REGION SÖRMLAND

MISSIV

Revisionen

Datum
2019-01-31

Dokumentnummer
RE-REV19-0003

För kännedom
Enligt sändlista

Regionstyrelsen
Nämnden för kultur, utbildning och friluftsverksamhet
Nämnden för primärvård, rättspsykiatri och Dammsdalskolan
Patientnämnden

Skyddade personuppgifter

Region Sörmlands revisionskontor har på uppdrag av regionens revisorer genomfört en granskning av hanteringen av skyddade personuppgifter från Skatteverket.

Syftet med granskningen är att bedöma om regionstyrelsen och övriga berörda nämnder, säkerställer att hanteringen av skyddade personuppgifter är ändamålsenlig och bedrivs med god intern kontroll. Hanteringen har granskats för grupperna patienter, elever och medarbetare.

Revisorerna diskuterade om en förstudie skulle göras som ett första steg för att ta reda på mer information på området. På grund av den höga risken och de allvarliga konsekvenserna vid felaktig hantering och för fortsatt förtroende för verksamheten, beslutade revisorerna att en övergripande granskning skulle prioriteras i granskningsplanen

Vår sammanfattande bedömning är att regionstyrelsen och berörda nämnder delvis säkerställer en ändamålsenlig hantering av skyddade personuppgifter och att hanteringen delvis sker med god intern kontroll. Bedömningen är att det finns risk att skyddade personuppgifter kan röjas.

Hanteringen av skyddade personuppgifter ingår i informationssäkerhetsarbetet och granskningen har visat på brister på ett antal områden. Bland annat bedöms inte det styrande dokumentet informationssäkerhetsanvisningen vara helt ändamålsenligt på området skyddade personuppgifter. Det är inte formulerat på ett tydligt sätt så det framgår hur hantering ska ske för samtliga grupper som kan ha skyddade personuppgifter. Det är inte heller känt i verksamheterna. E-utbildningarna i informationssäkerhet som finns innehåller inget avsnitt om skyddade

personuppgifter. Det saknas verksamhetsspecifika dokumenterade rutiner för arbetssätt för skyddade personuppgifter som utgår från de regionsgemensamma dokumenten.

Revisorerna ställer sig bakom de rekommendationer som framförs i rapporten.

Ett gemensamt yttrande från regionstyrelsen, nämnden för kultur, utbildning och friluftsverksamhet, nämnden för primärvård, rättpsykiatri och Dammsdalskolan och patientnämnden på rapporten samt uppgifter om verkställda och planerade åtgärder emotses av revisorerna senast 8 maj 2019.

I det avslutande skedet av granskningen har regeringen meddelat beslutade lagändringar från januari 2019 som syftar till att förbättra och öka skyddet för hotade och förföljda personer. Dessa lagändringar bör beaktas i det fortsatta arbetet med regionens hantering av skyddade personuppgifter.

Gustaf Wachtmeister
Ordförande

Marita Bengtsson
Vice ordförande

Sändlista
Jan Grönlund, regiondirektör
Kajsa Fisk, HR-direktör
Mikael Palo, verksamhetsområdes chef Kultur & Utbildning Sörmland
Anna Ormegaard, divisionschef primärvård
Charlotta Widerberg, verksamhetschef Dammsdalskolan
Anna Wångmar, enhetschef patientnämndens kansli
Lars Gunnar Svensson, säkerhetschef, säkerhets- och beredskapsenheten
Jonas Jensen, informationssäkerhetsansvarig, säkerhets- och beredskapsenheten
Caroline Dexfalk, chefsjurist, juridiska staben

REGION SÖRMLAND

Revisonen

Datum

2019-01-24

Dokumentnummer

RE-REV19-0003

Granskningsrapport
Skyddade personuppgifter

Handläggare
Åsa Forsman

Datum
2019-01-24

Dokumentnummer
RE-REV19-0003

Innehåll

Handläggare
Åsa Forsman

Datum
2019-01-24

Dokumentnummer
RE-REV19-0003

Sammanfattning

Region Sörmlands revisionskontor har på uppdrag av regionens revisorer genomfört en granskning av hanteringen av skyddade personuppgifter från skatteverket. Syftet med granskningen är att bedöma om regionstyrelsen och övriga berörda nämnder, säkerställer att hanteringen av skyddade personuppgifter är ändamålsenlig och bedrivs med god intern kontroll. Hanteringen har granskats för grupperna patienter, elever och medarbetare.

Vår sammanfattande bedömning är att regionstyrelsen och berörda nämnder delvis säkerställer en ändamålsenlig hantering av skyddade personuppgifter och att hanteringen delvis sker med god intern kontroll. Bedömningen är att det finns risk att skyddade personuppgifter kan röjas.

Granskningen har visat att det finns regionsgemensamma styrdokument inom området informationssäkerhet, där skyddade personuppgifter ingår. Styrdokumentet informationssäkerhetsanvisningen bedöms inte vara helt ändamålsenligt på området skyddade personuppgifter. Det är inte formulerat på ett tydligt sätt så det framgår hur hantering ska ske för samtliga grupper som kan ha skyddade personuppgifter. Styrdokumenten är inte kända i verksamheterna. Det får till följd att de inte tillämpas och det saknas bland annat verksamhetsspecifika dokumenterade rutiner som beskriver hur hantering, arbetsätt, kommunikation med mera ska ske för att undvika att skyddade personuppgifter röjs. Egenkontroller görs inte i nuläget och regionstyrelsen, nämnder och verksamheter följer inte upp informationssäkerhetsarbetet.

Samtliga som intervjuas anger att medarbetarna får utbildning på området via de obligatoriska regionsgemensamma e-utbildningarna om informationssäkerhet. Det är felaktigt då utbildningarna inte innehåller något avsnitt om skyddade personuppgifter. Kunskap på området är en förutsättning för att kunna tänka på vilka risker som kan uppstå i den egna verksamheten och vilka rutiner som behöver finnas för att undvika att skyddade personuppgifter röjs.

Det är positivt att det finns dokumenterade rutiner i verksamheterna för hantering i olika IT-system, att märkning görs och att information döljs. Behörigheterna i IT-systemen är begränsade. Loggningskontroller utförs i hälso-och sjukvården. Samtliga delar är i enlighet med de regionsgemensamma styrdokumenten och skatteverkets vägledning.

Handläggare
Åsa Forsman

Datum
2019-01-24

Dokumentnummer
RE-REV19-0003

Efter genomförd granskning lämnar vi nedanstående rekommendationer till **regionstyrelsen** för det fortsatta arbetet med hanteringen av skyddade personuppgifter och för att stärka informationssäkerhetsarbetet:

- ✓ Utveckla de regionsgemensamma styrdokumenten så att perspektiv finns med för alla grupper som kan ha skyddade personuppgifter
- ✓ Säkerställ att de regionsgemensamma styrdokumenten är kända
- ✓ Tydliggör vad som ska gälla för att lämna ut uppgifter om medarbetares namn och arbetsplats.
- ✓ Komplettera de regionsgemensamma e-utbildningarna om informationssäkerhet så att skyddade personuppgifter ingår
- ✓ Säkerställ att verksamheterna har dokumenterade rutiner för arbetsätt för samtliga delar i hanteringen av skyddade personuppgifter och som utgår från de regionsgemensamma styrdokumenten
- ✓ Utveckla och samla informationen på intranätet
- ✓ Slutför utvecklingsarbetet av hur "egenkontroll informationssäkerhet" ska genomföras och säkerställ att verksamheter årligen genomför "egenkontroll informationssäkerhet" utifrån det regionsgemensamma styrdokument
- ✓ Säkerställ att regionstyrelsen och nämnder genomför uppföljning av informationssäkerhetsarbetet utifrån det regionsgemensamma styrdokument

Efter genomförd granskning lämnar vi nedanstående rekommendationer till **nämnden för primärvård, rättspsykiatri och Dammsdalskolan, patientnämnden och nämnden för kultur, utbildning och friluftsverksamhet** för det fortsatta arbetet med hanteringen av skyddade personuppgifter

- ✓ Säkerställ att verksamheterna har dokumenterade rutiner för arbetsätt för samtliga delar i hanteringen av skyddade personuppgifter och som utgår från de regionsgemensamma styrdokumenten

I det avslutande skedet av granskningen har regeringen meddelat beslutade lagändringar från januari 2019[1] som syftar till att förbättra och öka skyddet för hotade och förföljda personer. Dessa lagändringar bör beaktas i det fortsatta arbetet med regionens hantering av skyddade personuppgifter.

