Region Skåne
Området för strategisk krisberedskap, säkerhet och miljöledning

Mats Persson
Informationssäkerhetschef
Mats.E.Persson@skane.se

BESLUT

Datum: 2021-10-25
Dnr: 2021-O002308

Instruktion åtgärder vid misstanke om dataintrång avseende patientuppgifter

Patientinformation är mycket känslig och skyddas av stark sekretess. Genom att ge medarbetare tillgång till känslig sekretesskyddad information såsom patientuppgifter, har Region Skåne visat ett särskilt förtroende för berörda medarbetare. Vid misstanke om att en medarbetare olovligen berett sig tillgång till uppgifter om patienter ska detta utredas skyndsamt och hanteras enligt bilagd instruktion. I samråd med hälso- och sjukvårdsdirektör Pia Lundbom och tf HR-direktör Vivianne Sahlin fattar informationssäkerhetschefen härmed beslut om att:

- Bifogat underlag " Instruktion åtgärder vid misstanke om dataintrång avseende patientuppgifter" fastställs.
- Beslut om "Dataintrång - åtgärder vid misstanke om olovlig åtkomst", daterad 2013-10-09 upphör att gälla.

Mats Persson
Informationssäkerhetschef

Region Skåne
Området för strategisk krisberedskap, säkerhet och miljöledning

Malin Nyman
Informationssäkerhetsspecialist
Malin.Nyman@skane.se

Instruktion

Datum: 2021-10-22
Dnr: 2021-O002308

Instruktion åtgärder vid misstanke om dataintrång avseende patientuppgifter

1 Bakgrund

1.1 Dataintrång

Dataintrång är ett samlingsbegrepp för ett stort antal gärningar, som alla har gemensamt att någon olovligen bereder sig tillgång till en uppgift i ett IT-system. Om någon olovligen till exempel har berett sig tillgång till patientuppgifter kan denne dömas för dataintrång.

4 kap 9 c § första stycket brottsbalken (1962:700):

”Den som olovligen bereder sig tillgång till en uppgift som är avsedd för automatiserad behandling eller olovligen ändrar, utplånar, blockerar eller i register för in en sådan uppgift döms för dataintrång till böter eller fängelse i högst två år. Detsamma gäller den som olovligen genom någon annan liknande åtgärd allvarligt stör eller hindrar användningen av en sådan uppgift.”

Brottsbalkens bestämmelse om dataintrång omfattar alla typer av uppgifter som är avsedda för automatiserad behandling. Så kallad hacking, spridande av virus och överbelastningsattacker är exempel på handlingar som utgör brott enligt paragrafen om dataintrång. Det är också olagligt att ge sig själv tillgång till information som är lagrad digitalt och som tillhör någon annan. Anställda som har tillgång till dataregister i tjänsten får inte göra slagningar på

personer vars ärende de inte handlägger. I Region Skåne är patientuppgifter mest förekommande, varför instruktionen hanterar just misstanke om dataintrång avseende patientuppgifter. Utredning av andra typer av intrång kan se olika ut beroende på vilken typ av dataintrång som misstänks. Om intrånget misstänks vara en hacker-, cyber- eller överbelastningsattack ska Servicedesk alltid kontaktas omgående.

2 Omfattning

Denna instruktion innehåller:

- allmän beskrivning av dataintrång
- beskrivning av det särskilda regelverket för anställdas åtkomst till patientuppgifter
- rutin för utredning vid misstanke om dataintrång avseende patientuppgifter
- åtgärder om utredning visar fortsatt misstanke
- vägledning beträffande arbetsrättsliga åtgärder i samband med utredning

3 Regelverk för anställdas åtkomst till patientuppgifter

Patientdatalagen (2008:355), PDL, och Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLF-FS 2016:40) reglerar personuppgiftsbehandling och hälso- och sjukvårdspersonals åtkomst till uppgifter om patienter. För åtkomst till patientuppgifter i elektroniska journalsystem krävs dels att medarbetaren fått särskild tilldelad möjlighet till åtkomst samt att medarbetaren har en laglig grund för att bereda sig åtkomst. Verksamhetschefen är ansvarig för att varje medarbetares behov och tillgång till uppgifter kontrolleras och att lämplig behörighet tilldelas[1]. Med medarbetare avses i instruktionen en person som är anställd i Region Skåne.

