



## Personliga inloggningar

Alla har ett personligt ansvar för att värna om informationssäkerheten och den inre sekretessen. De som arbetar för en vårdgivare ansvarar även för att skydda sitt personliga lösenord och andra hjälpmedel för kontroll av behörighet.

För att uppnå tillräcklig kontroll av att användarna utnyttjar sin behörighet på rätt sätt är det nödvändigt att aktiviteter i systemen kan härledas till enskilda individer.

Därför ställer föreskrifterna krav på personliga inloggningar som kan hänföras till enskilda användare. Det innebär att endast personliga inloggningar är tillåtna och att så kallade grupp-konton inte får förekomma.



## Patientens direktåtkomst

Med den nya lagen öppnas möjligheter för vårdgivaren att erbjuda patienten direktåtkomst till sina journaler.

Direktåtkomst sker genom kommunikation över Internet och därför ställs höga krav på säkerhet. Patienten måste identifiera sig genom stark autentisering för att få tillgång till uppgifterna.

Direktåtkomsten kan bara omfatta sådana patientuppgifter som får lämnas ut till patienten själv. Detta innebär att sekretessprövning är nödvändig i samband med att patientuppgifter görs tekniskt tillgängliga för patienten. Vårdgivaren måste därför ha ett system för att spärra uppgifter som inte kan lämnas ut till en patient för att de är sekretessbelagda eller omfattas av tystnadsplikten.

Om patienten inte får se alla uppgifter ska det finnas tydlig information om att inte alla patientuppgifter är tillgängliga. Patienten måste också få information om vart han eller hon ska vända sig för att få hjälp med att förstå dokumentationen.

Patientdatalagen  
Informationshantering och journalföring  
– informationssäkerhet för god vård  
(art.nr. 2008-126-24) kan beställas från

Socialstyrelsens beställningsservice  
120 88 Stockholm

Fax: 08-779 96 67  
e-post: [socialstyrelsen@strd.se](mailto:socialstyrelsen@strd.se)

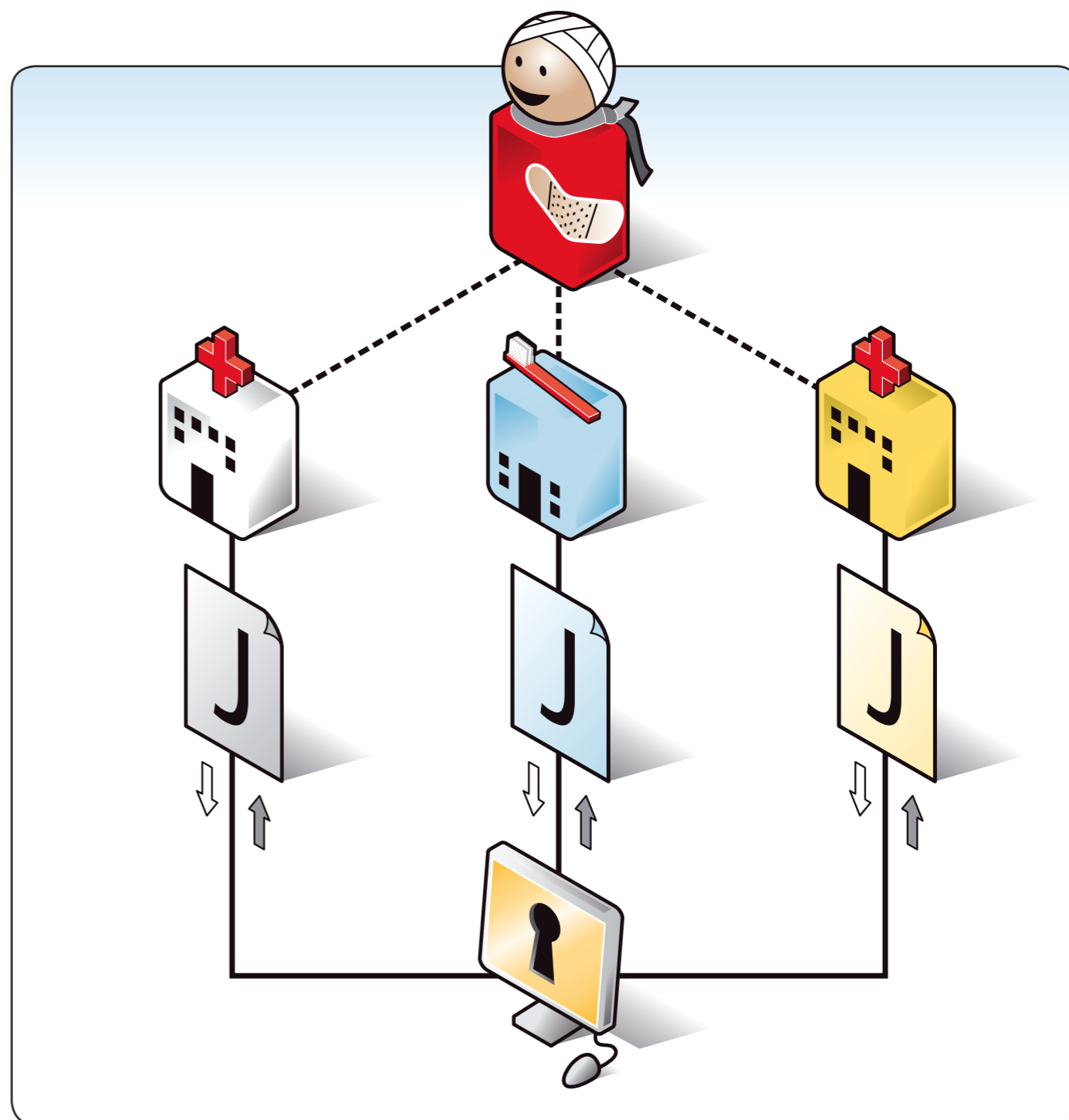
Foldern kan också laddas ner från Socialstyrelsens  
webbplats [www.socialstyrelsen.se](http://www.socialstyrelsen.se)