[1] Beslutsunderlag: Prop. 2017/18:145 Ökat skydd för hotade och förföljda personer samt åtgärder för att öka kvaliteten i folkbokföringen

Handläggare
Åsa Forsman

Datum
2019-01-24

Dokumentnummer
RE-REV19-0003

Bakgrund

Uppgifter inom folkbokföringsverksamheten är i regel offentliga enligt 22 kap 1 § i offentlighets- och sekretesslagen. Personer (och deras närstående) som till exempel utsätts för eller riskerar att utsättas för hot, våld eller förföljelse, kan lida skada eller men om deras personuppgifter lämnas ut.

Skyddade personuppgifter är en metod och ett samlingsnamn som skatteverket använder för olika typer av skyddsåtgärder beroende på av arten av hot och som personen kan ansöka om.

Det är viktigt att hantera personuppgifter för personer med skyddade personuppgifter med stor aktsamhet. Brister i hanteringen är en hög riskfaktor och kan få mycket allvarliga konsekvenser om uppgifter röjs till utomstående personer eller görs offentliga.

Enligt skatteverket[2] har cirka 16 000 personer skyddade personuppgifter i Sverige. Andra kvartalet 2018 hade Sverige 10 171 524 innevånare[3] och Sörmlands län hade 293 182 innevånare[4]. Utifrån antalet bosatta i Sörmlands län, skulle det innebära att cirka 460 personer skulle kunna ha skyddade personuppgifter i länet.

En person med skyddade personuppgifter kan bland annat vara patient, elev eller medarbetare och behöva komma i kontakt med olika delar av regionens organisation. Det innebär att ett stort antal medarbetare behöver ha kunskap om rutiner och riktlinjer på området. Ett stort antal medarbetare och i kombination med att de har behörighet till många olika IT-system där personuppgifter finns, ökar risken för att felaktig hantering kan ske och att personuppgifter röjs.

Hanteringen av skyddade personuppgifter ingår i Region Sörmlands informationssäkerhetsarbete. Att bedriva detta arbete med hög kvalitet, är avgörande för allmänhetens förtroende för verksamheten. Det är därför viktigt att styrande dokument och rutiner finns, är kända, och tillämpas av alla verksamheter.

Utifrån en bedömning av risk-och väsentlighet har revisorerna i Region Sörmland beslutat att genomföra en granskning på övergripande nivå av den

[2] Telefonintervju med medarbetare på skatteverkets sekretessgrupp 2018-09-27
[3] Befolkningsstatistik kvartal 2 2018, SCB:s hemsida 2018-09-27
[4] Befolkningsstatistik kvartal 2 2018, SCBS: hemsida 2018-09-27

interna styrningen och kontrollen, i rutiner, riktlinjer och arbetsätt, för hantering av skyddade personuppgifter. Revisionen har inte kunskap om vilka rutiner och riktlinjer som finns i organisationen på området. Området har inte granskats tidigare och ingår i revisionsplan 2018.

Revisorerna diskuterade om en förstudie skulle göras som ett första steg för att ta reda på mer information på området. På grund av den höga risken och de allvarliga konsekvenserna vid felaktig hantering och för fortsatt förtroende för verksamheten, beslutade revisorerna att en övergripande granskning skulle prioriteras i granskningsplanen. Detta för att bedöma den interna styrningen och kontrollen på området snarast och inte skjuta den längre fram i tiden.

Syfte

Syftet med granskningen är att bedöma om regionstyrelsen och övriga berörda nämnder, säkerställer att hanteringen av skyddade personuppgifter är ändamålsenlig och bedrivs med god intern kontroll.

Revisionsfrågor

Säkerställer regionstyrelsen och övriga berörda nämnder en ändamålenlig hantering av skyddade personuppgifter och sker hanteringen med god intern kontroll?

- ✓ Finns det styrande dokument och rutiner för hanteringen av skyddade personuppgifter?
- ✓ Är styrande dokument och rutiner ändamålsenliga?
- ✓ Är styrande dokument och rutiner kända?
- ✓ Tillämpas styrande dokument och rutiner?

Metod

Granskningen har skett genom dokumentstudier av styrande dokument i Region Sörmland, rutiner och externa regelverk/lagstiftning på området. Intervjuer har genomförts med medarbetare som valts ut för att kunna bedöma hanteringen av skyddade personuppgifter för patienter, elever och medarbetare. I hälso-och sjukvården har intervjuerna i verksamheterna gjorts utifrån stickprov. De intervjuade har fått faktaavstämma innehållet i granskningsrapporten.

Tidsperioden för granskningen är nutid, hösten 2018 och granskningen har genomförts under september-december 2018.

Avgränsning

Granskningen avser regionstyrelsen, nämnden för primärvård, rättspsykiatri och Dammsdalskolan (privata vårdgivare ingår inte), patientnämnden och nämnden för kultur, utbildning och friluftsverksamhet.

Nämnderna är valda för att göra en övergripande granskning för verksamheter som bedriver hälso-och sjukvård och skola och för att granska hanteringen av skyddade personuppgifter för patienter, elever och medarbetare. Granskningen omfattar inte fakturahantering i ekonomisystemet utan hantering i verksamhetsspecifika IT-system.

Revisionskriterier

Lagar och rekommendationer:
Offentlighets- och sekretesslagen
Patientdatalagen
Skatteverket, vägledning för hantering av sekretessmarkerade personuppgifter i offentlig förvaltning
Datainspektionen, checklista för skolor
Skolverket, unga med skyddade personuppgifter, stödmaterial

Styrande dokument i Region Sörmland
Säkerhetspolicy
Informationssäkerhetsanvisning
Posthantering för personer med skyddade personuppgifter från skatteverket
Riktlinje avseende åtgärder vid dataintrång

Granskningsresultat

Skyddade personuppgifter

Den som är utsatt för hot kan i vissa fall få skyddade personuppgifter. Det innebär att till exempel namn och adress skyddas i folkbokföringsregistret. I vanliga fall är uppgifterna i det svenska folkbokföringsregistret offentliga. Det finns tre typer av skyddade personuppgifter eller skyddad identitet som man också kan säga:

- ✓ sekretessmarkering och kvarskrivning som är den lägre graden av skyddade personuppgifter
- ✓ kvarskrivning som är ett starkare skydd än sekretessmarkering
- ✓ fingerade personnummer som innebär att personen får ett nytt namn och personnummer

Sekretessmarkering och kvarskrivning ansöker man om hos Skatteverket. Fingerade personuppgifter ansöker man om hos Polisen[5].