3.1 Inre sekretess

All vård och behandling som bedrivs av Region Skåne utgör ett och samma sekretessområde. För att ha rätt att ta del av patientuppgifter inom sekretessområdet måste personen arbeta hos vårdgivaren. Medarbetaren måste även delta i vården av patienten eller av annat skäl behöva uppgifterna för sitt arbete inom hälso- och sjukvården. Uppfylls dessa krav får medarbetaren enligt patientdatalagen ta del av uppgifterna.

Om inte medarbetaren deltar i vården av en patient eller har annan arbetsuppgift som kräver tillgång till patientuppgifter är det alltså inte tillåtet att ta del av dessa. Att exempelvis ta del av patientuppgifter enbart i utbildningssyfte är inte tillåtet. Regelverket gäller även för exempelvis medarbetarens närståendes patientjournaler. En medarbetare får inte lagligen ta del av närståendes patientuppgifter genom sin behörighet, om inte det finns en vårdrelation eller annan arbetsuppgift med patienten (den närstående). Medarbetare har inte heller rätt att ta del av sina egna patientuppgifter genom att utnyttja sin yrkesmässiga behörighet till IT-systemet. Undantag kan finnas för medarbetare som behandlar sig själva eller förskriver läkemedel till sig själva. Medarbetaren som väljer att logga in och ta del av patientuppgifter är

[1] Instruktioner om styrning av behörigheter för åtkomst till uppgifter om patienter, 2019-03-08, Dnr: 1800025

personligen ansvarig för att vederbörande verkligen har rätt att göra det.

3.2 Sammanhållen journalföring

Sammanhållen journalföring är en möjlighet för vårdgivare (exempelvis Region Skåne) att vid behov ta del av en patients journal hos andra vårdgivare via ett IT-system. För att åtkomsten ska vara tillåten finns tre kriterier som måste vara uppfyllda; personalen ska ha en aktuell vårdrelation, patientuppgifterna ska antas ha betydelse för vården och patienten måste samtycka till personuppgiftsbehandlingen. Samtycke kan även ges i förväg för planerade och konkreta vårdsituationer. Exempel på sådana situationer är remisser och samordnad vårdplanering. Samtycket ska dokumenteras i patientens journal, så att det går att spåra i efterhand. Det bör även framgå hur och när patienten har samtyckt. Verksamhetschefen ansvarar för medarbetarnas behörighetstilldelning även vid sammanhållen journalföring.

3.3 Loggkontroller

Verksamhetschefen ansvarar för att anställdas åtkomst till patientuppgifter följs upp, vilket även omfattar kontroll av åtkomst till andra vårdgivares patientuppgifter. Uppföljningen sker via loggkontroller enligt särskilda instruktioner[2].

3.4 Information till personal

Det är viktigt att chefer inom vården informerar sina medarbetare om de regler som styr tillgången till patientjournaler och annan vårdinformation. Ansvarig chef ska även informera att om medarbetaren olovligen bereder sig tillgång till patientuppgifter kan det leda till polisanmälan samt arbetsrättsliga åtgärder, ytterst att anställningen i Region Skåne upphör. Information riktad till medarbetare finns på intranätet, även i utskriftvänlig version. Den som tillhör hälso- och sjukvårdspersonalen bär enligt 6 kap. 2 § patientsäkerhetslagen (2010:659), PSL, själv ansvaret för hur han eller hon fullgör sina arbetsuppgifter.

4 Rutin för utredning vid misstanke om dataintrång avseende patientuppgifter

Misstanke om att en medarbetare olovligen berett sig tillgång till patientuppgifter uppstår oftast i samband med så kallade stickprovskontroller eller riktade kontroller som görs i verksamheten. Vid kontrollerna granskas medarbetarens logg för åtkomst till patientuppgifter i systemen eller vilka medarbetare som varit inne i en viss patients journal. Riktad kontroll är specifik mot viss patient eller anställd och kan vara föranledd av en särskild händelse, exempelvis på grund av att en allmänt känd person vårdats på enheten, en ovanlig diagnos eller efter misstanke från patient. Misstanke kan även uppstå genom automatiserade kontroller och logganalysverktyg där systemet enligt vissa parametrar signalerar för åtkomst som kan vara olovlig.

[2] Instruktioner om loggkontroll för granskning av åtkomst till patientuppgifter, 2019-11-12, Dnr: 1800025

Om misstanke gäller dataintrång i en journal som är för en patient med skyddade personuppgifter, är det viktigt att patienten informeras *snarast*, för att ge vederbörande möjlighet att agera utifrån det inträffade.

