Behovs och riskanalys för behörighetstilldelning - Rutin. Hälso- och sjukvård Region Gävleborg

Innehåll

1. Syfte och omfattning 1
2. Allmänt 1
3. Ansvar och roller 2
3.1. Verksamhetschef 2
3.2. Informationssäkerhetsenheten 2
3.3. Hälso- och sjukvårdsdirektör 2
4. Beskrivning 2
4.1. Behovsanalys 3
4.2. Riskanalys 3
4.3. Säkerhetsåtgärder 4
4.4. Behörigheter 4
4.5. Dokumentation 5
5. Plan för kommunikation och implementering 5
6. Dokumentinformation 5
7. Referenser 6

1. Syfte och omfattning

Syftet med denna rutin är att säkerställa att Region Gävleborg uppfyller 4 kap 2 § i Patientdatalagen samt Socialstyrelsens föreskrift 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.”

Denna rutin omfattar samtliga verksamheter som har behov av tillgång till patientuppgifter. Rutinen bygger på Behovs- och riskanalys för behörighetstilldelning - Direktiv.

2. Allmänt

Patientdatalagen ger vårdgivaren rätt att ta del av den patientinformation som krävs för att ge patienter en god och säker vård. Vårdgivaren ska bestämma villkor för tilldelning av behörighet för åtkomst till sådana uppgifter om patienter som förs helt eller delvis automatiserat.

Det är inte tillåtet att ge vårdpersonal tillgång till all information i vårdinformationssystemen utan behörigheten ska baseras på det behov som varje yrkeskategori har i respektive verksamhet. Behörigheten ska begränsas till vad

som behövs för att den enskilde ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården.

Omfattningen av behörigheten ska baseras på en behovs- och riskanalys för behörighetstilldelning utifrån verksamhetens uppdrag. Resultat ligger sedan till grund för den behörighetsprofil som används vid tilldelning av behörigheter för medarbetare inom verksamheten.

3. Ansvar och roller

3.1. Verksamhetschef

Verksamhetschef ansvarar för att
- Behovs- och riskanalys för behörighetstilldelning genomförs, samt årlig revidering i Platina.
- Vid behov delegera uppgiften som analysledare/analysteam till medarbetare inom verksamheten.
- Ansvarar för att meddela IT Platina-ID för giltigt behovs och riskanalys.

3.2. Informationssäkerhetsenheten

Informationssäkerhetsfunktionen ansvarar för att
- Implementera och uppdatera denna rutin,
- ta fram mall för dokumentation av behovs- och riskanalys för behörighetstilldelning,
- utgöra ett stöd för verksamhetschefen vid upprättande av behovs- och riskanalys för behörighetstilldelning,
- samt följa upp att denna rutin efterlevs.

3.3. Hälso- och sjukvårdsdirektör

Hälso- och sjukvårdsdirektör ska årligen eller vid behov fastställa denna rutin.

4. Beskrivning

Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLF-FS 2016:40) kräver att vårdgivaren genomför en behovs- och riskanalys för behörighetstilldelning som underlag för behörighetstilldelningen i vårdgivarens vårdinformationssystem. Det uttryckliga kravet på att vårdgivaren ska tilldela varje användare en individuell behörighet för åtkomst till patientuppgifter och att det ska föregås av en behovs- och riskanalys återfinns i 4 kap. 2 § Socialstyrelsens föreskrifter HSLF-FS 2016:40.

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.

Detta innebär att behörigheter ska tilldelas utifrån det behov olika yrkeskategorier har i berörd verksamhet. Behovet baseras på de arbetsuppgifter respektive yrkeskategori har i verksamheten.

Behovs- och riskanalysen för behörighetstilldelning ska göras individuellt för respektive medarbetare. Dock kan en mer generell analys göras för en specifik yrkeskategori med specifika arbetsuppgifter. Denna ska sedan verksamhetschefen stämma av mot när en individ tilldelas sin behörighet.

Det har genomförts en övergripande behovs- och riskanalys på en övergripande nivå, Behovs och riskanalys för behörighetstilldelning - behörighetstilldelning vårdgivarnivå. Hälso- och sjukvård Region Gävleborg**.** Detta dokument har begränsad åtkomst i Platina och för åtkomst kontaktas informationssäkerhetsenheten.

4.1. Behovsanalys

Behovet av tillgång till patientinformation styrs av

- verksamhetens uppdrag (t.ex. onkologisk verksamhet, akutsjukvård, ortopedisk verksamhet, primärvårdsverksamhet, etc.)
- yrkeskategori (t.ex. läkare, sjuksköterska, undersköterska, dietist, kurator, medicinsk sekreterare, etc.)
- arbetsuppgifter (t.ex. diabetessjuksköterska, jour, bakjour, avvikelsehantering, kvalitetsuppföljning, etc.)

Behovsanalysen ska således identifiera och förteckna verksamhetens uppdrag, de olika yrkeskategorier som finns i verksamheten samt de uppdrag som medarbetarna har i verksamheten.

Behovet av åtkomst till patientuppgifter ska fastställas utifrån verksamhetens arbetssätt och uppdrag.

4.2. Riskanalys

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.

För att kunna bedriva en god och säker vård krävs det tillgång till relevant patientinformation. Vad som räknas som relevant baseras på verksamhetens uppdrag.