Personuppgifter, inklusive sekretessmarkeringen, aviseras från Skatteverket till andra myndigheter. Mottagande myndighet väljer själv hur den ska hantera sekretessmarkerade personuppgifter i sina system. Det finns inte några rättsliga regler för hanteringen. Spridningen av sekretessmarkeringen till olika myndigheter i samhället medför därför många frågor om hanteringen av densamma.

Med enhetliga rutiner kan hanteringen underlättas inom den offentliga förvaltningen och minska risken att sekretessmarkerade personuppgifter lämnas ut oavsiktligt. Skatteverket har därför i samråd med andra myndigheter utarbetat följande allmänna information och vägledning för hantering av sekretessmarkerade personuppgifter[6].

Styrande dokument och organisation på central nivå

Det finns fyra styrande dokument på olika nivåer på området informationssäkerhet dit skyddade person uppgifter hör och det är två enheter som har utfärdat dem. Den ena är Säkerhets- och beredskapsenheten och den andra är juridiska staben.

Enligt information på intranätet arbetar Säkerhets- och beredskapsenheten med att, inom säkerhet och beredskapsområdet, skapa förutsättningar för regionen att på ett effektivt och ändamålsenligt sätt bedriva sina verksamheter. Verksamheten är experter och ger stöd inom bland annat området informationssäkerhet där skyddade personuppgifter ingår. Säkerhet – och beredskapsenheten är organiserad i Verksamhets- och ledningsservice och arbetar på uppdrag av regionstyrelsen.

---

5 Skatteverket.se/privat/folkbokforing/skyddadepersonuppgifter.4.18e1b10334ebe8bc80001711.html?q=vad+%C3%A4r+skyddade+personuppgifter

6 https://www.skatteverket.se/foretagochorganisationer/myndigheter/informationsutbytemellanmyndigheter/folkbokforingsekretessmarkeradepersonuppgifter.4.18e1b10334ebe8bc80002541.html?q=skatteverkets+v%C3%A4gledning+f%C3%B6r+hantering+av

Informationssäkerhetsansvarig ingår i säkerhets- och beredskapsenheten och har intervjuats.

Av information på intranätet framgår det att juridiska staben är den centrala enhet som ska främja rättssäkerheten i regionens verksamheter och ska förebygga rättstvister. Arbetet sker både genom förebyggande insatser som till exempel information och utbildning och som stöd i det konkreta arbetet. Juridiska staben är organiserad i staber och regionsövergripande verksamheter och arbetar på uppdrag av regionstyrelsen. En av juristerna har intervjuats.

Säkerhetspolicy[7]- styrande dokument
Säkerhetspolicy är huvuddokumentet och utfärdad av säkerhets- och beredskapsenheten och är beslutad av regionfullmäktige. Den finns på externa hemsidan och på intranätet. Säkerhetspolicyn innehåller inget om hantering av skyddade personuppgifter.

informationssäkerhetsanvisning[8]- styrande dokument
Informationssäkerhetsanvisning kompletterar policyn och är utfärdad och beslutad på tjänstemananivå av informationssäkerhetsansvarig, vilket är i enlighet med fullmäktiges beslut av policyn. Anvisningen har en regionsövergripande inriktning men har enligt informationssäkerhetsansvarig sin tyngdpunkt på patienter. Anledning är att det finns särskild registerlagstiftning att ta hänsyn till och att det är det största verksamhetsområdet. Anvisningen finns på intranätet och har ett avsnitt om skyddade personuppgifter som säger att:

- ✓ Rutiner ska finnas för olika typer av kontakt
- ✓ Tydlig märkning ska finnas
- ✓ Om IT-stöd används ska information om individens skydd från skatteverket användas
- ✓ Uppgifter om bostadsadress, hemtelefonnummer och personnummer med mera får endast utlämnas ut på patientens begäran

Anvisningen innehåller ett avsnitt om att varje nämnd och styrelse ska följa upp informationssäkerhetsarbetet. Inget specifikt framgår om hanteringen av skyddade personuppgifter ska ingå. Informationssäkerhetsansvarig

[7] Säkerhetspolicy, LS-LED17-1393-1, 2017, beslutad av Regionsfullmäktige den 26 september 2017§ 102/17, giltig från 2017-11-01
[8] Informationssäkerhetsanvisning , LS-LED17-1200-1, beslutad av informationssäkerhetsansvarig, giltig från 2017-11-01

ansvar för att sammanställa resultatet i en informationssäkerhetsberättelse och rapporteringen ska utgöra en särskild del i patentsäkerhetsberättelsen.

Anvisningen beskriver också att medarbetare ska erhålla nödvändig utbildning i informationssäkerhet. Informationssäkerhetsansvarig ansvar för att tillhandahålla utbildningar och följa upp utbildningsnivån på regionsövergripande nivå. Chef ansvarar för att medarbetare genomför utbildning och att de repeteras regelbundet.

Riktlinjer avseende åtgärder vid dataintrång[9]- styrande dokument
Riktlinjen är upprättad av juridiska staben och är beslutad av regionstyrelsen. Riktlinjen finns på externa hemsidan och på intranätet. Den anger chefs- och medarbetares ansvarar för informationssäkerhet, att endast de som är inblandade i vården får ta del av journalen, att loggningskontroller ska göras och åtgärder som ska vidtas om intrång upptäcks. I riktlinjen anges att säkerhetspolicyn gäller för all informationshantering i regionen och riktlinjen har på så vis koppling till den.

Instruktion för posthantering[10] för personer med skyddade personuppgifter från skatteverket-styrande dokument
Instruktionen är upprättad och beslutad av informationssäkerhetsansvarig och finns på intranätet. En instruktion är den lägsta nivån av tre för styrande dokument men denna instruktion har ingen koppling till de andra styrande dokumenten. Instruktionen beskriver hur det praktiskt ska gå till när post ska skickas till patienten via så kallad förmedlingsadress hos skatteverket. Dokumentet innehåller också ett avsnitt i punkform, som stöd för hur man bör göra i kontakter med den enskilde patienten och att anpassad rutin bör upprättas för detta på individnivå.

På intranätet, under hantera informationssäkerhet, finns en broschyr ”informationssäkerhet i Region Sörmland”. Den vänder sig till samtliga medarbetare och beskriver hur information ska hanteras i de daglig arbetet för att upprätta regionens informationssäkerhet. Hantering av skyddade personuppgifter nämns inte specifikt.

[9] Riktlinjer avseende avseende åtgärder vid dataintrång, LS LED11-477, beslutad av regionsstyrelsen 6 september 2011 § 155/11
[10] Posthantering för personer med skyddade personuppgifter från skatteverket, LS-LED 15-1138-1, beslutad av informationssäkerhetsansvarig, giltig från 2015-09-01

Utbildning

Enligt det styrande dokumentet informationssäkerhetsanvisning ska medarbetare genomgå utbildning i informationssäkerhet och ska också regelbundet repetera utbildningarna.

Regionen har ett IT-stöd för utbildningar och kompetenshantering där e-utbildningar finns. Enligt informationssäkerhetsansvarig finns det två e-utbildningar som ger kunskap och förståelse för hur informationssäkerhet upprätthålls. E-utbildningen informationssäkerhet är obligatorisk för alla medarbetare och e-utbildningen informationssäkerhet i vården är obligatorisk för medarbetare i hälso-och sjukvården.

Ingen av utbildningarna innehåller någon information om vad skyddade personuppgifter är och hur hantering ska ske för att undvika att de röjs.

