



Stockholms
stad

Informationssäkerhet med logghantering och åtkomstkontroll av hälso- och sjukvårdsjournaler i Vodok och nationell patientöversikt (NPÖ)

UPPRÄTTAD AV MEDICINSKT
ANSVARIGA SJUKSKÖTERS KOR
OCH MEDICINSKT ANSVARIGA
FÖR REHABILITERING

Innehåll

1. Inledning	1
1.1 Hälso- och sjukvårdens värdegrund	1
2. Syfte.....	2
3. Ansvar	2
3.1 Information till personal	2
4. Egenkontroll av åtkomst till uppgifter.....	3
4.1 Behörighet för loggkontroller i Vodok och NPÖ	3
4.1.1 Vodok	3
4.1.2 NPÖ.....	3
5. Metod för loggkontroller i Vodok och NPÖ	4
5.1 Loggkontroll journaler i Vodok och NPÖ	4
5.2 Loggkontroll användare i Vodok och NPÖ	4
5.3 Sökmetod vid loggkontroll av journal och användare i Vodok.....	4
5.4 Sökmetod vid loggkontroll av journal och användare i NPÖ	5
5.5 Resultat utan anmärkning	5
5.6 Resultat med avvikelse	5
5.7 Resultat – misstanke om olovligt intrång	6
6. Andra riktade loggkontroller	6
7. Arkivering.....	6
Bilagor	6

1. Inledning

Informationssäkerhet är en del av det systematiska kvalitetsarbetet och ska genom ledningssystemet säkerställa att:

1. Dokumenterade personuppgifter är åtkomliga och användbara för den som har behörighet (*tillgänglighet*).
2. Patientens personuppgifter är oförvanskade (*riktighet*).
3. Obehöriga inte ska kunna ta del av personuppgifterna (*konfidentialitet*).
4. Åtgärder kan härledas till en användare (*spårbarhet*).

Begreppen tillgänglighet, riktighet, konfidentialitet och spårbarhet är centrala i arbetet för att nå en god informationssäkerhet.

Denna riktlinje för informationssäkerhet genom logghantering och åtkomstkontroll av hälso- och sjukvårdsjournaler i Vodok och nationell patientöversikt (NPÖ) beskriver hur informationen ovan säkerställs. Riktlinjerna gäller för verksamheter inom Äldreomsorgen och Socialtjänsten i Stockholms stad.

I patientdatalagen (PDL) och i Socialstyrelsens föreskrifter om journalföring och behandling av personuppgifter i hälso- och sjukvården regleras, bland annat vårdgivarens ansvar för logghantering och åtkomstkontroll till patientuppgifter vid elektronisk journalföring (Vodok) och sammanhållen journalföring (NPÖ).

Personal har inte rätt att ta del av några uppgifter som rör en patient som de inte har en aktuell vårdrelation med. Patienten har rätt att få veta vem som läst i journalen.

4 kap. 3 § Patientdatalagen, PDL (2008:355).

Socialstyrelsen föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården.

1.1 Hälso- och sjukvårdens värdegrund

Vården ska ges med respekt för alla människors lika värde.

Patientens ska visas omtanke och patientens självbestämmande och integritet ska respekteras.

Hälso- och sjukvårdspersonal ska utföra sitt arbete i överensstämmelse med vetenskap och beprövad erfarenhet. Vården ska så långt möjligt utformas och genomföras i samråd med patienten.

Hälso- och sjukvårdspersonal är skyldig att bedriva ett systematiskt patientsäkerhetsarbete och ska arbeta förebyggande för att förhindra att patienten drabbas av eller riskerar att drabbas av vårdskada.

2. Syfte

Syftet med logghantering och åtkomstkontroll är att granska att åtkomsten till patientuppgifter sker enligt gällande lagstiftning.

Det sker genom att följa upp:

- Sekretess/konfidentialitet, det vill säga att endast behöriga användare kommer åt journalinformationen.
- Spårbarhet, det vill säga vem som läst eller gjort ändringar i journalen.

3. Ansvar

I patientdatalagen framgår att vårdgivaren är skyldig att se till att åtkomst till uppgifter om patienter dokumenteras och kan kontrolleras.

Det är verksamhetschefen enligt hälso- och sjukvårdslagen (HSL) som ansvarar för att säkerställa att personalen har rätt åtkomstbehörighet för sina arbetsuppgifter genom att tilldela, förändra och avsluta/ta bort behörigheter för legitimerad personal.

