Koncernkontoret		
Enheten för informationssäkerhet informationssakerhet@skane.se	**Datum**: 2013-10-09 Dnr:	
Dokumentförvaltare: Enheten för informationssäkerhet Koncernkontoret		**Dokumentets status**: Beslutad
Dokumentid: Dataintrång - åtgärder vid misstanke om olovlig åtkomst **Dokumentformat:** A4	**Version:** 2.0	**Dokumenttyp:** Instruktion **Dokumentklass:** Styrande dokument **Ämne:** Ledningssystem för informationssäkerhet

INSTRUKTION

Dataintrång - åtgärder vid misstanke om olovlig åtkomst

Revisionshistorik

Datum	Ver.	Namn	Kommentar
2013-10-09	2.0	Enheten för informationssäkerhet	Reviderad och ersätter ”Vägledning avseende åtgärder vid dataintrång” (2008)

Inledning

Om någon obehörig har berett sig tillgång till patientuppgifter kan denne dömas för dataintrång enligt 4 kap 9c § i brottsbalken: ”Den som i annat fall än som sägs i 8 och 9 §§ 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”.

Denna anvisning beskriver dels rutin för hantering vid misstanke om dataintrång och dels straff- och arbetsrättsligt förfarande när arbetsgivaren i sin utredning konstaterat att obehörig åtkomst till patientuppgifter, dataintrång, skett. Brottsbalkens bestämmelse om dataintrång omfattar alla typer av uppgifter som är avsedda för automatiserad behandling. För Region Skånes del är patientuppgifter mest förekommande, varför anvisningen framför allt behandlar obehörig tillgång till sådana uppgifter. Men anvisningen kan i tillämpliga delar användas även vid andra typer av dataintrång.

Handläggning vid misstanke om dataintrång

Misstanke om dataintrång kan uppstå vid en systematisk och regelbunden stickprovskontroll i verksamheten alternativt vid riktad kontroll. Riktad kontroll är specifik mot viss patient eller anställd och föranledd av misstanke om dataintrång t ex på grund av att en berömd person vårdats på enheten eller efter misstanke från patient.

Denna instruktion är ett komplement till gällande regional instruktion för ”Loggkontroll - granskning av åtkomst till patientuppgifter”.

Om obehörig åtkomst misstänks ska detta handläggas skyndsamt enligt följande rutin:

- Vid misstanke om dataintrång kontaktas verksamhetschef på berörd vårdenhet eller motsvarande. Om verksamhetschefen är jävig ska istället dennes chef kontaktas.

- Underlag ska säkerställas i loggar från IT-stöd 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.

- På varje förvaltning ska finnas en stödjande funktion bestående minst av representanter från förvaltningens HR/personalavdelning, informationssäkerhetsamordnare samt personuppgiftsombudets företrädare (PUO-företrädare). Denna funktion ska bli informerad om händelsen och vara stödjande i utredningsarbetet.
  Motsvarande regionala funktioner; HR/personal, informationssäkerhet och PUO kan vid behov kontaktas.

- Berörd medarbetare ska kontaktas och ges möjlighet att förklara skälen till aktuell loggförekomst. Kontakten tas av verksamhetschefen. 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 HR/personalavdelningen delta.

- Vid samtalet bör följande frågor besvaras:
  - Varför har medarbetaren sökt information om denna patient?
  - Känner medarbetaren patienten privat eller har 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, ska verksamhetschef informera berörd patient om detta.

- Vid bekräftad misstanke om dataintrång ska verksamhetschefen informera förvaltningschef, som i samråd med förvaltningens HR/personalavdelning, beslutar om fortsatt straff- och arbetsrättsligt förfarande enligt denna instruktion.

Straff- och arbetsrättsligt förfarande vid dataintrång

Polisanmälan
Om medarbetaren med uppsåt olovligen berett sig tillgång till patientuppgifter ska medarbetaren som huvudregel polisanmälas.

Arbetsrättsliga åtgärder

- Avstängning. Vid ett misstänkt dataintrång kan berörd arbetstagare stängas av från arbetet enligt § 10 i Allmänna Bestämmelser (AB). En avstängning är inte en bestraffning, utan sker i avvaktan på slutligt ställningstagande.
- Regler om disciplinpåföljd finns i AB § 11. I och med att arbetstagaren inte ska straffas två gånger för samma sak får emellertid ett disciplinärt förfarande inte inledas eller fortsätta om arbetsgivaren gjort polisanmälan. Som nämnts ovan görs normalt polisanmälan vid misstänkt dataintrång, vilket således medför att arbetsgivaren inte kan meddela en disciplinpåföljd. Om det däremot t.ex. föreligger särskilda skäl mot att göra en polisanmälan, kan det bli aktuellt att istället meddela disciplinpåföljd. Detsamma kan gälla om en polisanmälan inte leder till fällande dom, beroende på vilka skäl som ligger bakom att arbetstagaren inte döms.

Det är viktigt att chefer inom vården informerar sina medarbetare om de regler som styr tillgången till patientjournaler och annan vårdinformation. Förutom att dataintrång är olagligt är det också att betrakta som ett förtroendemissbruk. Genom att ge medarbetare tillgång till känslig sekretesskyddad information, har Region Skåne visat ett särskilt förtroende för medarbetarna. En medarbetare som olovligen bereder sig tillgång till patientuppgifter utnyttjar förtroendet för egen vinning även om nyttjandet sker av ren nyfikenhet. Patientinformation är mycket känslig och skyddas av den starkaste formen av sekretess. Att medarbetare olovligen bereder sig tillgång till sådan information innebär att patienternas och allmänhetens förtroende för Region Skåne skadas. En arbetstagare som är medveten om att Region Skåne inte accepterar brott mot sekretessreglerna – och trots det bryter mot tystnadsplikten eller begår ett dataintrång – riskerar att förlora sin anställning.

Bedömningen av vilka åtgärder som kan och lämpligen bör vidtas vid dataintrång ska ske mot bakgrund av omständigheterna i varje enskilt fall. Av betydelse är gärningens art och omfattning, arbetstagarens ställning och graden av skada som patienten/arbetsgivaren lidit. Med skada avses

inte enbart ekonomisk skada utan även den skada som tillfogas arbetsgivaren genom ett minskat förtroende från allmänheten.

Observera att kontakt ska tas med förvaltningens HR/personalavdelning innan beslut om arbetsrättsliga åtgärder fattas.