Lokal informationssäkerhetspolicy

Patientnämnden och dess förvaltning är beroende av information i olika former för det dagliga arbetet – avbrott i tillgång till information ger allvarliga konsekvenser för verksamheten.
Alla i nämnd och förvaltning, även vikarier, konsulter och andra, har ett personligt ansvar att värna om informationssäkerhet. Det omfattar information i alla dess former, digital, skriftlig eller muntlig.
De som kontaktar förvaltningen, anmälare, patienter, stödpersoner eller vården ska vara säkra på att den information de lämnar hanteras med tillräckligt skydd.

Målet för informationssäkerheten är att:

- känslig information aldrig görs tillgänglig så att personlig integritet eller sekretess hotas (konfidentialitet)
- information säkras så att den inte går förlorad genom misstag, inverkan av obehörig eller pga. tekniska fel (riktighet)
- information görs tillgänglig i förväntad utsträckning, inom önskad tid och på rätt plats (tillgänglighet)
- det alltid framgår vem som haft tillgång till informationen.

Patientnämnden och dess förvaltning följer de lagkrav som finns på informationssäkerhet, i första hand dataskyddsförordningen, offentlighets- och sekretesslagen och tryckfrihetsförordningen.

Riskbedömning av identifierade hot görs kontinuerligt och dessa hanteras med korrekta skyddsåtgärder.

Informationssäkerhetsincidenter anmäls i förvaltningens avvikelsehantering och utgör grunden för ständiga förbättringar av hanteringen av information.

Patientnämnden
Box 17535, 118 91 Stockholm
Hornsgatan 15

Telefon 08-690 67 00
Fax 08-690 67 18

E-post registrator@pan.sll.se
www.patientnamndenstockholm.se

Patientnämnden
STOCKHOLMS LÄNS LANDSTING

Informationsklass:K1R2T1
A1810-0012971

Lokala riktlinjer för informationssäkerhet patientnämnden

Innehåll:

Bakgrund
Roller och ansvar
Förteckning av informationstillgångar
Riskbedömning och riskhantering
Bevarande, rensning och gallring
Kontinuitetsplan
Intern informationsanvändning
Extern informationsanvändning
Nätverk
Utveckling av system
Krav
Drift hos extern part
Avvikelser
Utbildning
Uppföljning och övervakning

Bakgrund:

Dessa lokala riktlinjer utgår från 'Riktlinjer för informationssäkerhet inom Stockholms läns landsting' som antogs av landstingsstyrelsen 2011 och reviderades 2013.

Vad är informationssäkerhet?

Informationssäkerhet innebär skydd av information mot olika slags hot. Informationssäkerhet delas upp i administrativ och teknisk säkerhet. Den **administrativa säkerheten** omfattar utbildning, regler (t ex tydliga rutiner och kända riktlinjer), roller (rollfördelning, behörigheter, ansvarsfördelning) och uppföljning.
Teknisk säkerhet omfattar fysisk säkerhet (t ex förvaringssätt, passerkort, sekretess och besöksrutiner) och it-säkerhet som innefattar datasäkerhet och kommunikationssäkerhet (omfattar lösenord, virusskydd, back up-system, skärmsläckare mm.)
Alla i nämnd och förvaltning har ett personligt ansvar att värna om informationssäkerheten.

Informationssäkerhetsarbete innebär att skydda följande säkerhetsaspekter:
- **konfidentialiteten** d.v.s. information får inte göras tillgänglig eller avslöjas på ett sådant sätt att den personliga integriteten eller sekretessen hotas.
- **riktigheten** d.v.s. information får inte förändras eller gå förlorad, av misstag, genom inverkan av obehörig eller på grund av tekniskt fel.
- **tillgängligheten** d.v.s. information ska kunna användas i förväntad utsträckning, inom önskad tid och på rätt plats.
- det är också viktigt att **spårbarhet** finns, det ska framgå vem som hanterat informationen.

Roller och ansvar i verksamheten

Patientnämnden

Patientnämnden är personuppgiftsansvarig och ytterst ansvarig för informationssäkerheten i nämnd och förvaltning. Nämnden ska anta lokal policy och lokala riktlinjer samt lokala anvisningar för informationssäkerheten.
Nämnden är ansvarig för att det årligen tas fram en plan för kommande års säkerhetsarbete, att det avsätts medel och att föregående års arbete följs upp. Nämnden ska utse datskyddsombud. Patientnämnden är ansva-

rig för att de krav som landstinget ställer på inköp, underhåll och utveckling följs. Nämnden ska löpande följa upp informationssäkerheten och i övrigt vidta de åtgärder som krävs för att uppnå och upprätthålla tillräcklig intern kontroll.