4.1 Intern utredning

Vid misstanke om att en medarbetare olovligen berett sig tillgång till uppgifter om patienter ska detta utredas skyndsamt enligt följande rutin:

Verksamhetschef på den vårdenhet där den misstänkte är anställd ska kontaktas. Den som leder utredningen ska vara opartisk. Om verksamhetschefen på något sätt är involverad i ärendet ska istället dennes chef kontaktas.

Underlag ska säkerställas i loggar från IT-systemet på en sådan detaljnivå att det går att utläsa i vilken omfattning åtkomst skett, vilka åtgärder som vidtagits med uppgifterna, vilken information åtkomsten rör, vid vilken vårdenhet och tidpunkt detta skett, identitet på involverad vårdpersonal och patient. Loggutdraget ska begränsas att endast innehålla uppgifter som rör det specifika ärendet. Loggutdrag kan tas fram av behörig person i verksamheten eller beställas via Enheten för journal- och arkivservice.

Verksamhetschef, eller den person verksamhetschefen utser, ska skyndsamt informera förvaltningens HR-funktion och informationssäkerhetsamordnare om händelsen. Dessa roller kan också vara stödjande i den fortsatta utredningen. Förvaltningens dataskyddssamordnare informeras för kännedom.

Berörd medarbetare ska kontaktas och ges möjlighet att förklara skälen till aktuell loggförekomst. Kontakten tas av verksamhetschefen eller utsedd person. Vid misstanke om dataintrång finns ofta anledning att anta att arbetsrättsliga åtgärder kan komma att bli aktuella. Inför samtalet ska medarbetaren därför informeras om möjligheten att ta med en facklig representant. Vid samtalet ska representant från förvaltningens HR-funktion delta. Följande frågor bör besvaras:

- Varför har medarbetaren sökt information om denna patient?
- Känner medarbetaren patienten privat eller finns det någon annan anknytning till patienten?
- Vilka patientuppgifter har medarbetaren tagit del av och på vilket sätt har patientuppgifterna använts?

Finns inte godtagbara skäl för åtkomst till uppgifterna, utan misstanken om dataintrång kvarstår eller bekräftats, ska verksamhetschef informera:

- berörd patient
- förvaltningschef, som efter samråd med HR-funktion, beslutar om eventuella arbetsrättsliga åtgärder och polisanmälan enligt denna instruktion
- förvaltningens dataskyddssamordnare, eftersom händelsen nu måste utredas som en personuppgiftsincident (se avsnitt "Personuppgiftsincident" i dokumentet)

I de fall misstanke avser legitimerad personal ska även förvaltningens chefläkare informeras då eventuell anmälan till IVO ska ske i samråd med honom eller henne, se avsnitt "4.2.5 Anmälan av legitimerad hälso- och sjukvårdspersonal till IVO" i dokumentet.

4.2 Åtgärder

4.2.1 Polisanmälan

Vid misstanke om dataintrång ska medarbetaren som huvudregel polisanmälas. Observera att det är förvaltningschef som, efter samråd med HR-funktion, bestämmer om polisanmälan ska göras.

4.2.2 Arbetsrättsliga åtgärder

Vid misstanke om dataintrång i arbetet kan arbetsgivaren allt efter omständigheterna välja mellan ett eller flera av följande alternativ:

- tillrättavisande samtal
- disciplinpåföljd enligt AB § 11
- uppsägning eller avskedande enligt 7 respektive 18 §§ lagen om anställningsskydd (LAS).

Ytterst riskerar en medarbetare som olovligen berett sig tillgång till patientuppgifter i ett IT-system att skiljas från sin anställning genom avsked. En helhetsbedömning av vilka arbetsrättsliga åtgärder som kan, och lämpligen bör, vidtas måste ske i varje enskilt fall.

4.2.2.1 Avstängning

Vid ett misstänkt dataintrång kan berörd medarbetare stängas av från arbetet enligt Allmänna Bestämmelser (AB) § 10. Inför beslut om avstängning är arbetsgivaren skyldig att begära och genomföra en överläggning med berörd arbetstagarorganisation. *En avstängning är inte en bestraffning, utan sker i avvaktan på slutligt ställningstagande.*

4.2.2.2 Särskilt angående disciplinpåföljd enligt AB § 11

I de fall disciplinpåföljd enligt AB § 11 är aktuellt att meddela ska följande noteras. Disciplinförfarande får inte inledas eller fortsätta om arbetsgivaren har anmält det misstänkta brottet till polismyndigheten. Om polis eller åklagare avskriver ärendet, eller om medarbetaren frikänns på grund av att gärningen visserligen har begåtts men inte är brottslig, kan arbetsrättslig disciplinpåföljd trots det komma ifråga för samma gärning. I de fall arbetsgivaren gör bedömningen att en polisanmälan inte ska göras kan det ändå bli aktuellt att meddela disciplinpåföljd. Notera att en polisanmälan inte hindrar arbetsgivaren från att säga upp eller avskeda medarbetaren.
Observera att kontakt ska tas med förvaltningens HR-funktion innan beslut om arbetsrättsliga åtgärder fattas.

