. Därför måste de uppgifter som finns dokumenterade i en journal finnas tillgängliga på ett överskådligt sätt för den hälso- och sjukvårspersonal som

är behörig att ta del av de uppgifterna. En gemensam struktur med mindre fritext medför ökad tillgänglighet och överblick.

Vid sammanhållen journalföring blir det än viktigare att journalspråket är enhetligt, det vill säga att de begrepp och termer som används är gemensamma. Journalföringen får inte leda till något onödigt administrativt arbete för hälso- och sjukvårdspersonalen. Varje journaluppgift bör om möjligt också bara noteras en gång eftersom dubbeldokumentation tynger journalerna och gör dem svårtillgängliga. Med hjälp av en enhetlig struktur blir det också lättare att se om en uppgift redan finns antecknad i journalen och alltså inte behöver journalföras på nytt (prop. 2007/08:126 s. 89).

Vissa uppgifter i en patientjournal kan behöva vara särskilt lättillgängliga, till exempel en fullständig anamnes, en aktuell läkemedelslista, uppgifter om att patienten bär på någon vårdhygienisk smitta, uppgifter om överkänslighet samt varningsinformation.

Med tanke på patientsäkerheten är det särskilt viktigt med rutiner för remisshantering. För en säker remisshantering kan det vara nödvändigt att patientjournalen innehåller tydliga bevaknings- och sökfunktioner för att man ska kunna kontrollera att remisser skickas och att remissvaret når den som ansvarar för remissen. Dessutom kan det behövas en tydlig bevakningsfunktion för att ta del av till exempel provsvar. Bestämmelser om remisshantering finns i Socialstyrelsens föreskrifter (SOSFS 2004:11) om ansvar för remisser för patienter inom hälso- och sjukvården, tandvården m.m.

Individanpassad vårdprocess

Information i en patientjournal behöver dokumenteras strukturerat så att den vid senare tillfällen kan återsökas och tillgängliggöras i sitt rätta sammanhang, kopplad till rätt individanpassad vårdprocess. En individanpassad vårdprocess är en patients faktiska process i vården. Den utgår ifrån en mer standardiserad beskrivning av en vårdprocess och anpassas utifrån den enskilda individens hälsoproblem och behov. Patienten kan ha flera olika pågående individanpassade vårdprocesser, vissa livslånga (vid kronisk sjukdom), andra under en kortare period.

I 4 kap. 2 § Socialstyrelsens föreskrifter och allmänna råd (SOSFS 2011:9) om ledningssystem för systematiskt kvalitetsarbete ställs krav på att vårdgivaren ska identifiera, beskriva och fastställa de processer i verksamheten som behövs för att säkra verksamhetens kvalitet. Socialstyrelsens nationella informationsstruktur (NI) kan användas som stöd för att beskriva verksamhetens processer och informationsbehoven i dessa. NI beskriver vårdprocessen i hälso- och sjukvården samt informationsbehoven på en övergripande nivå.

För att vid dokumentationstillfället kunna koppla information till rätt individanpassad vårdprocess, har behovet av någon form av process-id diskuterats. Ett process-id skulle kunna användas för att ”märka upp” information som dokumenteras. Beskrivningar av hur detta skulle kunna fungera i hälso- och sjukvården i framtiden finns bland annat i Socialstyrelsens rapport ”Hälsoärende och process-id – Förutsättningar för en sammanhållen vård- och omsorgsdokumentation kring individanpassade processer”. År 2016 påbörjade Socialstyrelsen ett arbete för att visa nyttan av att knyta ihop olika

händelser i patientens individanpassade vårdprocess med hjälp av ett processid och på detta sätt skapa förutsättningar för en sammanhållen dokumentation.

Patientjournalens innehåll

5 kap. 2 § HSLF-FS 2016:40

Vårdgivaren ska säkerställa att uppgifterna i en patientjournal är entydiga.

Allmänna råd
För att försäkra sig om att uppgifterna är entydiga bör vårdgivaren använda följande publikationer, när de är tillämpliga:
– Socialstyrelsens termbank
– Internationell statistisk klassifikation av sjukdomar och relaterade hälsoproblem (ICD-10-SE)
– Klassifikation av vårdåtgärder (KVÅ)
– Klassifikation av funktionstillstånd, funktionshinder och hälsa (ICF)
– Systematized Nomenclature of Medicine – Clinical Terms (Snomed CT).

Entydiga uppgifter

Vårdgivaren ska säkerställa att uppgifterna i en patientjournal är entydiga. Vårddokumentationen ska vara ett ändamålsenligt verktyg för patientens vård och behandling, oavsett var dokumentationen ska användas. Därför är det viktigt att använda en enhetlig och jämförbar terminologi. Väldefinierade begrepp och entydiga termer är särskilt viktiga vid sammanhållen journalföring så att olika vårdgivare och yrkesgrupper tolkar informationen på samma sätt (prop. 2007/08:126 s. 89).

Journalen behöver vara strukturerad på ett sätt så att information är möjlig att extrahera och ta del av i sitt rätta sammanhang. Information i en patientjournal behöver också registreras med entydiga och gemensamt överenskomna termer och koder, så att den inte kan misstolkas när den återanvänds i olika syften.

Socialstyrelsens termbank

Socialstyrelsens termbank innehåller begrepp som har analyserats enligt terminologilärans metoder och principer i samarbete mellan terminolog och sakkunniga. Begreppen har sedan förankrats hos kommuner, landsting, privata vårdgivare, myndigheter och andra organisationer. När begreppen är publicerade rekommenderas de för användning inom fackområdet vård och omsorg. Termbanken innehåller främst vård- och omsorgsadministrativa begrepp. Mer information finns på Socialstyrelsens webbplats.

Internationell statistisk klassifikation av sjukdomar och relaterade hälsoproblem (ICD-10-SE)

Klassifikationen är den svenska versionen av den tionde revisionen av The International Statistical Classification of Diseases and Related Health Problems (ICD-10) som utgavs av Världshälsoorganisationen (WHO). Det primära syftet med ICD-10 och denna svenska motsvarighet är att möjliggöra klassificering och statistisk beskrivning av sjukdomar och andra hälsoproblem som är aktuella som orsak till människors död eller kontakter med hälso- och sjukvården. Förutom traditionella diagnoser måste klassifikationen därför omfatta ett brett spektrum av symtom, onormala fynd, besvär och sociala förhållanden. Mer information finns på Socialstyrelsens webbplats.

Klassifikation av vårdåtgärder (KVÅ)

Klassifikationen KVÅ ska ses som en gemensam åtgärdsklassifikation för alla kategorier av hälso- och sjukvårdspersonal. Enhetlig registrering av åtgärder ska ligga till grund för verksamhetsuppföljning på lokal, regional och nationell nivå. Klassifikationen ska primärt möjliggöra uppföljning av vårdinnehållet och sekundärt till detta vårdtyngd och resursåtgång. Mer information finns på Socialstyrelsens webbplats.

Klassifikation av funktionstillstånd, funktionshinder och hälsa (ICF)

Klassifikationen är en av WHO:s huvudklassifikationer. ICF erbjuder en struktur och ett standardiserat språk för att beskriva funktionstillstånd och funktionshinder i relation till hälsa. Klassifikationerna kompletterar ICD-10 då två personer med samma sjukdom kan ha olika nivåer av funktionstillstånd. ICF kan användas som kliniskt verktyg för att beskriva och dokumentera aktuellt funktionstillstånd, sätta mål, bedöma behov och följa resultat inom olika områden i vården och omsorgen. De kan också användas som ett statistiskt verktyg för att samla in och sammanställa data för olika ändamål. Mer information finns på Socialstyrelsens webbplats.