Vår bedömning

Vid intervjun med informationssäkerhetsansvarig och på frågan hur regionen säkerställer att medarbetare utbildas om skyddade personuppgifter, var svaret att de båda utbildningarna i informationssäkerhet ger utbildning på området. Samtliga av de som har intervjuats har också svarat att regionens gemensamma e-utbildningar i informationssäkerhet innehåller information om skyddade personuppgifter. Då e-utbildningarna inte innehåller något om skyddade personuppgifter är det felaktigt, vilket gör att medarbetare inte får någon utbildning på området.

I enlighet med anvisningen görs varje år görs en uppföljning av hur många medarbetare som genomfört utbildningarna i informationssäkerhet. Resultatet presenteras i patientsäkerhetsberättelsen[11] och det framgår att de krav som sätts upp för att genomföra och repetera utbildningarna, inte nås. Åtgärder för att nå kraven framgår inte.

Anvisningen anger också informationssäkerhetsarbetet ska följas upp. Enligt informationssäkerhetsansvarig och i patientsäkerhetsberättelsen 2017[5] framgår det att uppföljning inte görs och att det pågår ett förändringarbete kring uppföljning. Planen är att nya egenkontroller och en förändrad revisionsprocess ska införas. Nya egenkontroller har tagits fram och testats och när beslut tagits ska dessa börja användas. Enligt informationssäkerhetsansvarig finns det i nuläget inte något datum för när förändringsarbetet är klart och när uppföljning ska påbörjas igen.

[11] Patientsäkerhetsberättelse 2017, LS-LED18-0779, Patientsäkerhetsenheten

Av patientsäkerhetsberättelsen framgår att när verksamheterna tidigare år skattat sin förmåga (i så kallade säkerhetsdialoger med säkerhets- och beredskapsenheten) på området kring skyddad identitet, är den god. Informationssäkerhetsansvarigs bild är att frågorna till verksamheterna ställts på en för ytlig nivå och speglar inte den verkliga förmågan. Det går samtidigt att läsa att det finns problem inom flera områden för informationssäkerhet generellt, bland annat för regler och riktlinjer.

Styrelsen och nämnder följer inte upp informationssäkerhetsarbetet.

Informationssäkerhetsansvarig bedömer att regelverk för informationssäkerhet följs av verksamheterna på en hyfsad nivå generellt sett och känner inte till att några incidenter skett där skyddade personuppgifter röjts.

Informationssäkerhetsansvarig känner inte till om det finns regelverk, hur de är utformade och hur hanteringen är på området för elever som utbildas inom Kultur och utbildning i Sörmland.

För det styrande dokumentet "Instruktion för posthantering för personer med skyddade personuppgifter från skatteverket" saknas koppling till övriga styrande dokument. På intranätet ges ingen övergripande information på en egen sida om vad skyddade personuppgifter är och vad som är viktigt att tänka på, om sökorden skyddade personuppgifter och skyddad identitet matas in. Detta försvårar möjligheten att ta del av styrande dokument och få stöd på området på ett enkelt sätt och i ett första skede. Information och styrande dokument fokuserar på hantering av patienter och det saknas till stor del för elever, medarbetare och andra som också kan ha skyddade personuppgifter.

Patienter

Av Region Sörmlands hemsida framgår det att regionen behandlar även personer vars personuppgifter är skyddade. I de fall regionen får uppgifterna från folkbokföringsregistret så bevakar regionen den enskildes intresse av att de skyddade personuppgifterna inte lämnas ut.
I de fall Region Sörmland får uppgifter från folkbokföringen finns uppgift om eventuell sekretessmarkering med. Det betyder att myndigheten bevakar den enskildes intresse av att de skyddade personuppgifterna inte lämnas ut till obehöriga[12].

[12] https://www.regionsormland.se/Webbplatsadministration/Webbplatsfunktioner/Om-Webbplatsen/Personuppgifter/Skyddade-personuppgifter/

I hälso- och sjukvården finns också krav på loggningskontroller generellt enligt patientdatalagen i syfte att kontrollera om obehöriga tagit del av patientuppgifter. Det anges också i det regionsgemensamma styrdokumentet riktlinjer avseende åtgärder vid dataintrång.

Intervju har gjorts på central nivå med förvaltningsledaren för journalhanteringssystemet, IT-förvaltning, D-data. Utifrån stickprov av verksamheter i hälso- och sjukvården har intervjuer genomförts med verksamhetschefer och medarbetare på Lindens vårdcentral och Kvinnokliniken Nyköpings lasarett. Vårdenhetschefen på Akutvårdavdelning Mälarsjukhuset har också intervjuats.

Rutiner

Enligt förvaltningsledaren finns det dokumenterade rutiner i journalsystemets rutinhandbok och i nationella Vårdhandboken på intranätet I båda handböckerna framgår det hur skyddade personuppgifter ska registreras. Rutin finns för hur och när loggningskontroller ska göras i journalsystemet generellt och för patienter med skyddade personuppgifter. Detta för att kontrollera om någon obehörig varit inne i patientjournaler.

Det finns en skriftlig instruktion för när kallelse skickas till patient med skyddad identitet, som beskriver posthantering.

Arbetsätt

Förvaltningsledaren har stöd av informationssäkerhetsansvarig i sitt arbete och får hjälp att lösa olika slags frågor.

Förvaltningsledarens bild är att medarbetarna i verksamheterna är vana att arbeta under sekretess och vet vad och hur de ska göra när de har patienter med skyddade personuppgifter. Den bilden delar också de andra medarbetarna som intervjuats.

Förvaltningsledaren beskriver det övergripande arbetssättet så här:
När en patient kommer till en klinik eller vårdcentral visar hen alltid sin legitimation. När personnumret läggs in i journalsystemet hämtas personuppgifterna från centrala folkbokföringsregistret som journalsystemet har koppling till. Om patienten har skyddade personuppgifter blir det inlagt med automatik och det blir en märkning i journalsystemet och personinformationen döljs. Märkningen gör medarbetarna uppmärksamma på att hanteringen ska ske med försiktighet så att de skyddade personuppgifterna inte riskerar att röjas. Kallelser och annan korrespondens sker sedan via instruktionen för posthantering för personer med skyddade

personuppgifter från skatteverket. Märkningen ger också en signal till medarbetare som inte har koppling till patientärendet, att inte gå in i journalen. Alla medarbetare som går in i en journal loggas. En medarbetare gör sig skyldig till dataintrång om hen går in i en patientjournal där hen inte är involverad i patientens vård. Verksamhetschefen gör loggningskontroller i journalsystemet på generell nivå och specifikt för patienter med skyddade personuppgifter.

Enligt förvaltningsledaren finns det olika behörigheter i journalsystemet och det är verksamhetschefen som bestämmer vilka behörigheter som tilldelas. Det är ett fåtal som ges behörighet att hantera skyddade personuppgifter per verksamhetschef.

De som intervjuats på verksamhetsnivå gör på liknande sätt och de arbetar som förvaltningsledaren beskriver, de gör registrering i journalsystemet enligt rutinen, loggningskontroller görs, de tar upp och diskuterar sekretess i allmänhet på personalmöten och om de skulle ha frågor på området skulle de kontakta de som arbetar med journalsystemet, juridiska staben eller säkerhets- och beredskapsenheten. Lindens vårdcentral och kvinnokliniken använder instruktionen för posthantering när de skickar kallelser med mera till patienter med skyddade personuppgifter.

På Lindens vårdcentral har de en särskild hantering för patienter med skyddade personuppgifter för att de ska känna sig trygga när de kontaktar och besöker vårdcentralen. De sätter bland annat samman ett team med så få medarbetare som möjligt runt patienten.