Förvaltningschef

Förvaltningschefen är informations- och systemägare hos patientnämndens förvaltning. Informations- och systemägaren bevakar alla delar av säkerheten för de informationstillgångar och it-system som identifierats, t ex extern hemsida, databaser, skriftlig dokumentation, datorer mm. Förvaltningschefen ska utforma och kommunicera instruktioner för informationssäkerhet, följa upp hur de efterlevs, tillsätta tillräckliga resurser för informationssäkerheten och årligen rapportera status på informationssäkerheten till nämnden. Informationsägaren ska fatta beslut om användares åtkomsträttigheter så att behörighet ges beroende på arbetsuppgifter. Uppföljning av behörighetstilldelningen ska göras årligen. Systemägaren ska besluta om införande, utveckling och avveckling av it-system och ska vid behov utse systemförvaltare. Förvaltningschefen ansvarar för att loggning sker på de verksamhetskritiska it-systemen. Behovet av skyddsåtgärder ska omprövas regelbundet. För att säkerställa verksamheten vid driftstörningar ska det finnas en kontinuitetsplan framtagen, förvaltningschefen ansvarar för att den uppdateras årligen eller efter incidenter. Dessutom ansvarar förvaltningschefen för att det utses en övergripande krisorganisation som ska ansvara för att få verksamheten att återgå till ett normalläge efter katastrofsituationer, störningar och oplanerade avbrott. Förvaltningschefen ansvarar för att en förteckning förs över alla viktiga informationstillgångar. Informationstillgångarna ska klassificeras (gällande konfidentialitet, tillgänglighet och riktighet) och informationssäkerhetsamordnaren ska föreslå en rutin för detta som förvaltningschefen fastställer. Dyrbar utrustning ska stöldmärkas. Förvaltningschefen ska utse informationssäkerhetssamordnare.

Dataskyddsombud

Dataskyddsombudet (på förvaltningen är det förvaltningsjuristen) ska självständigt se till att behandlingen av personuppgifter sker på ett korrekt sätt. En viktig skillnad mot personuppgiftsombudets roll är att dataskyddsombudet har en mer kontrollerande och självständig roll. Dataskyddsombudet är inte ansvarigt för att förvaltningen följer lagen men ska kontrollera och sedan rapportera till både ledningen och Datainspektionen. Ombudet ansvarar för en förteckning över de behandlingar av personuppgifter som sker. Därutöver ansvarar denne för utlämnande av registerutdrag, anmälan av personuppgiftsincidenter, upprättande av personuppgiftsbiträdesavtal samt utbildning av förvaltningens medarbetare i personuppgiftsfrågor.

Informationssäkerhetssamordnare
Informationssäkerhetssamordnaren ska regelbundet granska informationssäkerheten och analysera hur systemen förhåller sig till författningar, informationssäkerhetsriktlinjerna inom landstinget och förvaltningens instruktioner/anvisningar. Informationssäkerhetssamordnaren ska ansvara för den lokala efterlevnaden av rutiner och instruktioner/anvisningar. Informationssäkerhetssamordnaren ska sprida kunskap om regler, genomföra riskanalyser och kontrollera efterlevnaden i form av loggar i datasystemen och då särskilt CMC Motion. Informationssäkerhetssamordnaren ska vara kontaktperson mot landstingets informationssäkerhetschef och vara representant i landstingets informationssäkerhetsråd. Årligen ska informationssäkerhetssamordnaren rapportera granskningar, skyddsåtgärder, riskanalyser och förbättringsåtgärder till förvaltningschefen och till informationssäkerhetschefen i landstinget. Informationssäkerhetssamordnaren ska skriva förslag på tillämpningsanvisningar gällande informationssäkerhet och utforma förslag till handlinsplan för informationssäkerhet. Informationssäkerhetsasamordnaren ska regelbundet ompröva vilka skyddsåtgärder som måste vidtas tillsammans med förvaltningschefen. Informationssäkerhetssamordnaren föreslår rutiner för klassificering av informationstillgångar. Rutinerna fastställs av förvaltningschefen.

Systemförvaltare
Förvaltningschefen ska vid behov utse systemförvaltare över förvaltningens informationssystem. Systemförvaltare ska upprätta systemförvaltningsplaner. Dessa ska omfatta rutiner för införande, förvaltning och avveckling av systemen och ska uppdateras årligen eller efter incidenter.

Personuppgiftsbiträde
När extern part hanterar personuppgifter ska avtal om personuppgiftsbiträde enligt dataskyddsförordningen skrivas.

Personal
Rutiner ska finnas för att säkra informationssäkerheten i samband med rekrytering, nyanställning och avslutande av anställning. Riktlinjer om bisysslor ska finnas lätt tillgängliga. Patientnämnden är ansvarig för behandling av personalens personuppgifter. Personalen ska följa patientnämndens sekretess som regleras i 25 kapitlet 4 § offentlighets- och sekretsslagen (2009:400). Det gäller även konsulter om de deltar i verksamheten på samma sätt som övrig personal. Övriga personers tystnadsplikt ska regleras i avtal (städare, tolk och posthantering t ex).