Snomed CT

Snomed CT är ett internationellt, medicinskt begreppssystem som är utvecklat för att användas i elektroniska journalsystem och som är översatt till svenska. Man skulle kunna säga att Snomed CT är en omfattande ordlista som gör det möjligt för hälso- och sjukvårdspersonal att dokumentera information om patienten med hjälp av en kontrollerad och styrande terminologi. Användning av Snomed CT bidrar till att det kliniska innehållet i patientjournalerna håller högre kvalitet eftersom informationen är standardiserad. När det kliniska innehållet i dokumentationen standardiseras blir den entydig, jämförbar och lättare att tolka. Dessutom ges bättre förutsättningar för att informationen kan kommuniceras och överföras på ett mer automatiserat sätt och med bibehållen betydelse mellan olika informationssystem. Genom att dokumentera med hjälp av Snomed CT kan framtida behov av data fångas direkt i källan (patientjournalen). Det kan till exempel röra sig om att koppla ett kliniskt beslutsstöd till patientjournalen eller att hämta

uppgifter om patienter till ett register. Mer information finns på Socialstyrelsens webbplats.

5 kap. 3 § HSLF-FS 2016:40

Vårdgivaren ska, utöver vad som följer av 3 kap. 5-8 och 11 §§ patientdatalagen (2008:355), säkerställa att patientjournalen innehåller

1. en entydig identifikation av den berörda patienten,
2. patientens kontaktuppgifter,
3. uppgifter om namn och befattning på den personal som svarar för en viss journaluppgift, och
4. tidpunkten för varje vårdkontakt som patienten har haft eller som planeras.

Entydig identifikation av den berörda patienten

En patientjournal ska föras för varje patient och får inte vara gemensam för flera patienter (3 kap. 1 § PDL). Om uppgifterna finns tillgängliga ska en patientjournal alltid innehålla uppgift om patientens identitet (3 kap. 6 § PDL). Det är därför viktigt att vårdgivaren i verksamhetens ledningssystem har de processer och rutiner som behövs för att kontrollera patienternas identitet. Det är av stor vikt att vårdgivaren undviker att förväxla patienterna och att vårdgivaren gör det svårt för någon att använda en falsk identitet för att få vård. När det gäller vård av barn måste vårdgivaren försvissa sig om att den vuxne är vårdnadshavaren, som är den som enligt 6 kap. 11 § föräldrabalken har skyldighet att bestämma i frågor som rör barnets personliga angelägenheter.

Det är viktigt att alla journalhandlingar i patientjournalen är försedda med en entydig personidentifikation såsom för- och efternamn samt personnummer.

Rätt till anonym provtagning föreligger dock vid misstanke om hivinfektion (förordningen [2008:363] om provtagning för hivinfektion). Detta innebär att PDL:s krav på uppgifter om en patients identitet inte gäller om patienten begär att ett sådant prov tas anonymt. Anonymitetsskyddet bortfaller om provtagningen visar att patienten är hivsmittad.

Patientens kontaktuppgifter

Vårdgivaren ska även säkerställa att patientjournalen innehåller patientens kontaktuppgifter genom att notera dennes senast kända adress eller andra användbara kontaktuppgifter.

Namn och befattning

Patientjournalen ska också innehålla uppgifter om namn på den som ansvarar för en viss journaluppgift. Det ska också framgå vilken befattning den personen har.

Tidpunkt för vårdkontakt

Verksamhetens behov får avgöra hur tidsangivelser ska anges i journalerna. Inom vissa verksamheter kan det räcka med endast datum men ofta kan det vara väsentligt att ange ett klockslag. Exempelvis kan klockslaget för olika behandlingssituationer vara viktigt inom intensivvården, medan det oftast räcker med datum för ett årligt besök hos en tandläkare.

5 kap. 4 § HSLF-FS 2016:40

Vårdgivaren ska säkerställa att det är möjligt att föra patientjournal om

1. en patients identitet inte kan fastställas,
2. en patient saknar svenskt personnummer, eller
3. en patient har skyddade personuppgifter.

Vad gäller om en patients identitet inte kan fastställas?

En patientjournal ska enligt 3 kap. 6 § PDL innehålla uppgifter om en patients identitet. Det innebär dock inte att det är möjligt att neka en patient nödvändig vård för att hans eller hennes identitet inte kan fastställas. Vårdgivaren måste därför genom processer och rutiner i sitt ledningssystem säkerställa att det är möjligt att föra patientjournal även om en patients identitet inte kan fastställas. Detta gäller också vid vård av patienter som saknar svenskt personnummer eller som har skyddade personuppgifter.

Skyddade personuppgifter

Normalt är personuppgifter i folkbokföringsregistret offentliga, men på grund av olika hotbilder kan en persons uppgifter skyddas. Skyddade personuppgifter är Skatteverkets samlingsrubrik för de olika skyddsåtgärder som finns inom folkbokföringen. De skyddsåtgärder som ryms inom denna samlingsrubrik är sekretessmarkering, kvarskrivning och fingerade personuppgifter. Vårdgivaren ska säkerställa att det är möjligt att föra patientjournal även om patienten har skyddade personuppgifter.

Skatteverket kan välja att göra en sekretessmarkering om någon kan råka ut för personförföljelse eller annan skada om hans eller hennes personuppgifter lämnas ut. Då sätts en så kallad markering för särskild sekretessprövning (”sekretessmarkering”) för den personen i folkbokföringsdatabasen. Sekretessmarkeringen motsvarar i princip den hemligstämpling som en allmän handling kan få enligt 5 kap. 5 § OSL. Själva markeringen anger inte vilken folkbokföringsuppgift som kan vara känslig. Det behöver inte bara gälla adressen, utan det kan även vara ett nytt namn eller uppgifter om närstående.

Kvarskrivning är ett annat sätt att skydda personuppgifter i folkbokföringen. Genom ett beslut om kvarskrivning enligt 16 § folkbokföringslagen (1991:481) kan en person som har flyttat ändå fortsätta att vara folkbokförd på den gamla adressen i högst tre år.

Vid särskilt allvarliga hot kan en person få använda annan identitet. Den nya identiteten registreras på ett sådant sätt att det inte framgår att det rör sig om fingerade personuppgifter.

5 kap. 5 § HSLF-FS 2016:40

Vårdgivaren ska säkerställa att en patientjournal, i förekommande fall, innehåller uppgifter om

1. aktuellt hälsotillstånd och medicinska bedömningar,
2. utredande och behandlande åtgärder samt bakgrunden till dessa,
3. ordinationer och ordinationsorsak,
4. resultat av utredande och behandlande åtgärder,
5. slutanteckningar och andra sammanfattningar av genomförd vård,
6. överkänslighet för läkemedel eller vissa ämnen,
7. komplikationer av vård och behandling,
8. vårdrelaterade infektioner,
9. samtycken och återkallade samtycken,
10. patientens önskemål om vård och behandling,
11. de medicintekniska produkter som har förskrivits till, utlämnats till eller tillförts en patient på ett sådant sätt att de kan spåras,
12. intyg, remisser och annan för vården relevant inkommande och utgående information, och
13. vårdplanering.

Vårdgivaren ska vidare säkerställa att patientjournalen innehåller en markering som ger en varning om att en patient har visat intolerans eller har en överkänslighet som innebär en allvarlig risk för hans eller hennes liv eller hälsa. Markeringen ska göras på ett sådant sätt att den är lätt att uppmärksamma.

