Koncernkontoret
Avdelningen för hälso- och sjukvårdsstyrning

Pia Lundbom
Tf. hälso- och sjukvårdsdirektör
pia.lundbom@skane.se

BESLUT

Datum: 2019-03-08
Dnr: 1800025

Instruktioner om styrning av behörigheter för åtkomst till uppgifter om patienter

Syftet med dessa instruktioner är att beskriva förutsättningarna för åtkomst till uppgifter om patienter samt ge verksamhetschefer vägledning vid genomförande av behovs- och riskanalyser.

Målet är att värna såväl patientens krav på integritet som medarbetarens behov av åtkomst till patientinformation för att kunna utföra och god och säker vård.

Härmed beslutas att

- Instruktioner om styrning av behörigheter för åtkomst till uppgifter om patienter, fastställs.
- ”Instruktioner om styrning av behörigheter för åtkomst till uppgifter om patienter” med diarienummer 1700202, daterad 2017-03-01, upphör att gälla.
- Den regionövergripande behovs- och riskanalysen som genomfördes i september 2011 upphör att gälla. Behov- och riskanalys ska genomföras av verksamhetschef och anpassas till den enskilda verksamhetens behov av åtkomst till uppgifter om patienter i enlighet med denna instruktion.

Pia Lundbom

Koncernkontoret
Enheten för säkerhet och intern miljöledning

Johan Reuterhäll
Informationssäkerhetschef
johan.reuterhall@skane.se

INSTRUKTION

Datum: 2018-12-04
Dnr: 1800025

Styrning av behörigheter för åtkomst till uppgifter om patienter

Syftet med dessa instruktioner är att beskriva förutsättningarna för åtkomst till uppgifter om patienter samt ge verksamhetschefer vägledning vid genomförande av behovs- och riskanalyser.

Målet är att värna såväl patientens krav på integritet som medarbetarens behov av åtkomst till patientinformation för att kunna utföra och god och säker vård.

Bakgrund

Enligt 4 kap. 2 § patientdatalagen (2008:355) ska en vårdgivare bestämma villkor för tilldelning av behörigheter för åtkomst till sådana 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.

Av prop. 2007/08:126 s. 148 anges bl.a. att syftet med bestämmelsen är att inpränta skyldigheten för den ansvariga vårdgivaren att göra aktiva och **individuella behörighetstilldelningar** utifrån analyser av vilken närmare information olika personalkategorier och olika verksamheter behöver. Men det behövs inte bara behovsanalyser. Även riskanalyser måste göras där man tar hänsyn till olika risker som kan vara förknippade med en alltför vid tillgänglighet avseende vissa slags uppgifter. Generellt kan sägas att ju mer omfattande ett informationssystem är, desto större mängd olika behörighetsnivåer måste det finnas. Avgörande för beslut om behörighet för t.ex. olika kategorier av hälso- och sjukvårdspersonal till elektronisk åtkomst till uppgifter i patientjournaler bör vara att behörigheten ska begränsas till vad befattningshavaren behöver för ändamålet en god och säker patientvård. 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.

Socialstyrelsen har i 4 kap. 2-3 §§ Socialstyrelsens förskrifter om informationshantering och journalföring i hälso- och sjukvården (HSLF-FS 2016:40) gett närmare föreskrift om hur styrningen av behörighet ska ske. ”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” samt ” Vårdgivaren ska ta fram rutiner för ändring, borttagning och regelbunden uppföljning av behörigheterna för att säkerställa att dessa är riktiga och aktuella.”.

Vårdgivaren (Region Skåne) ansvarar för att varje användare tilldelas en individuell behörighet för åtkomst till patientuppgifter. Det är verksamhetschefen, eller den som verksamhetschefen delegerat arbetsuppgiften till, som ska genomföra behovs- och riskanalys för medarbetarna inom den egna verksamheten och för de som arbetar på uppdrag av verksamhetschefen. För att behörigheterna i varje enskild verksamhet varken ska bli för vida eller för snäva behöver verksamhetschefen ha möjlighet att utforma behörigheterna så att de motsvarar den enskilda verksamhetens behov.