Verksamhetschefen ansvarar även för egenkontroll av åtkomsten till patientuppgifter genom regelbundna och systematiska loggkontroller, dels av legitimerad personal, dels av patientjournaler. Verksamhetschefen kan överlåta till annan befattningshavare att utföra loggkontrollerna.

Legitimerad hälso- och sjukvårdspersonal ansvarar för att personliga lösenord och hjälpmedel, till exempel SIHTS- kort för autentisering inte är tillgängliga för någon annan.

Legitimerad hälso- och sjukvårdspersonal ansvarar också för att datorer som används för att hantera uppgifter om patienter inte lämnas utan att uppgifterna är skyddade mot obehörig åtkomst.

3.1 Information till personal

Verksamhetschefen ansvarar för att all legitimerad personal informeras om att regelbundna loggkontroller görs i verksamheten. De ska också känna till att olovligt intrång är straffbart enligt bestämmelserna om dataintrång, vilket kan leda till böter eller fängelse i högst två år enligt brottsbalkens 4 kap. 9c §.

Informationen ska vara skriftlig och undertecknas av den anställda som bekräftelse på att hen tagit del av informationen och förstått vad den betyder. Se bilaga 1. Information till personal om informationssäkerhet och logghantering i Vodok och NPÖ.

Socialstyrelsens föreskrifter och allmänna råd (SOSFS 2011:9) om ledningssystem för systematiskt kvalitetsarbete.
Hälso- och sjukvårdslag (2017:30) 4 kap. 2§.
Brottsbalken 4 kap. 9c §.

4. Egenkontroll av åtkomst till uppgifter

Egenkontroll av åtkomst till uppgifter ska göras systematiskt och återkommande. Varje journal i Vodok och varje användare ska kontrolleras minst en gång per år och resultatet av egenkontrollen ska dokumenteras.

En gång per år ska verksamheten göra en utvärdering/en samlad bedömning av resultatet av loggkontrollerna. Utvärderingen/den samlade bedömningen ska dokumenteras.

Av den samlade bedömningen ska det framgå hur ofta och i vilken omfattning egenkontrollerna gjorts. Den samlade bedömningen ska också innehålla en åtgärdsplan vid konstaterade brister, en tidsplan för när bristerna ska vara åtgärdade och vem som ansvarar. Utvärderingen/den samlade bedömningen ska ingå i den årliga patientsäkerhetsberättelsen.

Verksamheten ska ha lokal rutiner som säkerställer hur logghantering och åtkomstkontroll görs i Vodok och NPÖ.

4.1 Behörighet för loggkontroller i Vodok och NPÖ

4.1.1 Vodok

Verksamhetschefen beslutar om vem eller vilka som ska ha behörighet för att kunna genomföra loggkontroller i Vodok. Aktuella roller är: Vodok. Enhetschef och Vodok. Verksamhetschef HSL.

4.1.2 NPÖ

Verksamhetschefen kan utse en person med behörigheten administratör för att kunna genomföra loggkontroller i NPÖ. Stadsdelens Ek- administratör lägger upp behörigheten administratör under aktuellt medarbetaruppdrag.

De *lokala rutinerna* ska beskriva:

- vem eller vilka som har behörighet att göra loggkontroller i Vodok och NPÖ.

- Hur ofta stickprovskontroller av loggarna görs.
- Omfattningen av loggkontrollerna, det vill säga hur många journaler och användare som kontrolleras varje gång.
- Var loggkontrollerna och resultatet/den samlade bedömningen förvaras i verksamheten innan arkivering.

5. Metod för loggkontroller i Vodok och NPÖ

Alla användare och alla patientjournaler i Vodok ska kontrolleras minst en gång per år. För att säkerställa att detta sker kan loggkontrollerna med fördel göras samma datum varje månad.

Vid varje granskningstillfälle förs en logglista och ett protokoll över antalet granskade journaler, granskade användare med aktuella behörigheter, anmärkningar och åtgärder.

Vid loggkontroller i NPÖ kontrolleras även att patientens samtycke är dokumenterat i hälso- och sjukvårdsjournalen och att användaren har en aktuell vårdrelation till patienten.

Genomförda loggkontroller och resultatet ska dokumenteras på logglistan av den som granskat/kontrollerat loggarna. Loggarna granskas mot tjänstgöringslistan för att säkerställa att användare som varit inne i journalen varit i tjänst vid granskningstillfället.

Om resultatet överensstämmer med tjänstgöringslista dokumenterar granskaren detta på logglistan ”utan anmärkning”. Därefter tar verksamhetschef del av resultatet och signerar på logglistan.

Om avvikelser påvisats dokumenteras detta på logglistan. Se rubrik 5.6 Resultat med avvikelse.