Vilka krav ställer HSLF-FS 2016:40 på patientjournalens innehåll?

I 5 kap. 5 § HSLF-FS 2016:40 anges ett flertal krav på vilka uppgifter en patientjournal, i förekommande fall, ska innehålla. I det följande finns en redogörelse för varje specifikt krav.

Aktuellt hälsotillstånd och medicinska bedömningar

Medicinska bedömningar utförs av all hälso- och sjukvårdspersonal som deltar i vården och behandlingen av en patient.

Alla utförda medicinska bedömningar ska dokumenteras. Det är till exempel lämpligt att odontologiska bedömningar av bettförhållanden och slemhinnor registreras allmänt för bettet och munhygienen, om det inte finns några särskilda förhållanden som kräver detaljerade anteckningar. Det är viktigt att registrera eventuell karies och parodontala förhållanden för varje enskild tand. Av säkerhetsskäl är det betydelsefullt att även inkludera det som endast har noterats vid undersökningen, till exempel att slemhinnan är

utan anmärkning. Det är också lämpligt att notera käksystemets funktion i stort och eventuella funktionsstörningar i käkleder och tuggmuskulatur.

Utredande och behandlande åtgärder samt bakgrunden till dessa

Av patientens journal ska det framgå vilka utredande och behandlande åtgärder som genomförts. Det kan till exempel vara en kroppslig undersökning, laboratorieprover eller röntgen. Även bakgrunden till de utredande och behandlande åtgärder som vidtagits ska antecknas i journalen.

Om uppgifterna finns tillgängliga ska patientjournalen enligt 3 kap. 6 § PDL bland annat innehålla väsentliga uppgifter om bakgrunden till vården och väsentliga uppgifter om vidtagna och planerade åtgärder.

Ordinationer och ordinationsorsak

Ordinationer av läkemedel och andra behandlingar ska dokumenteras i patientjournalen.

När det gäller ordinerade läkemedel ska läkemedelsordinationen innehålla uppgifter om läkemedlets namn, läkemedelsform, styrka, dosering, administrationssätt och tidpunkterna för administrering, vilket framgår av 3 kap. 7 § Socialstyrelsens föreskrifter och allmänna råd (SOSFS 2000:1) om läkemedelshantering i hälso- och sjukvården.

Patientjournalen ska även innehålla uppgifter om annan behandling som ordineras, till exempel sjukgymnastisk eller arbetsterapeutisk behandling.

Även orsaken till ordinationen ska dokumenteras i patientens journal (ordinationsorsak). Socialstyrelsen har tagit fram ett kodverk för att dokumentera ordinationsorsak, Nationell källa för ordinationsorsak. Mer information om detta kodverk finns på Socialstyrelsens webbplats.

Resultat av utredande och behandlande åtgärder

Det är viktigt att resultaten av utredande och behandlande åtgärder framgår av patientjournalen. Det gäller även om resultaten är utan anmärkning.

Inom tandvården är det i regel viktigt att specificera alla tänder, tandgrupper eller områden som på något sätt har behandlats genom att ange tandens eller tandgruppens beteckning respektive områdets lokalisering samt uppgift om den vidtagna åtgärden.

Slutanteckningar och andra sammanfattningar av genomförd vård

Patientjournalerna ska också innehålla slutanteckningar och andra sammanfattningar av den genomförda vården. Inom hälso- och sjukvården är epikris en vedertagen term som används synonymt för slutanteckningar och andra sammanfattningar av genomförd vård.

Inom hälso- och sjukvården och tandvården är det ofta viktigt att en slutanteckning skrivs efter exempelvis omfattande behandlingsinsatser och när en remitterad patient går tillbaka till den remitterande hälso- och sjukvårdspersonalen.

Överkänslighet för läkemedel eller vissa ämnen

Patientjournalen ska innehålla uppgifter om patienten är överkänslig för något läkemedel eller vissa ämnen. Inom tandvården ska till exempel överkänslighet mot dentala material antecknas i journalen.

Komplikationer av vård och behandling

Ordet komplikation används inom hälso- och sjukvården i allmän betydelse som något ogynnsamt som tillstöter i en behandling.

Vid utredning av en skada på en patient bör i stället någon av termerna vårdskada eller icke undvikbar skada på patient användas (se Socialstyrelsens termbank). Av 3 kap. 3 § PSL framgår att vårdgivaren ska utreda händelser i verksamheten som har medfört eller hade kunnat medföra en vårdskada. Vårdgivarens skyldighet att informera patienter om inträffade vårdskador följer av 3 kap. 8 § PSL. I samma bestämmelse anges även att uppgift om den information som har lämnats ska antecknas i patientjournalen.

Vårdrelaterade infektioner

Även uppgifter om vårdrelaterade infektioner, det vill säga infektioner som uppstått under eller i anslutning till vårdtiden, ska dokumenteras i patientjournalen. Dokumentationen är av avgörande betydelse för vårdgivarens möjligheter att kunna spåra smittans ursprung, identifiera andra som utsatts för risk att bli smittade och vidta preventiva åtgärder som kan förhindra att fler personer drabbas.

Relevanta uppgifter kan bland annat vara vilken mikrobiologisk provtagning som genomförts, var patienten varit inlagd, vilka procedurer som patienten genomgått som kan innebära smittrisk, vilken behandling patienten fått och när den satts in. Under pågående utbrott dokumenteras lämpligen de uppgifter som vårdgivaren och smittskyddsläkaren efterfrågar för att bekämpa utbrottet.

Samtycken och återkallade samtycken

Patientjournalen ska också innehålla uppgifter om lämnade samtycken. Det kan till exempel vara att patienten har samtyckt till någon vård och behandling eller lämnat sitt samtycke till behandling av personuppgifter. Även återkallade samtycken ska noteras i journalen.

Patientens önskemål om vård och behandling

Patientjournalen ska innehålla uppgifter om patientens önskemål när det gäller vård och behandling, vilket är viktigt för att tillgodose patientens trygghet i vården och för att vården ska kunna ges med respekt för patientens självbestämmande och integritet (2 a § HSL, 3 § tandvårdslagen och 4 kap. 1 § patientlagen).

De medicintekniska produkter som har förskrivits till, utlämnats till eller tillförts en patient på ett sådant sätt att de kan spåras

Patientjournalen ska innehålla uppgifter om de medicintekniska produkter (till exempel kontaktlinsprodukter, kanyler, infusionsaggregat, sängar, rullatorer och liftar) som har förskrivits till, utlämnats till eller tillförts en patient på ett sådant sätt att de kan spåras.

Av 3 kap. 6 § Socialstyrelsens föreskrifter (SOSFS 2008:1) om användning av medicintekniska produkter i hälso- och sjukvården följer bland annat att verksamhetschefen ansvarar för att de medicintekniska produkter som har förskrivits, utlämnats eller tillförts till patienter kan spåras.

Socialstyrelsen har tagit fram skriften ”Förskrivning av hjälpmedel – Stöd vid förskrivning av hjälpmedel till personer med funktionsnedsättning”. Förskrivarstödet kan laddas ner från Socialstyrelsens webbplats.

Uppgifter som kan vara relevanta för att säkerställa spårbarheten till medicintekniska produkter inom tandvården kan till exempel vara typ och fabrikat för de material som temporärt eller permanent placeras i munhålan. Om vårdgivaren har en förteckning med kodbeteckningar över de material som används, är det lämpligt att använda den aktuella koden i journalen. Det är viktigt att en sådan kodförteckning hålls aktuell.