På kvinnokliniken förekommer det att patienter själva har valt att sekretessmarkera sin journal utan att ha skyddade personuppgifter. Då det råder sekretess på kliniken och i hälso-och sjukvården generellt är det alltid viktigt att medarbetarna tänker i sekretess-termer i kontakter när någon ringer till kliniken eller kommer på besök, enligt verksamhetschefen.

På akutvårdavdelningen kan det förekomma att patienter har behov av att skyddas på olika sätt och av olika anledningar utan att de har skyddade personuppgifter. De ges då en markering ”sekretess och upplysningsskydd” som bestäms i samråd med patienten vid inkomstsamtalet eller med till exempel polisen. Ett speciellt arbetsätt inträder i dessa fall och kliniken har en verksamhetsspecifik rutin för hanteringen i journalsystemet. Skulle vårdenhetschefen behöva information om hantering av skyddade personuppgifter skulle hen söka på intranätet efter rutinen för journalsystemet eller kontakta.

Introduktion och utbildning

Samtliga som intervjuats anger att utbildning som ges är de regionsgemensamma e-utbildningarna om informationssäkerhet och informationssäkerhet i vården.

Vår bedömning

I granskningen av verksamheterna har det framkommit att det enbart är Lindens vårdcentral som uppger att de har erfarenhet av att hantera skyddade personuppgifter. På kvinnokliniken och akutvårdsavdelningen är det ovanligt och man har därför inte så stor erfarenhet på området. Däremot förekommer det att de har patienter med andra typer av skydd och som behöver särskild hantering på ungefär samma sätt som patienter med skyddade personuppgifter.

Den samlade bedömningen är att hälso-och sjukvården i nuläget delvis säkerställer att hanteringen av skyddade personuppgifter för patienter är ändamålsenlig och sker med god intern kontroll.

Vi ser positivt på att det finns rutiner för flera områden. Rutinerna säkerställer att registrering i journalsystemet görs så att märkning finns, få har behörighet och att loggningskontroller utförs på rätt sätt och att kallelser skickas enligt instruktionen för posthantering. Samtliga delar är i enlighet med de regionsgemensamma styrdokumenten för posthantering och informationssäkerhetsanvisningen. I verksamheterna arbetar man under sekretess och har en generell kunskap, erfarenhet och medvetenhet.

Lindens vårdcentral och kvinnokliniken känner inte till de regionsövergripande styrdokumenten säkerhetspolicy och säkerhetsanvisningen. Akutvårdsavdelningen uppger att de vet att de finns och att de går att hitta på intranätet. Ingen av de intervjuade nämner skatteverkets vägledning. För att säkerställa att skyddade personuppgifter inte röjs, behövs ytterligare verksamhetsspecifika dokumenterade rutiner som beskriver hur hantering, arbetsätt, kommunikation med mera ska ske. Då e-utbildningar informationssäkerhet och informationssäkerhet i vården inte innehåller något avsnitt om skyddade personuppgifter, finns ingen utbildning på området.

I granskningen har det framkommit att verksamheterna anser att det är viktigt att alla arbetar på samma sätt med hanteringen av sekretess och med skyddade personuppgifter. De saknar en gemensam rutin eller ett

”grundläggande stödmaterial” att ha som vägledning vid behov, och som beskriver praktiskt arbetssätt och hantering med mera.

Patientnämnden

Patientnämndens kansli arbetar på patientnämnden uppdrag och handlägger synpunkter och klagomål från patienter och närstående på hälso- och sjukvård och tandvård inom offentlig finansierad verksamhet i Region Sörmland och i länets nio kommuner Eskilstuna, Flen, Gnesta, Katrineholm, Nyköping, Oxelösund, Strängnäs, Trosa och Vingåker.

Intervju har genomförts med enhetschefen för patientnämndens kansli.

Skriftliga rutiner

Det finns inga verksamhetsspecifika skriftliga rutiner.

Arbetsätt

När en patient anmäler ett klagomålsärende kan patienten ange sina personuppgifter eller vara anonym. Anmälan kan göras muntligt, skriftligt eller via e-tjänsten 1177 vårdguiden och att patienten anger sina personuppgifter. Via e-tjänsten fungerar det inte att vara anonym.

Kansliet har ett eget IT-system, ett diarie- och verksamhetssystem, som de anställda på kansliet har behörighet till och arbetar i. Behörigheten är inte styrd utan samtliga fyra anställda har tillgång till samma uppgifter eftersom de har behov av att kunna arbeta gå in för varandra i ärenden, om någon är frånvarande.

I IT-systemet finns ingen möjlighet att märka personuppgifter om en patient har skyddade personuppgifter. Det är ovanligt att kansliet får in klagomål från personer med skyddade personuppgifter och enligt enhetschefen har det under ett de senaste 15 åren inträffat endast ett fåtal gånger. Klagomålet har i dessa fall registrerats i IT-systemet med en notering om att patienten har skyddade personuppgifter

Om en patient väljer att anmäla klagomålet anonymt handläggs ärendet och förs fram till verksamheten som det avser, på en generell nivå. I de fall där klagomålet ska till vården och utredas och sedan besvaras skriftligt, begär kansliet alltid in en blankett ”Synpunkter/klagomål till patientnämnden”, innan handläggningen påbörjas. Patienten ger där sitt samtyckte till att patientnämnden får behandla de personuppgifter och handlingar som avser patienten och som hör till klagomålet.

Enhetschefen anser att det finns en medvetenhet och kunskap på kansliet om personuppgifter och sekretess, och att man aldrig använder personuppgifter i onödan. Kansliet arbete sker enbart inom regionens och kommunernas verksamheter för hälso- och sjukvård, och svar på klagomål begärs alltid från verksamhetschef. När återrapportering och uppföljning görs av klagomålsärenden till nämnden eller till externa parter förekommer aldrig personuppgifter. När verksamheten fått klagomålet för utredning och begäran om yttrande har hälso- och sjukvårdens sekretess trätt in.

Utbildning
Nya medarbetare tar del av regionens gemensamma e-utbildningar informationssäkerhet och informationssäkerhet i vården.

Vår bedömning
Risken för att skyddade personuppgifter skulle kunna röjas bedöms som låg. Den samlade bedömningen är att patientnämnden kansli i nuläget ändå inte säkerställer en helt tillfredställande hantering av skyddade personuppgifter för patienter.

Det är positivt att möjlighet finns att anmäla klagomål anonymt. Patienten ger sitt skriftliga samtycke innan handläggning påbörjas. Klagomålen utreds och besvaras av verksamheterna och då träder hälso-och sjukvårdens sekretess in. Det är få medarbetare som arbetar på kansliet och de arbetar gemensamt. Patientnämndens kansli har ett eget IT-system med få användare.

Vi har identifierat brister på några områden:
Enhetschefen har inte kännedom om de regionsgemensamma styrande dokumenten. Det finns inga verksamhetsspecifika skriftliga rutiner för hantering och arbetsätt. Det är enbart möjligt att göra en notering i IT-systemet, det görs ingen märkning. Det görs ingen uppföljning på området. Vi har inte tagit del av om det går att göra loggningskontroller i IT-systemet och om det i så fall görs.

Under vår granskning har det framkommit att informationen om att det är möjligt att lämna klagomål/synpunkter anonymt, inte alltid framgår i informationsmaterial som finns i skriftlig och digital form.