Målgrupp

Målgrupp är samtlig personal som har åtkomst till patientuppgifter, de som har ansvar för att tilldela behörighet till patientuppgifter samt de som administrerar och beställer system för åtkomst till patientuppgifter.

Individuell behovs- och riskanalys samt bedömning av behörighetstilldelning

Behörighet till patientuppgifter tilldelas vanligtvis inom ramen för vård- och behandling där åtkomst till patientuppgifter är en nödvändighet för att uppnå en god och säker patientvård. Behörighet ska baseras på den behovs- och riskanalys som genomförts utifrån verksamhetens uppdrag. Behovs- och riskanalysens resultat ska sedan ligga till grund för den behörighetsprofil som används vid tilldelning av behörigheter för medarbetare inom verksamheten.

Behörigheten ska motsvara det faktiska behovet och ska därmed varken vara för snäv vilket kan medföra patientsäkerhetsrisker eller för vid vilket kan innebära att patientens integritet påverkas negativt.

Tilldelning av behörighet kan ske av andra skäl än att åtkomst behövs för vård- och behandling. Sådana skäl kan vara att medarbetare behöver åtkomsten p.g.a. verksamhetsuppföljning, statistikframställning, central ekonomiadministration och liknande verksamhet som inte är individorienterad. I de flesta fall bör det därför räcka med tillgång till indirekta uppgifter som inte kan härledas till enskilda patienter. Inom det administrativa området bör det lämpligen bara vara enstaka personer som har elektronisk åtkomst till personnummer och andra uppgifter som direkt pekar ut enskilda patienter. Utgångspunkten är att åtkomst till patientinformation för andra ändamål än vård och behandling ska tilldelas mycket restriktivt.

I behörighetstilldelningen ingår även borttagning av behörigheter. Borttagning ska ske så snart behörigheten inte längre är nödvändig och syftar till att behörigheten ska motsvara det faktiska behovet.

Studerande och extern personal såsom konsulter, kan också tilldelas behörighet för åtkomst. De måste dock precis som övrig personal ha behov av åtkomst för att delta i vården av en patient eller för att de av annat skäl behöver uppgifterna för sitt arbete inom hälso- och sjukvården. För konsulter krävs att deras arbete utgör en del av vårdgivarens verksamhet, en grundförutsättning för detta är konsultens arbete utförs i vårdgivarens lokaler och inte på distans.

Studenters åtkomst till patientuppgifter

Hälso- och sjukvårdsstuderande som för sin utbildning behöver få tillgång till patientuppgifter kan ges tillgång utifrån samma kriterier som för anställda. Kriterierna är att det endera ska föreligga ett behov för att utföra arbetsuppgifter eller en vårdrelation till patienten. Praktikuppgifter får i detta sammanhang anses likställda med anställdas arbetsuppgifter.
Det ska observeras att tillgången uteslutande gäller patientuppgifter insamlade för syftet vård och behandling och därmed även kvalitetssäkring inom vårdgivaren Region Skåne (där patientsamtycke inte krävs), men inte vid deltagande i forskningsprojekt som kräver patients samtycke.
Unik identitet ska alltid användas i elektroniska vårdinformationssystem för att beteckna en hälso- och sjukvårdspersonal. På samma sätt ska studerande identifieras.

Hälso- och sjukvårdsstuderande ska dokumentera/registrera i regionens vårdinformationssystem under egen behörighet - praktiktidens längd är ovidkommande - och får således inte göra detta under handledares behörighet. Handledare ska finnas utsedd som kontrollerar dokumentationen/registreringen. Förteckning ska finnas över de studerandes identiteter (personnummer eller motsvarande), signaturer samt praktiktid och handledare.