Tandvårdsmodeller, exempelvis i gips, utgör inte journalhandlingar och hör därför inte till journalmaterialet (1 kap. 3 § PDL). Vid omfattande protetiska och/eller ortodontiska behandlingar kan dock studie- och arbetsmodellerna ha betydelse när behandlingsresultatet ska bedömas och därför är det lämpligt att modellerna sparas efter att behandlingen har avslutats. Själva modellerna kan ersättas med modellfoton. De blir i så fall en del av journalen och ska sparas i minst tio år (3 kap. 17 § PDL).

Intyg, remisser och annan för vården relevant inkommande och utgående information

Den som är skyldig att föra en patientjournal ska enligt 3 kap. 16 § PDL utfärda ett intyg om vården om patienten begär det. Den som har utfärdat intyget ska också anteckna detta i journalen och en kopia av intyget ska sparas i den.

Även uppgifter om remisser och annan för vården relevant inkommande och utgående information ska dokumenteras i patientens journal.

I 3 § Socialstyrelsens föreskrifter (SOSFS 2004:11) om ansvar för remisser för patienter inom hälso- och sjukvården, tandvården m.m. anges att vårdgivaren ska ge skriftliga direktiv och säkerställa att det finns rutiner för hur remisser ska utformas och hanteras. Verksamhetschefen ska fastställa rutiner för hantering av utgående remisser och inkommande remissvar. Dokumenterade rutiner ska finnas för bland annat vem eller vilka inom verksamheten som får utfärda remisser, hur remisserna ska registreras och sändas samt hur remissvaren ska tas emot och registreras (4-5 §§ SOSFS 2004:11).

Vårdplanering

Vårdgivaren ska vidare säkerställa att patientjournalen innehåller uppgifter om de vårdplaneringar som genomförts. Dokumentationen kan till exempel omfatta en beskrivning av vårdens planering, genomförande och resultat.

I 3 kap. Socialstyrelsens föreskrifter (SOSFS 2005:27) om samverkan vid in- och utskrivning av patienter i sluten vård finns särskilda bestämmelser om vårdplanering. I 3 kap. 6 § SOSFS 2005:27 anges att all vårdplanering enligt dessa föreskrifter ska dokumenteras i patientjournalen i den slutna vården.

Varningsmarkering

Vårdgivaren ska även säkerställa att patientjournalen innehåller en markering som ger en varning om att en patient har visat intolerans mot något eller en överkänslighet som innebär en allvarlig risk för patientens liv eller hälsa. En sådan markering ska vara lätt att uppmärksamma för alla som behöver använda uppgifterna i journalen. Det ska också framgå av markeringen vem som ansvarar för den aktuella uppgiften (5 kap. 3 § 3 HSLF-FS 2016:40). Socialstyrelsen har tagit fram ett kodverk för att dokumentera uppmärksamhetsinformation (varningsinformation och observandum). Mer information om detta kodverk finns på Socialstyrelsens webbplats.

Granskning av dokumentation

5 kap. 6 § HSLF-FS 2016:40

Vårdgivaren ska regelbundet granska att hälso- och sjukvårdspersonalen dokumenterar i patientjournalen enligt gällande författningar.

Den granskning som ska genomföras är en form av egenkontroll av den bedrivna verksamheten och kan beskrivas som en intern granskning av om hälso- och sjukvårdspersonalen dokumenterar i patientjournalen enligt gällande författningar (jämför 2 kap. 1 § och 5 kap. 2 § SOSFS 2011:9).

Bestämmelsen anger inte på vilket sätt granskningen ska genomföras. Det är således upp till vårdgivaren att mot bakgrund av den bedrivna verksamheten närmare bestämma formen för granskningen genom nödvändiga processer och rutiner i verksamhetens ledningssystem (3 kap. 1 och 2 §§ HSLF-FS 2016:40).

Granskningen ska göras regelbundet. Omständigheter som kan påverka omfattningen av granskningen och hur ofta den ska genomföras är till exempel verksamhetens inriktning och storlek, om hela eller delar av verksamheten är särskilt riskfylld, om förändringar genomförts i en verksamhet, om nya arbetssätt införts eller om nya metoder tillämpats.

Det är också upp till vårdgivaren att bestämma vem eller vilka personer som ska ansvara för granskningen. Vårdgivaren ansvarar för att den eller de personer som ansvarar för granskningen tilldelas rätt behörighet, det vill säga tillräckligt för att de ska kunna utföra sina arbetsuppgifter, men samtidigt inte mer omfattande än vad som är nödvändigt. Se vidare i avsnittet om styrning av behörigheter (s. 33).

Det är viktigt att det för såväl vårdgivaren som den personal som ska utföra granskningen är tydligt vem eller vilka som genom vårdgivarens uppdrag har fått behörighet och ansvar för de aktuella arbetsuppgifterna.

Hantering av personuppgifter

Åtgärder till skydd mot obehörig åtkomst

6 kap. 1 § HSLF-FS 2016:40

Hälso- och sjukvårdspersonalen ska ansvara för att

1. personliga lösenord och hjälpmedel för autentisering inte kan bli tillgängliga för annan, och
2. datorer eller andra enheter som används för att hantera uppgifter om patienter inte lämnas utan att uppgifterna är skyddade mot obehörig åtkomst.

6 kap. 2 § HSLF-FS 2016:40

Vårdgivaren ska säkerställa att uppdragstagare eller andra som arbetar för eller har slutit avtal med vårdgivaren förbinder sig att skydda uppgifter om patienter mot obehörig åtkomst enligt vad som anges i 1 §.

Hälso- och sjukvårdspersonalens ansvar

All hälso- och sjukvårdspersonal ska ansvara för att personliga lösenord och hjälpmedel för autentisering inte kan bli tillgängliga för någon annan. Det kan till exempel innebära att personalen inte har lösenord nedskrivna på lappar eller lånar ut lösenord och andra hjälpmedel för autentisering. Hälso- och sjukvårdspersonalen ansvarar också för att datorer eller andra enheter som används för hantering av uppgifter om patienter inte lämnas utan att uppgifter är skyddade mot obehörig åtkomst. Hälso- och sjukvårdspersonalen behöver exempelvis se till att ingen annan kan komma åt datorn när personen har loggat in i informationssystemet. Ett sätt att undvika detta kan vara att alltid låsa åtkomsten till datorn, exempelvis genom att trycka på tangenterna ”ctrl-alt-delete”, använda smartkort eller andra funktioner. Detta gäller även om datorn lämnas utan tillsyn för en kort stund. Den som arbetar hos en vårdgivare har även ett ansvar att inte ta del av uppgifter om en patient om han eller hon inte deltar i vården av patienten eller av annat skäl behöver uppgifterna för sitt arbete inom hälso- och sjukvården (4 kap. 1 § PDL).

Uppdragstagare och andra som arbetar för vårdgivaren

Vårdgivaren ansvarar för att säkerställa att uppdragstagare eller andra som arbetar för eller har slutit avtal med vårdgivaren förbinder sig att skydda uppgifter om patienter mot obehörig åtkomst enligt vad som anges i 6 kap. 1

§ HSLF-FS 2016:40. Bestämmelsen i 6 kap. 2 § HSLF-FS 2016:40 omfattar personal som inte är hälso- och sjukvårdspersonal, till exempel läkarsekreterare, annan administrativ personal och IT-personal. Vårdgivaren ska alltså säkerställa att även de förbinder sig att skydda uppgifter om patienter mot obehörig åtkomst genom att ansvara för att personliga lösenord och hjälpmedel för autentisering inte kan bli tillgängliga för annan, och att datorer eller andra enheter som används för att hantera uppgifter om patienter inte lämnas utan att uppgifterna är skyddade mot obehörig åtkomst.