Elever

Datainspektionen har en "checklista för skolor-skyddade personuppgifter i skola"[13]. I checklistan skriver datainspektionen att allt fler får skyddade personuppgifter vilket innebär att många skolor kommer att ha eller har barn och elever med skyddade personuppgifter i sin verksamhet. Att behandla dessa elevers personuppgifter ställer extra stora krav på den personuppgift-sansvarige i och med att behandlingen måste ske på ett sätt som inte ger upphov till svåra konsekvenser för de berörda registrerade. Checklistan är tänkt som en hjälp för den personuppgiftsansvarige som måste hantera skyddade personuppgifter på sin skola. Datainspektionen anger ett antal områden som skolor bör beakta när det gäller skyddade personuppgifter:

- ✓ Regler och rutiner ska finnas och ska vara skriftliga
- ✓ Riskbedömning ska göras från fall till fall
- ✓ Begränsa mängden uppgifter
- ✓ Begränsa åtkomsten
- ✓ Det ska framgå att personuppgifterna är skyddade
- ✓ Undvik spridning av uppgifterna i IT-systemen
- ✓ Informera och utbilda personalen
- ✓ Tillräckligt hög IT-säkerhet ska finnas
- ✓ Gör det möjligt att kontrollera åtkomsten
- ✓ Följ regelbundet upp rutinerna

Skolverket har ett stödmaterial där de ger praktiska råd till verksamheter som arbetar med barn och ungdomar som har skyddade personuppgifter.

Datainspektionens och skolverkets material liknar varandra och de områdena de tar upp har även skatteverket med i sin vägledning.

Intervjuer har genomförts med regionens verksamheter som har elever, med rektorer och medarbetare på gymnasieskolan Ökna, Åsa folkhögskola, Eskilstuna folkhögskola och ekonomi- och stabschefen för kultur och utbildning. Verksamheterna är organiserade i kultur och utbildning. Verksamhetschefen för Dammsdals skola och boende har också intervjuats. Dammsdal är en grundsär/grundskola, träningsskola samt gymnasiesär/gymnasieskola och är vid tidpunkten för vår granskning organiserad i Division psykiatri/funktionshinder i hälso- och sjukvården.

På Öknaskolan och Dammsdalskolan kan det förekomma att skolan behöver hantera skyddade personuppgifter för vårdnadshavare (till elever som är

[13] https://www.datainspektionen.se/globalassets/dokument/gammalt/skyddade-personuppgifter-i-skolan.pdf

under 18 år) som har skyddade personuppgifter. Den hanteringen ingår inte i granskningen.

Skriftliga rutiner

Enligt ekonom- och stabschef finns inga dokumenterade rutiner som är gemensamma för hantering av skyddade personuppgifter för elever i Kultur och utbildning i Sörmland.

Alla verksamheter har skriftliga rutiner från programleverantören för hantering av elever med skyddade personuppgifter, till de elevregistreringsprogram de har. Dammsdalskolan använder också vårdens journalsystem och det finns en rutinhandbok som beskriver hur registrering ska göras.

Öknaskolan har en skriftlig rutin som är kortfattad och som omfattar delar av området. Öknaskolan och Eskilstuna folkhögskola har också GDPR-rutiner som beskriver hanteringen av personuppgifter generellt.

Dammsdalskolan har en checklista som kan jämställas med en skriftlig rutin för hur man ska gå till väga i olika situationer som har med en elev att göra.

Arbetssätt

Öknaskolan och folkhögskolornas arbetsätt på området liknar varandra och verksamheterna registrerar elever med skyddade personuppgifter på ett speciellt sätt enligt rutinen från respektive programleverantör. Eleven får en särskild märkning och ”döljs”. Det är få medarbetare som har behörighet att göra registreringen och det är bara de som sedan kan se elevens identitet.

Skolorna beskriver att de har arbetsätt som träder in när en elev med skyddade personuppgifter går på skolan. Det finns inga dokumenterade rutiner som beskriver arbetssättet men man återger att man är väl medvetna om att hanteringen ska ske med största försiktighet och att medarbetare har kännedom om hur de ska göra för att förhindra att skyddade personuppgifter röjs. GDPR och personuppgiftshantering generellt tas upp på personalmöten och deras bedömning är att medarbetarna har koll på vad som gäller, eller vet var de kan ställa frågor som rör skyddade personuppgifter.

De medarbetare som är inblandade i elevens skolgång får information och löser tillsammans hur hanteringen runt eleven ska skötas. Öknaskolan uppger att man tar fram en handlingsplan som rektor ansvarar för. Eleven är delaktig i processen på skolorna.

På Åsa folkhögskola har den administrativa personalen som ansvarar för hantering av personuppgifter, löpande haft uppföljningar med den aktuella personalgruppen, då det varit aktuellt med elever som haft skyddade personuppgifter.

På Dammsdalskolan har man i närtid inte haft någon elev med skyddade personuppgifter. Enligt verksamhetschefen skulle hen få information först och informera berörda medarbetare och chefer om detta och hur det skulle hanteras. Checklistan skulle finnas som stöd i arbetet. Varje månad gör verksamhetschefen och två medarbetare loggningskontroller i journalsystemet, för att se vem eller vilka som varit inne i elevers journaler.

Dammsdalskolan har hittills inte gjort andra uppföljningar på området då de inte haft något att följa upp. Verksamhetschefens bedömning är att risken för att skyddade personuppgifter skulle kunna röjas är liten. Anledningar till detta är att skolan endast har 38 elever som ofta stannar i flera år och personalomsättningen är låg.

Utbildning

Alla verksamheterna uppger att medarbetare och chefer tar del av de regionsgemensamma e-utbildningarna i informationssäkerhet. På Dammsdalskolan genomgår de också e-utbildningen informationssäkerhet i vården.

Öknaskolan uppger att det pågår ett arbete med att ta fram ett introduktionsmaterial och en personalhandbok. Där kommer det att finnas en punkt som beskriver hur hanteringen sker för elever och vårdnadshavare som har skyddade personuppgifter. Utbildning och introduktion på området sker idag muntligt.

Folkhögskolorna har en checklista som används vid introduktion av nyanställda medarbetare och chefer. Ett moment är information och utbildning om sekretess och tystnadsplikt. Det framgår inte om skyddade personuppgifter specifikt ingår i den genomgången.

På Dammsdalskolan får nyanställda medarbetare en introduktion inom sekretess-området och skyddade personuppgifter ingår då.

Vår bedömning

I granskningen har det framkommit att det är ovanligt att elever har skyddade personuppgifter.

Handläggare
Åsa Forsman

Datum
2019-01-24

Dokumentnummer
RE-REV19-0003

Vår bedömning är att Dammsdalskolan säkerställer att hanteringen av skyddade personuppgifter är ändamålsenlig och bedrivs med god intern kontroll. De har kännedom om de regionsövergripande styrdokumenten. Checklistan som finns beskriver tydligt hur man ska gå till väga i olika situationer som har med eleven att göra, det finns rutiner för hantering i IT-systemen som få har tillgång till, vilket minskar risken för att skyddade personuppgifter skulle kunna röjas. Rutinhandboken följs vid registreringen i journalsystemet och loggkontroller utförs enligt gällande rutin vilket innebär att man skulle upptäcka om obehöriga tagit del av journalen. Utbildning ges på området. Samtliga moment överensstämmer med styrdokumenten, skatteverkets och datainspektionens vägledningar.

Den samlade bedömningen är att Kultur och utbildning i nuläget inte säkerställer en helt tillfredställande hantering av skyddade personuppgifter för elever.