En för vid/generös behörighet kan leda till konsekvenser som obefogad spridning av patientuppgifter eller förlorad riktighet i form av felaktig radering eller förändring av information. En för snäv behörighet kan innebära att användaren inte kan utföra sina arbetsuppgifter vilket medföra risker gällande patientsäkerheten.

Följande risker ska beaktas

- Risker som uppstår om medarbetare inom verksamheten inte har tillgång till relevant patientinformation
- Risker relaterade till för bred/generös tillgång till vårdinformation

Risker som kan påverka den enskildes fri- och rättigheter ska särskilt beaktas, riskerna som leder till negativa konsekvenser för patientsäkerheten eller att patientens integritet påverkas negativt. Faktorer som bör beaktas vid bedömningen av risken för patienters rättigheter och friheter är bland annat om det är frågan om personuppgifter som omfattas av tystnadsplikt, uppgifter om hälsa eller sexualliv, om det sker behandling av personuppgifter rörande sårbara fysiska personer, framför allt barn.

Riskerna dokumenteras tillsammans med behovsinventeringen i Platina enligt framtagen mall. Vid behov kan riskerna identifieras och värderas enligt gällande rutin för riskanalys inom Region Gävleborg.

I *Behovs och riskanalys för behörighetstilldelning - behörighetstilldelning vårdgivarnivå. Hälso- och sjukvård Region Gävleborg* har till övervägande del relevanta risker analyserats, det återstår för respektive verksamhetsområde att identifiera de risker som inte identifierats och analyserats av den övergripande riskanalysen.

4.3. Säkerhetsåtgärder

Tekniska och organisatoriska säkerhetsåtgärder ska vidtas för att skydda informationen och för att minimera eller eliminera identifierade risker. I *Behovs- och riskanalys för behörighetstilldelning - behörighetstilldelning vårdgivarnivå* har övergripande åtgärder identifieras som implementeras för samtliga verksamheter. Det kan finnas behov av ytterligare säkerhetsåtgärder på respektive verksamhetsområde.

4.4. Behörigheter

Behovs- och riskanalysen för behörighetstilldelning ska identifiera vilken behörighet inom berörda vårdinformationssystem respektive yrkeskategori i analyserad verksamhet har behov av att få tillgång till för att kunna erbjuda en god och säker vård.

Patientdatalagen medger inte att medarbetare ges tillgång till all tillgänglig patientinformation hos vårdgivaren. Det vill säga, det är inte tillåtet att tilldela

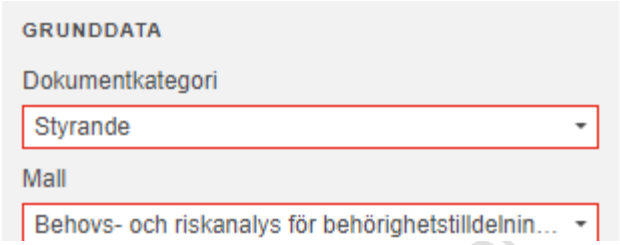
behörigheter så att man får tillgång till all tillgänglig patientinformation i våra journalsystem.

Om resultatet i behovs- och riskanalysen för behörighetstilldelning inte går att förverkliga genom lämplig behörighet i aktuellt IT-stöd ska detta rapporteras till IT-avdelningen med önskemål om förändring.

Verksamhetschefen ansvarar för att skicka beställning om tillägg samt borttagning av behörigheter till IT-support. I beställningen ska Platina ID för verksamhetsområdets behovs- och riskanalys anges. Verksamhetschef ansvarar för att IT-support är informerad om Platina ID för giltig behovs- och riskanalys.

4.5. Dokumentation

Behovs- och riskanalysen ska dokumenteras i Platina enligt framtagen mall och denna ska revideras minst årligen.



Dokumentkategori: Styrande
Titel: *Behovs- och riskanalys för behörighetstilldelning – verksamhetsområde xxxx*
Fastställare: Ansvarig verksamhetschef
Ledningssystem: 11. Säkerhet
Dokumenttyp: Redovisande dokument
Organisation: verksamhetsområdet
Granskare: avgör verksamhetschef
Slutgranskare: avgör verksamhetschef
Fastsställare: Verksamhetschef

5. Plan för kommunikation och implementering

Implementering sker via Plexus samt enskilt med respektive VC i anslutning till arbetet med behovs- och riskanalys för behörighetstilldelning.

6. Dokumentinformation

Denna rutin har tagits fram av informationssäkerhetsenheten med stöd av IT-avdelningen, representanter från Hälso- och sjukvården och juridikavdelningen. Dokumentet är framtaget enligt Integritetsskyddsmyndighetens vägledning.

7. Referenser

Dokumentnamn	Plats
Behovs- och riskanalys för behörighetstilldelning - Direktiv	Platina
Behovs och riskanalys för behörighetstilldelning - behörighetstilldelning vårdgivarnivå. Hälso- och sjukvård Region Gävleborg	Platina
Behovs och riskanalys för behörighetstilldelning - Mall. Hälso och sjukvård Region Gävleborg	Platina
Patientdatalag (2008:355)	Riskdagen.se
Behovs- och riskanalys inom hälso och sjukvården – en vägledning	imy.se
HSLF-FS 2016:40 Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården	Socialstyrelsen.se