Personuppgiftslagens bestämmelser om säkerheten vid behandling av personuppgifter och tillsynsmyndighetens befogenheter gäller även när personuppgifter behandlas enligt PDL. I 30–32 §§ personuppgiftslagen finns bestämmelser om säkerheten vid behandling av personuppgifter. Dessa bestämmelser gäller utöver PDL:s bestämmelser om informationssäkerhet (prop. 2007/08:126 s. 215).

Upplysning om spärrade uppgifter

6 kap. 3 § HSLF-FS 2016:40

Om en patient har motsatt sig att hans eller hennes personuppgifter görs tillgängliga för någon som arbetar vid en annan vårdenhet, i en annan vårdprocess eller för någon annan vårdgivare än den där uppgifterna har lämnats, ska det framgå av dokumentationen att det finns spärrade uppgifter.

Det ska framgå av dokumentationen att det finns spärrade uppgifter om en patient. Med andra ord ska det framgå av dokumentationen om en patient inte vill att hans eller hennes personuppgifter görs tillgängliga för en annan vårdenhet eller i en annan vårdprocess inom en vårdgivare verksamhet eller för andra vårdgivare. Det kan vara viktigt för den som ska vårda en patient att veta om det finns ytterligare uppgifter om patienten. Kännedomen om att det finns spärrade uppgifter kan initiera en önskvärd dialog mellan en patient och hälso- och sjukvårdspersonalen i en enskild vårdsituation (prop. 2007/08:126 s. 249).

Signering av journalanteckningar

6 kap. 4 § HSLF-FS 2016:40

Vårdgivaren ska säkerställa att det finns rutiner för signering av journalanteckningar och för bekräftelse av åtgärder som gäller en patients vård och behandling.

6 kap. 5 § HSLF-FS 2016:40

Vårdgivaren får besluta om undantag från kravet på signering i 3 kap. 10 § patientdatalagen (2008:355). Sådana undantag ska framgå av rutinerna för signering.

Undantag enligt första stycket får dock inte avse signering av

1. väsentliga ställningstaganden om vård och behandling,
2. förhållningsregler enligt smittskyddslagen (2004:168), eller
3. slutanteckningar eller andra sammanfattningar av genomförd vård.

Signering och bekräftelse

Vårdgivaren ska säkerställa att det finns rutiner för signering av journalanteckningar som gäller en patients vård och behandling. Den som för patientjournal ansvarar för sina uppgifter i journalen (3 kap. 4 § PDL). En journalanteckning ska signeras av den som ansvarar för uppgiften, om det inte finns något synnerligt hinder (3 kap. 10 § PDL). I kravet på signering ligger att den som signerar en anteckning bekräftar dess riktighet, det vill säga kontrollerar innehållet så att han eller hon kan gå i god för det (Socialutskottets betänkande 1984/85:SoU33 s. 9). Med synnerligt hinder menas mycket starka skäl, vilket ska föreligga i det konkreta fallet (Socialutskottets betänkande 1984/85:SoU33 s. 10).

Enligt utskottet kunde det inte accepteras ett generellt undantag för vissa typer av vård, till exempel akutsjukvård. Från säkerhetssynpunkt finns ofta skäl till noggranna journalrutiner inom exempelvis akutsjukvården, där det kan vara fråga om omfattande medicinska ingrepp med många olika personer inblandade i vården (Socialutskottets betänkande 1984/85:SoU33 s. 10). Enligt lagrådet är grunderna för ett generellt undantag av annan art än bedömningen om huruvida synnerligt hinder föreligger (prop. 2007/08:126 s. 349).

Förutom rutiner för signering ska vårdgivaren ha rutiner för bekräftelse av åtgärder som gäller en patients vård och behandling. Det kan till exempel vara att någon med sin signatur eller namnunderskrift visar att han eller hon tagit på sig ansvaret för att åtgärda en remiss eller ett provsvar som har kommit in. Det kan utgöra viktiga led i säkra rutiner för att hantera exempelvis olika utlåtanden, svar och beställningar.

Bakgrund till signeringskravet

Kravet på signering infördes av patientsäkerhetsskäl i patientjournallagen, den lag som gällde innan PDL trädde i kraft 2008. Enligt förarbetena till PDL gör sig de patientsäkerhetsskäl som anfördes vid införandet av signeringskravet fortfarande gällande. Det gäller än mer vid anteckningar i stora eller kompatibla journalsystem där anteckningarna kan komma att läggas till grund för behandlingsåtgärder och medicinering av andra vårdenheter än den där anteckningarna gjorts. I sådana fall är det av särskild vikt att uppgifterna har kontrollästs så att risken för missförstånd och felskrivningar kan minimeras (prop. 2007/08:126 s. 94).

Journalanteckningar som ska signeras och undantag för signering

Vårdgivaren får besluta om undantag från kravet på signering i 3 kap. 10 § PDL. Sådana undantag ska framgå av rutinerna för signering. Det får dock inte göras undantag för signering av väsentliga ställningstaganden om vård och behandling, förhållningsregler enligt smittskyddslagen (2004:168) samt slutanteckningar eller andra sammanfattningar av genomförd vård. Vårdgivarens rutiner för signering ska säkerställa att dessa anteckningar alltid signeras. Exempel på väsentliga ställningstaganden kan vara uppgifter om en diagnos som ställts efter en utredning, vidtagna och planerade åtgärder, vårdplanering, remiss för utredning och undersökning samt ordination av läkemedel. Andra sammanfattningar av genomförd vård kan till exempel gälla operationsberättelser eller en sjuksköterskas sammanställningar av iordningställande och administrering av läkemedel.

Enligt förarbetena till PDL kan det finnas skäl att göra undantag från signeringskravet när nyttan av signeringen vägs mot det merarbete som signeringskravet skulle innebära (prop. 2007/08:126 s. 94 och 235). Vid bedömningen när undantag kan medges bör risker för patientsäkerheten eller andra viktiga faktorer som talar för signering övervägas (prop. 2007/08:126 s. 94). I 6 kap. 5 § HSLF-FS 2016:40 föreskrivs vilka journalanteckningar som alltid ska signeras. Vilka slags uppgifter som kan undantas från signering får varje vårdgivare själv bedöma och anpassa utifrån ett patientsäkerhetsperspektiv. Det är också vårdgivaren som får bedöma om även andra anteckningar ska signeras utöver dem som anges som obligatoriska i Socialstyrelsens föreskrifter. Exempel på sådant som inte behöver signeras kan vara anteckningar som endast innehåller administrativa uppgifter som att kopior av journaluppgifter skickats till Försäkringskassan, försäkringsbolag eller dylikt. Ett annat exempel kan vara att patienten avbokat eller inte infunnit sig till ett planerat besök. Rutinmässiga provtagningar som till exempel Hb, kroppstemperatur och liknande kan vara andra exempel på sådant som skulle kunna undantas. Daganteckningar som inte innefattar några väsentliga ställningstaganden om vård och behandling kan också vara exempel på sådana anteckningar som kan undantas i vårdgivarens rutiner för signering.