För mer information

[www.socialstyrelsen.se/patientjournal](http://www.socialstyrelsen.se/patientjournal)

# Informationshantering och journalföring

– informationssäkerhet för god vård



# Informationshantering och journalföring

## – informationssäkerhet för god vård

Från och med den 1 juli 2008 gäller den nya patientdatalagen. Syftet med lagen är att informationshanteringen inom hälso- och sjukvården ska vara organiserad så att den tillgodoser patientsäkerheten och god kvalitet samtidigt som den främjar kostnadseffektivitet.

Med nya tekniska lösningar kan journaler enkelt skickas mellan olika vårdenheter och vårdgivare. Förutsättningarna för en god och säker vård blir bättre om patientuppgifterna finns tillgängliga där de behövs. Men det ställer krav på att reglerna som säkrar patientens integritet blir tydligare.

Patientuppgifterna ska utformas och behandlas så att patientens integritet och trygghet stärks. Patienten får rätt att begära information om vilken åtkomst som förekommit till hans eller hennes patientuppgifter och kan bestämma över vilka vårdenheter som får ta del av uppgifterna. Om en patient har spärrat uppgifter ska det synas att uppgiften är spärrad och vilken vårdenhet som spärrat den. Dokumenterade personuppgifter ska hanteras och förvaras så att obehöriga inte får tillgång till dem.



### Ny föreskrift

Socialstyrelsen har utarbetat föreskrifter till patientdatalagen. Föreskrifterna (SOSFS 2008:14) om informationshantering och journalföring i hälso- och sjukvården kompletterar föreskrifterna (SOSFS 2005:12) om ledningssystem för kvalitet och patientsäkerhet i hälso- och sjukvården och föreskrifterna (SOSFS 2008:1) om användning av medicintekniska produkter i hälso- och sjukvården. De nya föreskrifterna innehåller bland annat:

- krav på informationssäkerhetspolicy
- regler om tilldelning av behörighet till åtkomst
- regler om kontroll av åtkomst till patientuppgifter
- regler om säkerhetskrav vid direktåtkomst för den enskilde
- regler om innehåll, utformning och hantering av journalhandlingar

Patientdatalagen ersätter patientjournalagen och vårdregisterlagen, den medför ändringar i sekretesslagen och ställer ökade krav på rutiner kring säkerhet och åtkomst.



