Gemensamma författningssamlingen avseende hälso- och sjukvård, socialtjänst, läkemedel, folkhälsa m.m.

ISSN 2002-1054, Artikelnummer 2016-4-44
Utgivare: Rättschef Pär Ödman, Socialstyrelsen

Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården;

HSLF-FS 2016:40

Utkom från trycket den 27 maj 2016

beslutade den 25 april 2016.

Socialstyrelsen föreskriver följande med stöd av 7 kap. 4 § och 8 kap. 5 § första stycket 1 och 3 patientsäkerhetsförordningen (2010:1369), 2 och 3 §§ patientdataförordningen (2008:360), 13 § andra stycket tandvårdsförordningen (1998:1338) samt 2 § 1 och 4, 3 § 1 och 4 § 5 förordningen (1985:796) med vissa bemyndiganden för Socialstyrelsen att meddela föreskrifter m.m. och beslutar följande allmänna råd.

Föreskrifterna i 3 kap. 2–20 §§, 4 kap. 2–12 §§ samt 6 kap. 2 och 6 §§ är utarbetade efter samråd med Datainspektionen.

1 kap. Tillämpningsområde

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

2 § 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.

Förhållandet till personuppgiftslagen

3 § 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.

2 kap. Definitioner

1 § 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

3 kap. Ledningssystem

1 § 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.

2 § 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.

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

Informationssäkerhetspolicy

4 § 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 personuppgifters tillgänglighet, riktighet, konfidentialitet och spårbarhet.

Riskanalyser

5 § 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.

Ledning och samordning av informationssäkerhetsarbetet

6 § 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.

Ta i drift informationssystem

7 § 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.

Driftdokumentation

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

Upphandling och utveckling

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

10 § 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.

Planering av verksamhet vid funktionsstörning

11 § 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.

Säkerhetskopiering

12 § 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.

13 § 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.

Fysiskt skydd av informationssystem

14 § 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.

Behandling av personuppgifter i öppna nät

15 § 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.

16 § 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.

17 § 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.

Utvärdering av skyddet mot olovlig åtkomst

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

Flyttbart medium för informationslagring

19 § 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.

Avveckling av medium för informationslagring

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

4 kap. Åtkomst till uppgifter om patienter

Styrning av behörigheter

1 § 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).

2 § 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.

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

Åtkomst till uppgifter inom en vårdgivares verksamhet

4 § 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.

5 § 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.

Åtkomst till ospärrade uppgifter om en patient vid sammanhållen journalföring

6 § 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 uppgift om spärrade uppgifter vid sammanhållen journalföring

7 § 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.

Nödöppning vid sammanhållen journalföring

8 § 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.

Kontroll av åtkomst till uppgifter

9 § 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.

10 § 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.

Direktåtkomst till uppgifter om den enskilde själv

11 § 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.

12 § 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.

5 kap. Patientjournalens struktur och innehåll

Patientjournalens struktur

1 § 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.

Patientjournalens innehåll

2 § 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).

3 § 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.

4 § 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.

5 § 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.

Granskning av dokumentation

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

6 kap. Hantering av personuppgifter

Åtgärder till skydd mot obehörig åtkomst

1 § 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.

2 § 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 §.

Upplysning om spärrade uppgifter

3 § 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.

Signering av journalanteckningar

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

5 § 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.

Skydd av journalanteckningar

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

Förvaring av patientjournalen

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

Journalhandlingar på andra språk än svenska

8 § 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.

9 § 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.

Översättning och tolkning

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

7 kap. Patientsäkerhetsberättelse

1 § 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. 7 § av hälso- och sjukvårdspersonalens journalföring.

2 § 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.

8 kap. Omhändertagande av patientjournal

1 § 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).

9 kap. Undantagsbestämmelse

1 § Socialstyrelsen kan medge undantag från bestämmelserna i dessa föreskrifter, om det finns särskilda skäl.

---

1. Denna författning träder i kraft den 1 mars 2017.
2. Genom författningen upphävs Socialstyrelsens föreskrifter (SOSFS 2008:14) om informationshantering och journalföring i hälso- och sjukvården.

Styrelsen för Socialstyrelsen

(Avdelningen för regler och behörighet)[1]

1 (Föredragande: Jonas Widell)

HSLF-FS
2016:40

HSLF-FS kan laddas ned eller beställas via
Socialstyrelsens publikationsservice
webb: www.socialstyrelsen.se/publikationer
e-post: publikationsservice@socialstyrelsen.se

Edita Bobergs AB, Falun, 2016