Löpande anteckningar i patientjournalen blir allmän handling

Högsta förvaltningsdomstolen har i HFD 2013 ref. 33 prövat frågan om osignerade journalanteckningar i en patientjournal inom den offentligt bedrivna hälso- och sjukvården utgör en del av en allmän handling. Enligt Högsta förvaltningsdomstolen kan signeringen av en journalanteckning inte tillmätas någon betydelse för bedömningen av när anteckningen ska anses utgöra en del av den allmänna handlingen i tryckfrihetsförordningens mening. Högsta förvaltningsdomstolen lyfte fram att det signeringskrav som införts i journallagstiftningen inte heller är avsett att ha någon sådan funktion, utan motiveras av patientsäkerhetsskäl (proposition 1984/85:189 om patientjournallag m.m. s. 19-20 och Socialutskottets betänkande 1984/85:SoU33 s. 7-10). Journalanteckningen blir omedelbart att anse som allmän när den skrivs in i patientjournalen. Korrigering av eventuella skrivfel i direkt anslutning till införandet bör fritt kunna ske (prop. 1984/85:189 s. 44) men om journalanteckningen ändras vid en senare tidpunkt, exempelvis i samband med signering, blir båda versionerna av anteckningen att anse som en allmän handling.

Skydd av journalanteckningar

6 kap. 6 § HSLF-FS 2016:40

Vårdgivaren ska säkerställa att uppgifter i en patientjournal inte kan ändras eller utplånas annat än med stöd av patientdatalagen (2008:355).

Ändra eller utplåna uppgifter i en patientjournal

Vårdgivaren ska säkerställa att uppgifter i en patientjournal inte kan ändras eller utplånas på annat sätt än vad som är tillåtet enligt PDL. I 8 kap. 3 § PDL finns bestämmelser om att en personuppgiftsansvarig på begäran av en registrerad ska rätta personuppgifter som inte har behandlats i enlighet med PDL. Enligt 3 kap. 14 § PDL får dock uppgifter i en journalhandling inte utplånas eller göras oläsliga i andra fall än som avses i 8 kap. 4 § samma lag (se avsnittet nedan om förstörande av en patientjournal).

Vid rättelse av en felaktighet ska det anges när rättelsen har skett och vem som har gjort den. Av förarbetena till PDL framgår att det innebär bland annat att en rättelse i en journalhandling alltid måste göras så att den ursprungliga texten klart framgår också efter rättelsen. Det är inte tillåtet att utplåna den ursprungliga texten (prop. 2007/08:126 s. 96). Det är ur patientsäkerhetssynpunkt mycket viktigt att uppgifter i journalhandlingar är riktiga (prop. 2007/08:126 s. 96).

Förstörande av en patientjournal

Inspektionen för vård och omsorg får besluta om att en patientjournal helt eller delvis ska förstöras (8 kap. 4 § PDL). Detta kan ske efter en ansökan från patienten eller någon annan person som omnämns i journalen. Förutsättningarna för detta är att godtagbara skäl anförs för ansökan och att patientjournalen eller den del av den som ansökan avser, uppenbarligen inte behövs för patientens vård. Det krävs också att det från allmän synpunkt uppenbarligen inte finns skäl att bevara journalen. Enligt förarbetena till den tidigare gällande patientjournallagen innebär kravet på godtagbara skäl att en patient inte utan vidare kan få sin journal eller en del av den förstörd (prop. 1984/85:189 s. 50). Det krävs att anteckningarna rimligen kan medföra en psykisk belastning eller liknande för patienten om de bevaras. Genom inskränkningen att det från allmän synpunkt uppenbarligen inte finns skäl att bevara journalen ges enligt förarbetena en möjlighet att beakta olika samhällsintressen som avser journalmaterialet som till exempel insynen, forskningen och ekonomin i vården (prop. 2007/08:126 s. 100). Om journalhandlingarna exempelvis legat till grund för ett beslut hos en myndighet eller är bevis i en rättslig process kan de oftast inte heller förstöras av allmänna skäl.

Innan ansökan slutligt prövas får den som ansvarar för en journalhandling som omfattas av ansökan ges tillfälle att yttra sig. Ett avslag kan överklagas till förvaltningsrätten, medan ett bifall inte kan överklagas.

Uppgifter om en patient som förts in i fel patientjournal

I en ansökan om journalförstöring till Inspektionen för vård och omsorg (IVO) angavs att en patients (P1) journal felaktigt skannats in i en annan patients (P2) journal. IVO avvisade ansökan och motiverade i sitt principiella beslut att de främmande uppgifterna i patientjournalen som rör en annan person aldrig blir en del av P2:s journal, eftersom en patientjournal inte kan vara gemensam för flera patienter. När en vårdgivare har fört in uppgifter om en patient i en annan patients journal ska detta således inte tas om hand inom ramen för journalförstöringsinstitutet, utan åtgärdas inom ramen för respektive vårdgivares systematiska kvalitetsarbete (se Socialstyrelsens föreskrifter [SOSFS 2011:9] om ledningssystem för systematiskt kvalitetsarbete). Det innebär att de felaktigt införda uppgifterna inte ska raderas, utan flyttas till den patientjournal där de rätteligen hör hemma. Därmed ska alltså inte de felaktiga uppgifterna vara kvar i P2:s journal. Det principiella beslutet finns på IVO:s webbplats.

I ett annat ärende, som också gällde en ansökan om journalförstöring, konstaterade kammarrätten i Stockholm att det var korrekt av IVO att avvisa en patients ansökan om journalförstöring (dom den 9 november 2016, mål nr. 7703-15). Av domstolens bedömning framgår att bestämmelserna i PDL innebär att en patientjournal inte kan vara gemensam för flera patienter. Mot bakgrund av att en patient bara kan ha en journal, ansåg kammarrätten att bestämmelsen i 8 kap. 4 § PDL måste förstås som att IVO:s behörighet att besluta om förstöring av en patientjournal är begränsad till de delar av

journalen som rör patienten själv. Patienten kan dock begära att vårdgivaren "lyfter ur" de uppgifter som inte rör patienten ur dennes patientjournal.

Förvaring av patientjournalen

6 kap. 7 § HSLF-FS 2016:40

Vårdgivaren ska säkerställa att uppgifter i patientjournalen förvaras på ett sådant sätt att de är läsbara fram till dess att de gallras.

Bevarande av journalhandlingar

Enligt 3 kap. 17 § PDL ska en journalhandling sparas i minst tio år efter det att den sista uppgiften fördes in i handlingen. För den offentliga hälso- och sjukvården och tandvården gäller bestämmelserna i arkivlagen (1990:782) om att bevara och gallra allmänna handlingar (3 kap. 18 § PDL).

Samrådsgruppen för kommunala arkivfrågor är en samverkansgrupp mellan Riksarkivet och Sveriges Kommuner och Landsting (SKL). Samrådsgruppen verkar för utveckling av arkivområdet och utarbetar bland annat råd om bevarande och gallring inom en rad kommunala områden, till exempel när det gäller landstingens, regionernas och kommunernas patientjournaler och övrig medicinsk dokumentation. Skriften ”Bevara eller gallra. Nr 6: Patientjournaler och övrig vårddokumentation” ger råd om bevarande- och gallringsfrågor inom hälso- och sjukvård i kommuner, landsting/regioner för bland annat patientjournaler, läkemedelshantering, mödravård och medicinsk service. Skriften finns att ladda ner och beställa från SKL:s webbplats.

Av 1 kap. 2 § PDL framgår att dokumenterade personuppgifter ska hanteras och förvaras så att obehöriga inte får tillgång till dem. Det kan till exempel innebära att journalhandlingar är inlåsta när de inte används och när de används är under betryggande övervakning.