5.1 Loggkontroll journaler i Vodok och NPÖ

Vid varje granskningstillfälle väljs ett antal journaler ut för loggkontroll. Se bilaga 2 Logglista- kontroll av loggar journaler.

5.2 Loggkontroll användare i Vodok och NPÖ

Vid varje granskningstillfälle väljs ett antal användare ut för loggkontroll. Se bilaga 3 Logglista- kontroll av loggar användare.

5.3 Sökmotord vid loggkontroll av journal och användare i Vodok

Gem Loggning är den sökning som används vid loggkontroller. Gem Loggning kan göras av personer med rollen Vodok enhetschef och Vodok Verksamhetschef HSL.

Instruktionen finns i Lathund för enhetschef i Vodok för rollen Vodok Enhetschef och Vodok Verksamhetschef HSL.

Lathunden ligger under Paraplyapplikationer/Dokumentation till vänster i inloggningsfönstret till Vodok.

- Klicka på Sök.
- Välj Gem Loggning.
- Bocka som standard för alla åtgärder i rutan Åtgärder.
- Välj för vilken period sökningen gäller.
- Välj specifik organisation i organisationsträdet
- Om du vill söka på personnummer (patientens personnummer) eller användare (ange användar- id).
- Klicka på Sök.

OBS! Det går att kombinera personnummer, användar- id och organisation för att få ett specifikt resultat.

- Sortera resultatet som vid en vanlig sökning genom att klicka på de olika rubrikerna.
- Välj de termer som ska ses genom fliken Termurval.
- Klicka på Rapporter (Skriv ut) för att kunna skriva ut resultatet av sökningen.
- Välj mellan utskrifterna Loggning eller Loggning enkel. Med utskriften Loggning fås alla värden i listan och med utskriften Loggning enkel fås en rad per aktivitet/användare/patient/dag.

5.4 Sökmetod vid loggkontroll av journal och användare i NPÖ

Verksamhetschefen eller utsedd administratör tar varje månad ut en loggrapport från Ineras Säkerhetstjänst.

Logga in med e-tjänstekort på nedanstående län
<https://loggtjanst.inera.se/>

- Välj medarbetaruppdrag Administration.
- Välj Hjälp i menyraden till vänster.
- Klicka på Användarhandbok. Instruktioner för hur loggrapporter tas fram i NPÖ beskrivs i kapitel 2.4 Loggrapport.

5.5 Resultat utan anmärkning

Om egenkontrollen av loggarna överensstämmer med tjänstgöringslista noterar verksamhetschefen detta på logglistan på följande vis: Utan anmärkning, datum, namnunderskrift och signatur.

5.6 Resultat med avvikelse

Om egenkontrollen av loggarna inte överensstämmer med tjänstgöringslista noterar verksamhetschefen detta på logglistan med hänvisning till aktuell avvikelse.

Verksamhetschefen tar reda på orsaken till avvikelser. När orsaken till avvikelse klarlagts, dokumenterats och eventuella åtgärder vidtagits, dokumenteras detta på logglistan med datum och verksamhetschefens namnunderskrift.

5.7 Resultat – misstanke om olovligt intrång

Vid misstanke om olovligt intrång ska verksamhetschefen dokumentera detta på logglistan med hänvisning till aktuell avvikelse. Åtgärder som verksamhetschefen vidtagit ska framgå av kommentarerna.

Verksamhetschefen ska även omgående informera medicinskt ansvarig sjuksköterska (MAS). Utredning görs av verksamhetschef i samråd med MAS, som granskar aktuella patienters dokumentation. Om misstanken om olovligt intrång kvarstår ska polisanmälan göras av verksamhetschefen. Utredningen lämnas på begäran till polisen.

Respektive nämnd ska alltid underrättas vid misstanke av olovligt intrång.

6. Andra riktade loggkontroller

Särskilda loggkontroller kan behöva göras, till exempel:

- För externa användare, som mobilt team/jourpatrull.
- För enskild patient, till exempel kända personer, eller vid annan nära relation till patienten när ingen aktuell vårdrelation föreligger.

7. Arkivering

Logglistor, protokoll över vilka journaler och användare som kontrollerats den aktuella perioden och utvärderingen/den samlade bedömningen ska arkiveras (bevaras) i stadsdelen. Vid avvikelser arkiveras även tjänstgöringslistor tillsammans med ovanstående.

Bilagor

1. Information till personal om informationssäkerhet med logghantering och åtkomstkontroll i Vodok och NPÖ.
2. Logglista- kontroll av loggar journaler.
3. Logglista- kontroll av loggar användare.