4.2.2.3 Vägledning arbetsrättsliga åtgärder

Av betydelse vid den arbetsrättsliga bedömningen är bland annat gärningens art och omfattning, medarbetarens ställning och graden av skada eller men som patienten/ arbetsgivaren lidit. Med medarbetarens ställning avses att ju högre ställning medarbetaren har inom en organisation, desto större krav kan arbetsgivaren ställa på medarbetaren. Med skada avses inte enbart ekonomisk skada, utan även den skada som tillfogas arbetsgivaren genom ett minskat förtroende från allmänheten till följd av det inträffade.

Genom att ge medarbetare tillgång till känslig sekretesskyddad information såsom patientuppgifter, har Region Skåne visat ett särskilt förtroende för berörda medarbetare. En medarbetare som olovligen bereder sig tillgång till patientuppgifter utnyttjar förtroendet för egen vinning även om nyttjandet till exempel sker av ren nyfikenhet. Patientinformation är

mycket känslig och skyddas av stark sekretess. Att medarbetare olovligen bereder sig tillgång till sådan information innebär att patienternas och allmänhetens förtroende för Region Skåne skadas.

4.2.3 Personuppgiftsincident

Att olovligen bereda sig tillgång till patientuppgifter ska även betraktas som en personuppgiftsincident enligt dataskyddsförordningen (EU) 2016/679. Händelsen ska därför utredas och hanteras av förvaltningens dataskyddssamordnare enligt gällande instruktion för personuppgiftsincidenter. Notera att vissa typer av personuppgiftsincidenter ska anmälas till Integritetsskyddsmyndigheten inom 72 timmar efter det att incidenten har upptäckts. Det är av den anledningen som dataskyddssamordnaren ska informeras skyndsamt om dataintrånget.

4.2.4 Avvikelseanmälan

Verksamhetschefen ansvarar för att en avvikelse rapporteras i Region Skånes IT-stöd för avvikelsehantering.

4.2.5 Anmälan av legitimerad hälso- och sjukvårdspersonal till IVO

Vårdgivaren är enligt 3 kap. 7 § patientsäkerhetslagen (PSL) skyldig att snarast anmäla till Inspektionen för vård och omsorg (IVO) om det finns skälig anledning att befara att en person, som har *legitimation* för ett yrke inom hälso- och sjukvården och som är verksam eller har varit verksam hos vårdgivaren, kan utgöra en fara för patientsäkerheten. I samband med att frågan om polisanmälan ska göras eller ej, bör således även ställning tas till om anmälan till IVO enligt ovan ska ske. Anmälan ska göras av eller i samråd med chefläkare (anmälningsansvarig svarande mot Patientsäkerhetslagen 3 kap §3-7) i enlighet med förvaltningens rutin för dessa ärenden.

I IVO:s ansvar ligger att utreda legitimerad hälso- och sjukvårdspersonal vars yrkesutövning kan ifrågasättas utifrån ett patientsäkerhetsperspektiv eller ur förtroendesynpunkt. Skälen till granskningen kan vara oskicklighet, olämplighet, brottslighet m.m.

Observera att Region Skåne ska göra en bedömning av om polisanmälan ska ske enligt denna rutin oaktat att anmälan till IVO har skett.

Vårdgivare inom offentlig verksamhet som avskedar en arbetstagare som står under tillsyn av IVO är skyldiga enligt förordning (2013:196) att snarast anmäla detta till IVO och bifoga en kopia av beslutet om avskedandet.

I vissa fall kan även anmälan enligt lex Maria bli aktuell. Sådan bedömning görs enligt förvaltningens sedvanliga rutiner av respektive chefläkare.

4.2.7 Särskilt gällande studenter och hyrpersonal

Gäller misstanke om dataintrång studerande eller inhyrd personal handläggs och utreds ärendet enligt denna instruktion. Dock kan inte arbetsrättsliga åtgärder tillgripas.