Olika medier för lagring är olika känsliga för åldrande. Ett medium, exempelvis en CD-skiva eller ett band, som används för elektronisk lagring av information kan av olika orsaker bli oläsbart över tiden. Det kan exempelvis bero på hur mediet förvaras och på förändringar i fukt och temperatur i mediets närmiljö. Det skulle därför kunna analyseras vilka krav som ställs på lagringen utifrån val av medium och över tiden testa att mediet fortfarande går att läsa. Ett elektroniskt medium är även beroende av en tillhörande uppspelningsteknik för att läsa tillbaka uppgifterna. Då den tekniska utvecklingen går snabbt och gamla tekniker byts ut kan det finnas anledning att bevara den teknik som krävs för att läsa tillbaka uppgifter som finns lagrade på ett visst medium.

Journalhandlingar på andra språk än svenska

6 kap. 8 § HSLF-FS 2016:40

Följande yrkesutövare får föra patientjournal på ett annat språk än svenska.

1. Den yrkesutövare som har fått ett behörighetsbevis för ett yrke i hälso- och sjukvården eller tandvården eller i detaljhandel med läkemedel enligt bestämmelserna om erkännande av utländsk utbildning i 6 kap. 1 § patientsäkerhetsförordningen (2010:1369) får föra patientjournal på danska eller norska.
2. Den yrkesutövare som i kraft av utomnordisk utbildning har fått ett förordnande av Socialstyrelsen att utöva yrke i hälso- och sjukvården får föra patientjournal på engelska, om det anges i förordnandet.

6 kap. 9 § HSLF-FS 2016:40

Om vårdgivaren anlitar hälso- och sjukvårdspersonal som enligt 8 § får föra patientjournal på något annat språk än svenska, ska denne säkerställa att

1. kravet på noggrannhet i dokumentationen upprätthålls, och
2. väsentliga ställningstaganden som gäller vård och behandling, förhållningsregler enligt smittskyddslagen (2004:168) samt slutanteckningar eller andra sammanfattningar av genomförd vård finns upprättade på svenska.

Språket i patientjournalen

I 6 kap. 8 § HSLF-FS 2016:40 föreskrivs de undantag som gäller från huvudregeln att föra patientjournal på svenska. I 3 kap. 13 § PDL anges att de journalhandlingar som upprättas inom hälso- och sjukvården ska vara skrivna på svenska språket, vara tydligt utformade och så lätta som möjligt att förstå för patienten.

Enligt huvudregeln ska alltså patientjournalen vara skriven på svenska. I hälso- och sjukvården används i stor utsträckning ett fackspråk som kan vara svårt att förstå för patienten. Journalerna utgör i första hand arbetsdokument i vårdarbetet och det borde därför kunna accepteras en språklig utformning med viss inblandning av fackuttryck (prop. 1984/85:189 s. 21). Det är viktigt att använda en lättförståelig svenska och allmänt vedertagna förkortningar, både med hänsyn till patienten och till den övriga personalen som kan behöva använda journalen (prop. 1984/85:189 s. 42). Kravet på att journalhandlingar ska vara skrivna på svenska innebär dock inte att varje ord eller

term i handlingen måste vara på svenska. Möjligheterna att i alla lägen använda svenska ord och uttryckssätt begränsas i viss mån av att det svenska språket saknar exakta synonymer till olika vedertagna fackuttryck på främmande språk. Termer av latinsk eller annan utländsk härstamning måste därför godtas när adekvata motsvarigheter inte finns i det svenska språket (prop. 1984/85:189 s. 42). Om däremot svenska motsvarigheter finns, får inte de utländska orden eller uttryckssätten väljas (prop. 1984/85:189 s. 42). Av förarbetena till PDL framgår att bestämmelsen ansågs viktig dels från patientsäkerhetssynpunkt, bland annat med hänsyn till strävan efter enhetlighet i journalföringen. Det blir än viktigare i omfattande journalsystem eftersom journalanteckningarna då kan komma att läsas och förstås av fler personer inom hälso- och sjukvården. Risken för att tidigare journalanteckningar missförstås vid en senare vårdkontakt kan komma att öka om anteckningarna förts på annat språk än svenska. Dessutom kan det antas att möjligheterna till uppföljning skulle försämras (prop. 2007/08:126 s. 94-95).

Vårdgivarens ansvar

Om vårdgivaren anlitar hälso- och sjukvårdspersonal som får föra patientjournal på något annat språk än svenska enligt 6 kap. 8 § HSLF-FS 2016:40, ska vårdgivaren säkerställa att kravet på noggrannhet i dokumentationen upprätthålls (6 kap. 9 § HSLF-FS 2016:40). Vårdgivaren ska också säkerställa att väsentliga ställningstaganden om vård och behandling, förhållningsregler enligt smittskyddslagen eller andra sammanfattningar av genomförd vård finns upprättade på svenska.

Översättning och tolkning

6 kap. 10 § HSLF-FS 2016:40

Vårdgivaren ska säkerställa att en patient kan ta del av sin patientjournal på ett sådant sätt att han eller hon kan förstå innehållet.

Förstå innehållet i patientjournalen

Ur patientsäkerhetssynpunkt är det viktigt att patienten är delaktig i och förstår innebörden av sin vård och behandling, liksom de ordinationer och instruktioner som han eller hon får. En patient som inte behärskar det svenska språket och som vill ta del av sin journal kan behöva få innehållet översatt, till exempel med hjälp av en tolk eller genom en skriftlig översättning. En patient som på grund av någon funktionsnedsättning inte kan ta del av och förstå det skriftliga innehållet kan också behöva få hjälp med att ta del av sin patientjournal på ett sådant sätt att han eller hon kan förstå innehållet.

Det övergripande målet för hälso- och sjukvården och tandvården är en god hälsa och vård på lika villkor för hela befolkningen (2 § HSL, 2 § tandvårdslagen och 1 kap. 6 § patientlagen).

Vården ska så långt som möjligt utformas och genomföras i samråd med patienten (5 kap. 1 § patientlagen, 3 a § tandvårdslagen och 6 kap. 1 § PSL). I 8 § förvaltningslagen (1986:223), som är aktuell för hälso- och sjukvården vid handläggning av förvaltningsärenden som till exempel beslut om tvångsvård, stadgas att när en myndighet har att göra med någon som inte behärskar svenska eller som är allvarligt hörsel- eller talskadad, bör myndigheten anlita tolk.

Information till patienten

Patienten ska få information om bland annat sitt hälsotillstånd och de metoder som finns för undersökning, vård och behandling (3 kap. 1 § 1-2 patientlagen). Informationen ska anpassas till mottagarens ålder, mognad, erfarenhet, språkliga bakgrund och andra individuella förutsättningar. Mottagarens önskan om att avstå från information ska respekteras (3 kap. 6 § patientlagen).

Det är av central betydelse att informationen lämnas i former som stärker patientens delaktighet och självbestämmande. Den som lämnar informationen måste hjälpa mottagaren att värdera informationen, ge aktiv vägledning och försäkra sig om att patienten har ett tillräckligt underlag för att kunna utöva delaktighet och självbestämmande. I det ingår att så långt som möjligt försäkra sig om att mottagaren har förstått innehållet i och betydelsen av den lämnade informationen (prop. 2013/14:106 s. 53).