Elektronisk åtkomst och behörighet

För åtkomst till patientuppgifter i elektroniska journalsystemen måste medarbetaren ha en tilldelad behörighet. Verksamhetschefen är ansvarig för att varje medarbetares behov och tillgång till uppgifter kontrolleras och att lämplig behörighet tilldelas. Medarbetaren är själv ansvarig för användningen av sin behörighet.

Den faktiska möjligheten att genom tilldelad, teknisk behörighet i IT-stödet bereda sig tillgång till patientuppgifter innebär inte att en medarbetare också har rätt att ta del av uppgifterna. Övriga kriterier (vårdrelation, behov av uppgifterna för arbetet m.m.) måste vara uppfyllda. Det är inte heller tillåtet att ta del av patientuppgifter genom elektronisk åtkomst om medarbetaren saknar teknisk behörighet för detta, oavsett om övriga kriterier är uppfyllda. Det är alltså aldrig tillåtet att använda en annan medarbetares behörighet för åtkomst till patientuppgifter.

Den tilldelade behörigheten kan jämföras med en nyckel som ger medarbetaren möjlighet att öppna registret med patientuppgifter. För att få nyckeln av verksamhetschefen krävs att den anställde har ett dokumenterat uppdrag (arbetsuppgift), uppdraget ska också tydliggöra ändamålet för behandlingen; t.ex. vård- och behandling, administration, kvalitetssäkring eller verksamhetsuppföljning. För att få använda nyckeln krävs slutligen också att det finns ett lagligt stöd för åtkomsten, dvs. att den anställde i det enskilda fallet deltar i vården av patienten eller av annat skäl behöver uppgifterna för sitt arbete.

Styrning av åtkomst och uppföljning i systemstöd

Beslut om behörighet utgår från behovs- och riskanalysen och utgår inte från vilka tekniska möjligheter som för stunden finns implementerat i ett visst IT-stöd (journalsystem etc.). Om den behörighet till åtkomst som behovs- och riskanalysen resulterar i inte går att ange i ett IT-stöd så ska detta rapporteras till förvaltningsgruppen[1] för aktuellt IT-stöd. Syftet med detta är att utveckla IT-stödet så att behörighetshanteringen blir bättre.
Respektive systemansvarig ansvarar för att det finns rutiner för hur tilldelning,

[1] Förvaltningsgruppen som definieras i den Verksamhetsstyrda styr- och förvaltningsmodellen för IT och MT-system

förändring, borttagning av behörigheter ska gå till utifrån de förutsättningar som systemstödet har. System ska utformas så att det enkelt går att få en överblick över aktuella tilldelade behörigheter.

Lagstiftning

- Patientdatalag (2008:355)
- Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLF-FS 2016:40)

Grundläggande regler

1. När är det tillåtet för en medarbetare att behandla journaluppgifter?

Vårdpersonal som möter patienter ska ta del av den egna vårdenhetens journaluppgifter och även ospärrade patientuppgifter från andra vårdenheter i den utsträckning som behöver för att ge en god och säker vård.
Vidare förutsätts medarbetare att i enlighet med verksamhetschefens instruktioner löpande följa upp sitt arbete som ett led i kvalitetssäkringen av vården.
Kvalitetssäkring kan ske genom individuell kvalitetsuppföljning avseende patienter man har, eller i närtid har haft, en vårdrelation till eller som projektbaserad kvalitetssäkring avseende patienter utifrån en viss diagnos eller annat urval.
Kvalitetssäkring ska återkopplas till verksamheten. Det finns regionala anvisningar[2] för kvalitetssäkring som mer detaljerat beskriver förutsättningarna.
Följande förutsättningar gäller för att få *behandla* (samla in, registrera, läsa och använda) patientuppgifter (tillåtna ändamål enligt lag och några förenklade exempel inom parentes).