Folkhögskolorna och Öknaskolan har en skriftlig rutin i registreringsprogrammet, det blir en märkning och få medarbetare har behörighet till programmet. Hantering och/eller handlingsplan med mera tas fram av skolornas medarbetare/rektor i dialog med eleven. Samtliga delar är i enlighet med det styrande dokumentet säkerhetsanvisningen, skatteverkets och datainspektionens vägledningar. Det finns en kunskap, erfarenhet och medvetenhet på skolorna på området och uppföljning har gjort av hanteringen på Åsa folkhögskola. Alla dessa delar är positiva.

De regionsövergripande styrdokumenten är inte specifikt kända. Det saknas dokumenterade rutiner som beskriver hur hantering, arbetsätt, kommunikation med mera ska ske för att undvika att skyddade personuppgifter röjs. Av Eskilstuna folkhögskola och Öknaskolans svar framgår det inte om någon uppföljning skett av samma typ som på Åsa folkhögskola. Vi har inte tagit del av att loggningskontroller utförs i elevregistreringsprogrammen för att följa upp om obehöriga försökt komma åt uppgifter.

Medarbetare

Region Sörmland har cirka 8 000 medarbetare och de kan finnas medarbetare som har skyddade personuppgifter i alla delar av organisationen.

Region omfattas av offentlighetsprincipen, vilket innebär att uppgifter om medarbetare kan komma att lämnas ut om någon begär det. Uppgifter som omfattas av sekretess enligt lag får dock inte lämnas ut.

Enligt chefsjuristen på juridiska staben är uppgifter om namn på de som är anställda hos regionen offentliga. Namnen kan inte sekretessbeläggas och rimligen inte heller var man arbetar, såvida inte sekretess råder på grund av skyddade personuppgifter. Enligt offentlighets- och sekretessförordningen omfattas däremot medarbetare i hälso-och sjukvården av sekretess när det gäller hemadress, hemtelefonnummer och personnummer.

Enligt skatteverkets vägledning är uppgift om arbetsplats en uppgift som ska skyddas för en person som har skyddade personuppgifter för att inte röja var personen befinner sig.

Nedan presenteras resultatet av intervjuer för hantering av skyddade personuppgifter för medarbetare på central nivå och på verksamhetsnivå var för sig. Rekommendationer ges gemensamt i den avslutande textdelen.

Central nivå

Intervjuer har gjorts med enhetschefen för chefsstöd i HR-staben, förvaltningsledare HR-staben, lönechef, förvaltningsledare, IT-förvaltningen, D-data och teamledaren för telefonväxeln.

Skriftliga rutiner

Vid intervjuer har det framkommit att regionens styrande dokument inte är kända. Några av de intervjuade känner till skatteverkets vägledning och har tagit del och stöd av den när behov funnits. Det finns dokumenterade rutiner för hantering av skyddade personuppgifter på områdena för:

- ✓ jobbansökan
- ✓ personaladministrativa systemet (hur markering/märkning sker och hur integrering med centrala befolkningsregistret (CBR) från skatteverket)
- ✓ praktisk hantering i HR-staben vid begäran om uppgifter och vanliga förfrågningar (om anställda från externa parter, till exempel löneuppgifter)

- ✓ elektronisk katalog för information om medarbetare och organisation
- ✓ information till medarbetare om regionens hantering av personuppgifter

Rutiner för det personaladministrativa systemet finns på intranätet. Övriga rutiner finns hos respektive verksamhet.

Arbetsätt

Om en person med skyddade personuppgifter söker jobb i Region Sörmland sker det inte i IT-systemet för rekrytering utan i pappersform och hanteras manuellt. Personen får information om hur regionen hanterar ansökan och personuppgifter.

Ett fåtal medarbetare har behörighet i det personaladministrativa systemet för att hantera registrering av medarbetare med skyddade personuppgifter. Registrering görs enligt rutinen och all personinformation döljs och det blir en märkning i systemet. Medarbetaren informeras om regionens hantering av personuppgifter enligt den skriftliga rutinen. Man kommer överens med medarbetaren om hur till exempel lönespecifikationen ska hanteras. Lönechefens bild är att när en medarbetare har en markering i systemet så hanterar alla på personalservice uppgifterna med stor varsamhet.

När det kommer förfrågan om att ta del av uppgifter om medarbetare, till exempel lönelistor, följer HR rutinen som finns. Märkningen i det personaladministrativa systemet gör att medarbetare med skyddade personuppgifter inte kommer med. Vid tveksamheter om uppgifter ska lämnas ut tar HR stöd av juridiska staben.

Regionen har en elektronisk katalog. Syftet med katalogen är att samla all information om organisation och anställda på ett ställe och göra den tillgänglig för användare och system inom regionen (och även nationellt via HSA-samarbetet[14]). I elektroniska katalogen finns information om kontaktinformation till anställda, organisationstillhörighet och uppgifter om hemadress med mera som hämtas från det centrala folkbokföringsregistret. Uppgifterna om hemadress med mera är normalt offentliga men regionen har valt att hantera dem med stor försiktighet för samtliga medarbetare och

[14] Nationell katalogtjänst som är ett nationellt samarbete kring katalog och katalogtjänster. Den möjliggör att personal och invånare säkert, enkelt och effektivt kan hitta och hämta kvalitetssäkrad information såväl inom den egna organisationen som i andra HSA-anslutna organisationer.

de visas bara för administratörerna som har behörighet att hantera uppgifter i katalogen.

Uppgifterna i katalogen används för att ge tillgång till system, passerkort och för att kunna logga in på regionens datorer. Anställda i regionens organisation kan söka i katalogen och få del av den arbetsrelaterade informationen om en medarbetare.

Medarbetare med skyddade personuppgifter registreras enligt rutinen och förses med en särskild markering som gör att hemadress med mera döljs. Informationen kan sedan bara ses av ett fåtal personer på centrala katalogförvaltningen. Katalogen kompletteras med arbetsrelaterade uppgifter (titel, telefonnummer, e-postadress, arbetsplats med mera). Enligt strukturen i katalogen kopplas medarbetaren till den organisation hen tillhör. Enligt förvaltningsledaren är det möjligt att en medarbetare kan komma överens med sin katalogadministratör att uppgifter om arbetsplats och besöksadress ska döljas och inte framgå vid en sökning. Uppgiften om organisationstillhörighet är obligatorisk och går inte att dölja, vilket gör att arbetsplats indirekt framgår vid sökning.

Den skriftliga rutinen med information till medarbetare beskriver att medarbetare som har skyddade personuppgifter har rätt att, under vissa förhållanden, välja att inte registreras i katalogen. Detta kan dock medföra begränsningar beroende på vilka IT-system med mera personen behöver ha tillgång till i sitt arbete.

Är en medarbetares uppgifter märkta i den eletroniska katalogen och uppgifterna går vidare till den nationella HSA-katalogtjänsten, får de med automatik en markering där som gör att hen inte blir synlig/sökbar där. Samma sak gäller för e-tjänstekorten (SITHS-kort).

Regionens centrala växel tar emot samtal och kopplar vidare till medarbetare direkt eller till mottagning/verksamhet där medarbetare arbetar. Växeln har en egen telefonkatalog som D-data ansvarar för. I telefonkatalogen finns uppgifter om telefonanknytning, mobiltelefonnummer, titel och arbetsplats. Uppgifterna har ingen koppling till den elektroniska katalogen utan kommer till D-data från medarbetaren själv, från administratör eller ansvarig chef. Alla medarbetare finns inte i telefonkatalogen. De som saknas är främst de som inte har en egen telefonanknytning.