Informationen ska bland annat anpassas efter mottagarens språkliga bakgrund (3 kap. 6 § patientlagen). Patienter som inte förstår eller talar svenska fullt ut har rätt till samma goda information som andra patienter. Hälso- och sjukvårdens verksamheter bör vid behov anlita tolk och har ett ansvar för att utforma sin information så att den blir tillgänglig för alla (prop. 2013/14:106 s. 118). Informationen ska även anpassas efter mottagarens andra individuella förutsättningar såsom utbildningsbakgrund, könsidentitet, religion, kognitiva och andra funktionsnedsättningar, livssituation eller andra omständigheter som kan påverka hur informationen bör ges (prop. 2013/14:106 s. 118).

Av 3 kap. 7 § patientlagen framgår att den som ger informationen så långt som möjligt ska försäkra sig om att mottagaren har förstått innehållet i och betydelsen av den lämnade informationen. Informationen ska lämnas skriftligen om det behövs med hänsyn till mottagarens individuella förutsättningar eller om han eller hon ber om det. Att ge patienten ett utdrag ur journalen kan vara ett sätt att lämna skriftlig information, där till exempel ordinationer och andra instruktioner kan utläsas. Detta kan vara viktigt även om patienten kan få tillgång till hela sin journal via Internet (prop. 2013/14:106 s. 53-54).

Patientsäkerhetsberättelse

7 kap. 1 § HSLF-FS 2016:40

Patientsäkerhetsberättelsen ska, utöver vad som anges i 3 kap. 10 § patientsäkerhetslagen (2010:659), innehålla uppgifter om

1. de uppföljningar av informationssäkerheten som framgår av 3 kap. 6 § 3 och som är av större betydelse,
2. de riskanalyser som har gjorts enligt bestämmelserna i 3 kap. 5 §,
3. de åtgärder som har vidtagits för förbättring av informationssäkerheten enligt vad som framgår av 3 kap. 6 § 4 och som är av större betydelse,
4. den utvärdering vårdgivaren har genomfört enligt 3 kap. 18 § av skydd mot olovlig åtkomst till datornätverk och informationssystem, och
5. den granskning som har gjorts enligt 5 kap. 6 §* av hälso- och sjukvårdspersonalens journalföring.

* I 7 kap. 1 § 5 HSLF-FS 2016:40 anges en felaktig hänvisning till 5 kap. 7 §. Den 1 april 2017 träder en ändring i kraft som innebär att hänvisningen ändras till 5 kap. 6 §.

7 kap. 2 § HSLF-FS 2016:40

Ytterligare bestämmelser om innehållet i en patientsäkerhetsberättelse finns i 7 kap. 2 och 3 §§ Socialstyrelsens föreskrifter och allmänna råd (SOSFS 2011:9) om ledningssystem för systematiskt kvalitetsarbete.

Patientsäkerhetsberättelsens innehåll

Vårdgivaren ska senast den 1 mars varje år upprätta en patientsäkerhetsberättelse av vilken det ska framgå hur patientsäkerhetsarbetet har bedrivits under föregående kalenderår, vilka åtgärder som har vidtagits för att öka patientsäkerheten och vilka resultat som har uppnåtts (3 kap. 10 § PSL).

I 7 kap. 1 § HSLF-FS 2016:40 ställs ytterligare krav på vilka uppgifter som patientsäkerhetsberättelsen ska innehålla. Patientsäkerhetsberättelsen ska innehålla uppgifter om uppföljningar av informationssäkerheten som har gjorts och som är av större betydelse. Den ska även innehålla uppgifter om de riskanalyser som har gjorts, samt förbättringsåtgärder av informationssäkerheten som har vidtagits och som är av större betydelse. Patientsäkerhetsberättelsen ska också innehålla uppgift om vårdgivarens utvärdering av skydd mot olovlig åtkomst till datornätverk och informationssystem. Vidare ska patientsäkerhetsberättelsen innehålla uppgifter om granskningen som gjorts av att hälso- och sjukvårdspersonalen dokumenterar i patientjournalen enligt gällande författningar.

Patientsäkerhetsberättelsen ska även innehålla de uppgifter som anges i 7 kap. 2 och 3 §§ Socialstyrelsens föreskrifter och allmänna råd (SOSFS 2011:9) om ledningssystem för systematiskt kvalitetsarbete. Bestämmelserna i SOSFS 2011:9 beskrivs i Socialstyrelsens handbok ”Ledningssystem för systematiskt kvalitetsarbete - Handbok för tillämpningen av föreskrifter och allmänna råd (SOSFS 2011:9) om ledningssystem för systematiskt kvalitetsarbete”. Handboken kan laddas ner från Socialstyrelsens webbplats.

Omhändertagande av patientjournal

8 kap. 1 § HSLF-FS 2016:40

Om en enskild verksamhet i hälso- och sjukvården inte ska drivas vidare, ska

1. vårdgivaren,
2. dödsboet,
3. konkursboet, eller
4. likvidatorn

säkerställa att de patientjournaler som finns i verksamheten tas om hand på ett sådant sätt att obehöriga inte kan ta del av dem.

Om patientjournalerna inte kan tas om hand i enlighet med vad som framgår av första stycket, ska den som ansvarar för dem ansöka hos Inspektionen för vård och omsorg om omhändertagande av journalerna enligt bestämmelserna i 9 kap. 1 § andra stycket patientdatalagen (2008:355).

I 8 kap. 1 § HSLF-FS 2016:40 regleras omhändertagande av patientjournaler när en enskild verksamhet i hälso- och sjukvården inte ska drivas vidare. Bestämmelsen gäller privata vårdgivare (i företagsform) och privatpraktiserande enskilda läkare, tandläkare, psykologer, sjukgymnaster, sjuksköterskor med flera som, i egenskap av ägare, ansvarar för att förvara och arkivera patientjournaler.

Ansvar när en enskild verksamhet inte ska drivas vidare

Om en enskild verksamhet inom hälso- och sjukvården inte ska drivas vidare ska vårdgivaren se till att verksamhetens patientjournaler tas om hand på ett sådant sätt att obehöriga inte kan få del av uppgifter om patienterna. Det innebär bland annat att vårdgivaren behöver beakta de regler som gäller för att bevara journalhandlingar (se bland annat 1 kap. 2 § och 3 kap. 17 § PDL).

Om den som bedrivit verksamheten har avlidit ansvarar dödsboet för att vidta nödvändiga åtgärder för att säkerställa att verksamhetens patientjournaler tas om hand på ett sådant sätt att obehöriga inte kan ta del av dem. Om vårdgivaren har gått i konkurs bär konkursboet ansvaret. Om ett aktiebolag ska avvecklas genom likvidation ansvarar likvidatorn på motsvarande sätt.

Ansökan om omhändertagande av journalerna

Om patientjournalerna inte kan tas om hand enligt vad som framgår ovan, ska den som ansvarar för dem ansöka hos Inspektionen för vård och omsorg (IVO) om omhändertagande av journalerna enligt 9 kap. 1 § PDL.

Om det på sannolika skäl kan antas att patientjournaler inom enskild hälso- och sjukvård inte kommer att handhas enligt PDL eller föreskrifter som har meddelats i anslutning till lagen, får IVO besluta att patientjournalerna ska tas om hand (9 kap. 1 § första stycket PDL). IVO 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 (9 kap. 1 § andra stycket PDL).

Det finns också andra tillfällen när IVO kan besluta om att omhänderta ett journalarkiv, till exempel om yrkesutövaren blir sjuk, avlider, går i konkurs, flyttar utomlands, förlorar sin legitimation eller verksamheten läggs ned av andra skäl. I de fallen är det arkivmyndigheten i det aktuella landstinget som tar hand om patientjournalerna, alternativt arkivmyndigheten i den aktuella kommunen om kommunen inte tillhör något landsting (9 kap. 3 § PDL).