1. att fullgöra de skyldigheter som anges i 3 kap. PDL (dvs. bestämmelser om vad som ska journalföras) och upprätta annan dokumentation som behövs i och för vården av patienter *(t.ex. läsa och skriva i journal samband med vårdrelation, samt upprätta intyg)*
2. administration som rör patienter och som syftar till att ge vård i enskilda fall eller som annars föranleds av vård i enskilda fall *(t.ex. tidsbokning, patientrelaterad ekonomiadministration och motsvarande)*
3. att upprätta annan dokumentation som följer av lag, förordning eller annan författning *(t.ex. anmälan enligt lex Maria och smittspårning)*
4. att systematiskt och fortlöpande utveckla och säkra kvaliteten i verksamheten
5. administration, planering, uppföljning, utvärdering och tillsyn av verksamheten (t.ex. verksamhetsuppföljning och intern granskning)
6. att framställa statistik om hälso- och sjukvården
7. fullgöra uppgiftsutlämnande som sker i överensstämmelse med lag eller förordning (t.ex. *sekretessbedömning inför ett eventuellt utlämnande av journaluppgifter)*

2. När är det inte tillåtet att ta del av patientuppgifter?

Har du inte en vårdrelation eller en arbetsuppgift som kräver tillgång till patientuppgifter är det inte tillåtet att del av patientuppgifter.
Utbildning är normalt inte en patientrelaterad arbetsuppgift i patientdatalagens bemärkelse. Du får alltså inte ta del av journaluppgifter endast i syfte att utbilda dig själv om en viss åkomma. Ska patientuppgifter användas för utbildning av andra ska de sammanställas av någon som har fått ett uppdrag att utföra detta och sedan

[2] Hantering av patientuppgifter för kvalitetssäkring inom vård och behandling i Region Skåne, diarienummer 1302691, daterad 2014-06-25

avidentifieras innan de används för utbildning.
Nyfikenhet är aldrig en acceptabel anledning för att ta del av patientuppgifter. Det är inte tillåtet att använda sin behörighet till IT-stöden för att ta del av sina egna patientuppgifter eftersom man inte har en vårdrelation till sig själv.
Överträdelse kan medföra rättsliga konsekvenser. Är du tveksam ska alltid kontakt tas med verksamhetschef för samråd.

3. Vad innebär begreppet inre sekretess

Begreppet ”inre sekretess” innebär att bara viss personal inom en vårdgivare har rätt att ta del av en patients journaluppgifter. Behörig personal tar alltid del av journaluppgifter på eget ansvar. Sekretessen innebär också att uppgifterna inte får spridas vidare, vare sig muntligen eller på annat sätt. Inre sekretess berör både elektroniska journalsystem och pappersjournaler, det vill säga all dokumenterad information om patienten.

4. Vad innebär begreppet ”deltar i vården av en patient” (vårdrelation)?

Vårdrelation innebär att medarbetare aktivt deltar i vården av en patient. Vårdinsatsen kan vara direkt; d.v.s. medarbetare som själv utför vården eller indirekt; medarbetare blir konsulterad angående vården av patienten. Det kan också gälla administration som rör patienter och som syftar till att ge vård i enskilda fall eller som annars föranleds av vård i enskilda fall.
Det är alltid medarbetaren själv, inte vårdgivaren som organisationen (Region Skåne) som har vårdrelationen. En läkare som inte längre behandlar en patient deltar inte längre i vården av patienten och saknar därmed vårdrelation även om patienten själv fortfarande behandlas inom vårdgivaren men av annan hälso- och sjukvårdpersonal t.ex. på en annan vårdenhet.
När ett deltagande i vården av en patient mer exakt börjar och slutar kan verka diffust. Normalt börjar vården med att patienten kontaktar sjukvården och avslutas när vårdinsatsen avslutas. I förarbetena till Patientdatalagen anges att vårdrelationen är avslutad då en patient skrivs ut som färdigbehandlad och det inte finns några inplanerade återbesök. Detsamma gäller om patienten skrivs ut för fortsatt vård eller uppföljning på annan vårdenhet eller i annan vårdgivares regi, d.v.s. när ansvaret för patienten tagits över av någon annan.