Teamledaren uppger att växeln får lämna ut de uppgifter som står i telefonkatalogen. Mobiltelefonnummer och anknytning kan vara överstrukna och det innebär att växeln inte får lämna ut dem. Teamledaren

uppger att uppgifter om arbetsplats inte går att stryka över. Växeln har inte vetskap om någon medarbetare har skyddad identitet och kan därmed inte i nuläget markera det på något sätt i telefonkatalogen. Om växeln inte hittar den information som efterfrågas i telefonkatalogen, till exempel uppgifter om telefonnummer eller arbetsplats söker de alltid efter uppgifterna i den elektroniska katalogen.

Utbildning

Personalservice utbildar chefer och administratörer i det personaladministrativa systemet och enligt lönechefen nämns då inget om skyddade personuppgifter. Nyanställda chefer genomgår utbildning på HR-området men enligt enhetschefen för chefsstöd ingår inte området hantering av skyddade personuppgifter.

När centrala katalogförvaltningen utbildar administratörer i den elektroniska katalogen ingår en kort muntlig information om skyddade personuppgifter. Enligt teamledaren för växeln genomgår och repeterar medarbetarna e-utbildningen om informationssäkerhet ingen information eller utbildning om skyddade personuppgifter ges.

Vår bedömning

Vi ser positivt på att det finns rutiner för flera områden. Rutinerna säkerställer att olika typer av registrering i det personaladministrativa systemet och den elektroniska katalogen görs, så att märkning finns. På nationell nivå i HSA och för e-tjänstekort (SITHS-kort) blir det också en märkning som gör att medarbetaren inte är synlig/sökbar. Märkning är ett krav i det styrande dokumentet informationssäkerhetsanvisning och en rekommendation enligt skatteverkets vägledning. Märkningar minskar risken att skyddade personuppgifter inte röjs. Behörigheter har begränsats till ett fåtal medarbetare att hantera och ta del av skyddade personuppgifter vilket också är positivt.

I granskningen har det framkommit flera brister:
De regionsövergripande styrande dokumenten är okända. I dokumenten framgår inte tydligt vad som gäller för hanteringen av medarbetare med skyddade personuppgifter.
Det saknas skriftliga rutiner för flera områden, bland annat för växeln och telefonkatalogen. Det saknas också information som stöd för chefer som beskriver hantering i det vardagliga arbetet med mera.

Ingen av de som intervjuats i granskningen har kunnat svara på vad som gäller om någon ringer till växeln (eller till någon annan medarbetare) och

frågar om en medarbetare arbetar i Region Sörmland och på vilken arbetsplats, och om informationen ska lämnas ut eller inte. Enligt skatteverkets vägledning är uppgift om arbetsplats en uppgift som ska skyddas för en person som har skyddade personuppgifter. Det framgår inte tydligt i de regionsövergripande styrande dokumenten.

Växeln har ingen en rutin som beskriver vilka uppgifter som får lämnas ut om medarbetare och hur växeln ska hantera information som finns i telefonkatalogen respektive i den elektroniska katalogen. De har inte information om vilka medarbetare som eventuellt har skyddad identitet. Det finns därmed en risk att uppgift om till exempel arbetsplats och namn röjs vilket kan få konsekvenser för en medarbetare som kan vara utsatt för hot.

Medarbetare som har skyddad identitet får inte information om att växeln lämnar ut uppgifter om arbetsplats i det material de får från centrala katalogförvaltningen om hur personuppgifter behandlas. Även om medarbetaren har gjort ett aktivt val att inte finnas med i telefonkatalogen eller valt att dölja uppgifter om arbetsplatsens besöksadress, finns alltid uppgifterna om organisationstillhörighet i den elektroniska katalogen. Den har växeln och samtliga medarbetare tillgång till vilket gör att risk finns att uppgifter om namn och arbetsplats röjs.

Verksamhetsnivå

Intervjuer har genomförts med verksamhetschefer och medarbetare på Lindens vårdcentral, kvinnokliniken, Nyköpings lasarett, akuten Mälarsjukhuset, Öknaskolan, Åsa folkhögskola, Eskilstuna folkhögskola och Dammsdalskolan

Skriftliga rutiner

Öknaskolan har en rutin som är kortfattad och omfattar delar av området. Dammsdalskolan har dokumenterade rutiner som beskriver hur praktisk hantering på arbetsplatsen, och i det dagliga arbetet, skulle gå till om medarbetare med skyddade personuppgifter arbetade där. Övriga verksamheter som intervjuats har inga dokumenterade rutiner.

Arbetsätt

Samtliga som intervjuats uppger att det är ovanligt med medarbetare som har skyddade personuppgifter. De har därför ingen eller lite erfarenhet på området. De uppger att det finns en stor medvetenhet på området generellt sett och anser att risken är mycket liten att identiteten skulle kunna röjas om en medarbetare hade skyddade personuppgifter. I verksamheterna är man van vid att arbeta med sekretess med mera i det dagliga arbetet med

patienter och elever, och det finns viss erfarenhet på området för patienter och elever som kan ha skyddade personuppgifter.

Flera av verksamheterna uppger också att de följer GDPR och personuppgifter lämnas inte ut till obehöriga. Sekretess och hantering av personuppgifter är något som ibland tas upp på arbetsplatsträffar med mera även om det då inte specifikt handlar om skyddade personuppgifter.

De flesta skulle vända sig till HR eller juridiska staben för att få stöd och kunskap på området för att göra rätt. Flera av de intervjuade önskar lättillgänglig övergripande information på intranätet och gemensamma rutiner att ha som grund för den praktiska hanteringen.

Utbildning

Samtliga som intervjuats anger att utbildning som ges är regionens gemensamma e-utbildningar om informationssäkerhet och informationssäkerhet i vården.

Vår bedömning

Det är svårt att bedöma hanteringen av skyddade personuppgifter för medarbetare i verksamheterna, då de som intervjuats uppger att det är ovanligt och att det finns lite erfarenhet på området.

Den samlade bedömningen är att Region Sörmland i nuläget inte säkerställer en helt tillfredställande hantering av skyddade personuppgifter för medarbetare.

Det är positivt att flera av verksamhetscheferna känner till och uppger att de vid behov skulle använda de gemensamma rutinerna för det personaladministrativa systemet. Lindens vårdcentral uppger att de skulle använda sig av rutinerna för den elektroniska katalogen.

Dammsdalskolan har en checklista som tydligt beskriver hanteringen av skyddade personuppgifter. De har även uppdaterat checklistan i samband med granskningen så det framgår hur man ska gå tillväga om någon kontaktar skolan och frågar efter en medarbetare
Vi har identifierat brister på flera områden:
De regionsövergripande styrdokumenten är inte specifikt kända förutom på Dammsdalskolan och på akutkliniken. I styrdokumenten framgår inte tydligt vad som gäller för hantering av medarbetare med skyddade personuppgifter. Styrdokumenten anger att verksamhetsspecifika instruktioner ska tas fram, vilket bara skett på Dammsdalskolan av de

verksamheter som ingått i granskningen. Öknaskolans rutin är kortfattad och beskriver inte alla områden för hantering av skyddade personuppgifter. Ingen av de intervjuade nämner skatteverkets vägledning vilket kan tolkas som att den inte är känd.

På Öknaskolan har inte alla medarbetare tillgång till intranätet vilket man anger som en risk. Alla medarbetare kan då inte få tillgång till nödvändig information.

Revisionen

Åsa Forsman
Sakkunnig revisor