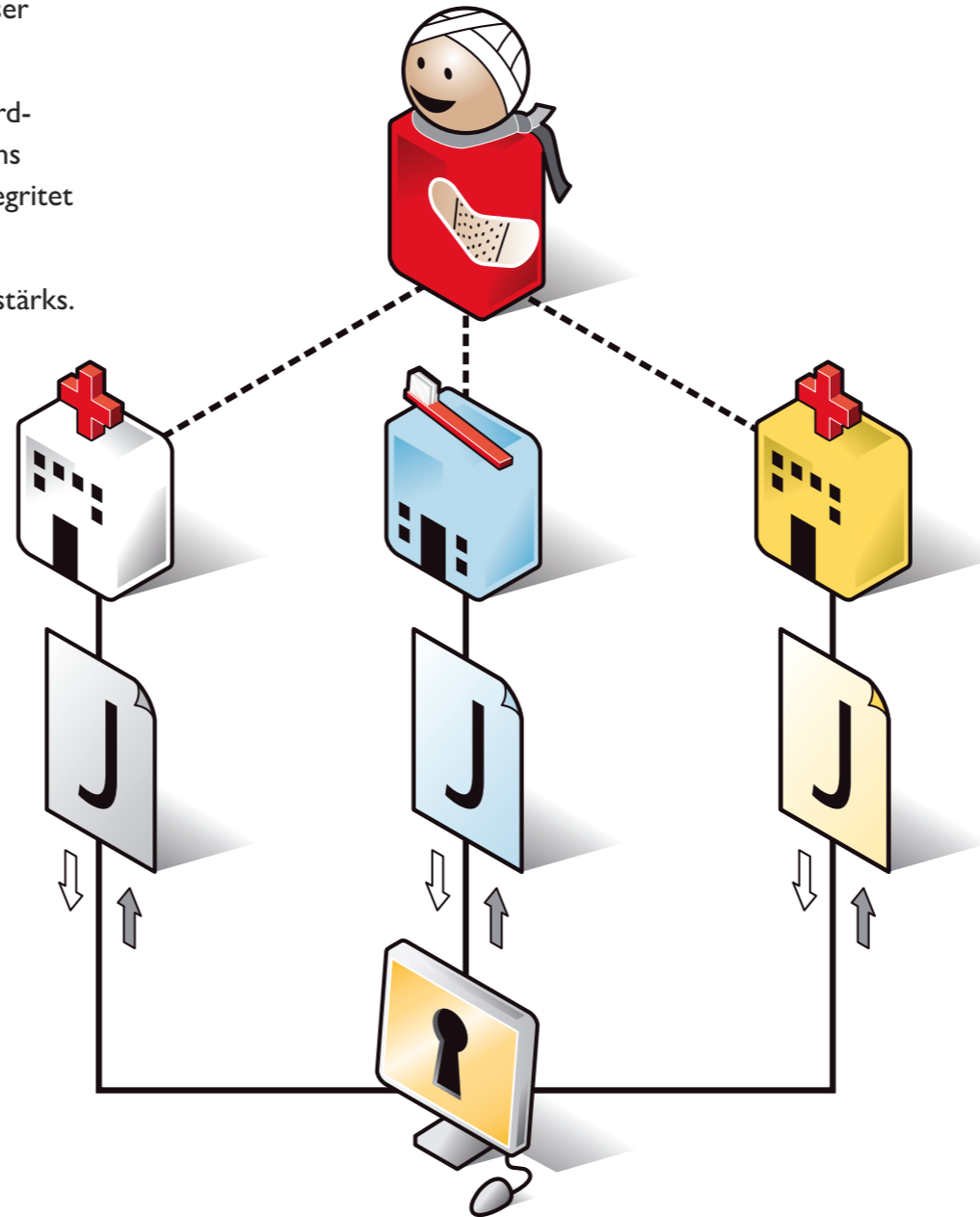
### Informationssäkerhet i vården efter 1 juli 2008

Alla vårdgivare ska utarbeta en informations-säkerhetspolicy som säkerställer att

- patientuppgifter i vårdgivarens dokumentation är åtkomliga och användbara för den som är behörig (tillgänglighet)
- patientuppgifterna är oförvanskade (riktighet)

- obehöriga inte kan ta del av patientuppgifterna (sekretess)
- det i sådana informationssystem som är helt eller delvis automatiserade är möjligt att i efterhand entydigt kunna härleda utförda aktiviteter till en identifierad användare (spårbarhet)

Vårdgivaren ska utse minst en person som ansvarar för informationssäkerhetsarbetet och regelbundet rapporterar granskningar, åtgärder, riskanalyser och förbättringar. Det ska finnas rutiner för säkerhetskopiering av patientuppgifter. Säkerhetskopior ska förvaras på ett betryggande sätt och väl åtskilda från originaluppgifterna.



### Öppna nät

Om man använder öppna nät, till exempel Internet, för att hantera patientuppgifter måste det finnas rutiner för att säkerställa att ingen obehörig kan ta del av uppgifterna vid överföringen (t.ex. kryptering) och att man endast kommer åt uppgifterna genom stark autentisering, det vill säga användarens identitet kontrolleras på minst två olika sätt.



### Styrning av åtkomst

Vårdgivaren ansvarar för att det finns rutiner som säkerställer att hälso- och sjukvårdspersonalens och andra befattningshavares behörighet för åtkomst till patientuppgifter begränsas till vad som är nödvändigt för att ge en god och säker vård. En användares behörighet utgör en nyckel till patientuppgifter. Användaren ska enbart ha tillgång till de nycklar denne behöver för att utföra sitt arbete – inga andra.

Vårdgivaren ansvarar också för att informationssystemet har en uppbyggnad som kräver att behöriga användare måste göra aktiva val för att komma åt ytterligare uppgifter. Det måste alltså finnas tekniska trösklar i informationssystemet som innebär att användaren aktivt måste välja ytterligare åtkomst till information, vanligtvis genom att svara ja genom att klicka ok på en fråga från systemet om du verkligen behöver uppgifterna i ditt arbete. Denna åtgärd kommer att loggas, som alla andra åtgärder. På detta sätt ska en användare inte av oaktamhet beredas tillgång till patientuppgifter som denne inte behöver för att utföra sitt arbete och därmed inte heller har rätt att ta del av.



### Kontroll av åtkomst

Kontroll av åtkomst är viktigt för att säkerställa att personal inte felaktigt utnyttjar sina behörigheter genom att titta, ändra eller ta bort information som de inte ska hantera.

Om en person som arbetar åt vårdgivaren inte behöver uppgifterna i sitt arbete ska han eller hon inte heller ta del av uppgifter i journalen.

Kontrollen av åtkomst ska ske regelbundet. Hur ofta styrs av verksamhetens omfattning, antal personer med åtkomst, modell för behörighetstilldelning, kontrollens omfattning och andra faktorer.