5. Vad innebär att varje användare ska tilldelas en individuell behörighet?

Alla användare ska ha en individuell behörighet. Detta innebär att endast personliga inloggningar är tillåtna. Gruppkonton med åtkomst till patientuppgifter får inte förekomma. Varje enskild användare är ansvarig för det som görs från hans eller hennes behörighet och ska hålla inloggningsuppgifter skyddade.

6. Hur gör jag en behovs- och en riskanalys?

Medarbetares behörighet till patientuppgifter ska vara anpassad till aktuella arbetsuppgifter. Tilldelas medarbetaren rätt behörighet, dvs. tillräcklig behörighet för att denne ska kunna utföra sina arbetsuppgifter på ett säkert sätt men samtidigt inte mer omfattande än vad som är nödvändigt?
Ett beslut om tilldelning av behörighet ska föregås av en behovs- och riskanalys. Tabellen nedan kan användas som stöd.

7. Hur ska behörigheterna följas upp?

Verksamhetschefen, eller den som verksamhetschefen delegerat arbetsuppgiften till, ska **minst en gång per år**, samt i samband med förändring av arbetsuppgifter, granska att varje medarbetares behörigheter överensstämmer med de arbetsuppgifter som medarbetaren har. Den årliga granskningen kan med fördel genomföras i samband med medarbetarsamtal eller liknande samtal som kontinuerligt genomförs med varje medarbetare.
Förändringar i arbetsuppgifter eller deltagande i projekt och arbetsgrupper kan påverka hur medarbetarens behörigheter ska se ut. Vid kontroll av behörigheter bör nedanstående uppmärksammas.

- För mycket (vida) behörigheter:
  Har det skett förändringar i medarbetarens arbetsuppgifter som gör att någon eller några behörigheter till journalsystem, andra IT-system eller gemensamma mappar inte längre behövs?

- För lite (snäva) behörighet:
  Behöver medarbetaren nya behörigheter i journalsystemet, annat IT-system eller gemensamma mappar för att kunna utföra sina arbetsuppgifter?

Uppföljning av loggar
Uppföljning av loggar ska ske i enlighet med instruktionen[3] för loggkontroll. Loggkontrollen är ett komplement till den regelbundna uppföljningen av behörigheter för att tillse att behörigheter inte missbrukas.

[3] Instruktion – Loggkontroll, granskning av åtkomst till patientuppgifter, daterad 2013-07-01

Bilaga 1 – Mall för genomförande av behovs- och riskanalys

Namn på medarbetare:_____

Datum för genomförande:_____

Behov av att…	**Ja/Nej**	**Ev. undantag**	**Överväganden**	**Övriga omständigheter**
Läsa och skriva i journalen inom ramen för en vårdrelation samt upprätta intyg				
Kunna läsa andra vårdenheters (inom Region Skåne) journaler				
Kunna läsa i andra vårdgivares (utanför Region Skåne) journaler				
Utföra patientadministration som rör patienter och som syftar till att ge vård i enskilda fall eller som annars föranleds av vård i enskilda fall *(t.ex. tidsbokning, patientrelaterad ekonomiadministration och motsvarande)*				
Upprätta annan dokumentation som följer av lag, förordning eller annan författning *(anmälan*				

enligt lex Maria och smittspårning)				
Systematiskt utveckla och säkra kvaliteten i verksamheten				
Administrera, planera, följa upp, utvärdera och/eller bedriva tillsyn av verksamheten *(t.ex. verksamhetsuppföljning och intern granskning)*				
Framställa statistik om hälso- och sjukvården				
Fullgöra uppgiftsutlämnande som sker i överensstämmelse med lag eller förordning *(t.ex. sekretessbedömning inför ett eventuellt utlämnande av journaluppgifter)*				

Undertecknas av verksamhetsansvarig

_____

_____

Namnförtydligande