Förteckning av tillgångar och klassificering

Årligen ska informationsägaren fastställa en förteckning över viktiga tillgångar som omfattar programvaror, databaser, skriftlig information, fysiska och immateriella tillgångar, nyckelpersoner samt avtal. Tillgångarna ska klassificeras dvs. tillgångens betydelse tydliggörs och det är utifrån denna klassifikation som riskanalyser görs. Landstingets modell för klassificering ska användas och säkerhetsaspekterna konfidentialitet, tillgänglighet och riktighet ska bedömas. Bedömd skada graderas enligt nivå 1 = försumbar skada, nivå 2 = medelsvår, nivå 3 = allvarlig skada.

Riskbedömning och riskhantering

Riskbedömning ska genomföras för de viktigaste informationssäkerhetsaspekterna och ska dokumenteras i förvaltningens plan för intern kontroll. Bedömningen görs i enlighet med landstingets gällande vägledning och ska grundas på den klassificering av informationstillgångar som genomförs årligen och ska resultera i lämpliga skyddsåtgärder. Skyddsåtgärderna ska grundas på identifierade risker. Grundregeln är att information inte ska lämnas oskyddad.

Bevarande, rensning och gallring

Skriftlig dokumentation (även e-post) ska bevaras och gallras i enlighet med gällande regelverk, bl a arkivlagen (1990:782) och Landstingsarkivets föreskrifter.

Kontinuitetsplanering

God kontinuitet som möjliggör att verksamheten upprätthålls även vid oplanerade avbrott och störningar ska planeras. Förvaltningen ska ha en uppdaterad plan för kontinuitetsplanering där även informationssäkerheten inräknas.

Intern informationsanvändning

Personlig användning av landstingets it-system och utrustning ska regleras i lokala rutiner/anvisningar framtagna av informationssäkerhetssamordnare i samverkan med it-ansvarig. Privat användning är tillåten i begränsad omfattning. Stark autentisering med e-tjänstekort används.

Extern informationsanvändning

Stark autentisering ska användas när extern informationsanvändare ges tillgång till förvaltningsinformation som är klassad K3.

Patientnämnden
Box 17535, 118 91 Stockholm
Hornsgatan 15

Telefon 08-690 67 14
Fax 08-690 67 18

E-post: registrator@pan.sll.se
www.pan.sll.se

Nätverk

Vad gäller design, konfiguration och användning av trådlösa nätverk ska patientnämnden följa de regler som Stockholms läns landsting beslutar.

Anskaffning och utveckling av system

När system anskaffas eller utvecklas ska det föregås av en analys av hur systemet förhåller sig till lagar och regler som styr nämnden och dess förvaltning.

Legala och externa krav:

Patientnämnden och dess förvaltning måste följa legala och externa krav som gäller för att kunna leva upp till god informationssäkerhet. De författningar som påverkar arbetet med informationssäkerhetsarbetet är bland annat:

- Tryckfrihetsförordningen och då särskilt 2 kapitlet om allmänna handlingars offentlighet och 4-6 kapitlena
- Offentlighets- och sekretesslagen (2009:400) och då särskilt 4-6 kapitlena om registrering och utlämnande av allmänna handlingar samt patientnämndens och hälso- och sjukvårdens sekretess i 25 kapitlet
- Arkivlagen (1990:782)
- Dataskyddsförordningen
- Brottsbalken och då särskilt vad gäller dataintrång och brott mot tystnadsplikt
- Lag (1998:112) om ansvar för elektroniska anslagstavlor
- Lag (2000:832) om kvalificerade elektroniska signaturer
- Kommunallagen (1991:900)
- Förvaltningslagen (1986:223)
- Lag (2007:1091) om offentlig upphandling
- Lag om kommunal redovisning (1997:614)
- Lag (1960:729) om upphovsrätt till litterära och konstnärliga verk
- Patentlagen (1967:837)
- Lag (1949:345) om rätten till arbetstagares uppfinningar
- Lag (1998:1656) om patientnämndsverksamhet m.m.
- Lag (1991:1128) om psykiatrisk tvångsvård vad gäller stödpersoner
- Lag (1991:1129) om rättspsykiatrisk vård vad gäller stödpersoner
- Smittskyddslagen (2004:168) vad gäller stödpersoner
- Säkerhetsskyddslagen (1996:627) (Vid frågor kontakta säkerhetsskyddschefen som finns inom Landstingsstyrelsens förvaltning)
- Lag (2002:833) om extraordinära händelser i fredstid hos kommuner och landsting
- Lag (1988:97) om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara
- Till ovan nämnda lagar kan det finnas förordningar och föreskrifter som är tillämpliga.

Drift hos extern part

Samma regler som gäller informationssäkerheten på förvaltningen ska gälla då förvaltningen köper externa it-tjänster eller förlägger drift av it-system externt. Förvaltningen ska beredas möjlighet att revidera informationssäkerheten. Krav på informationssäkerheten ska regleras i avtal och i de fall extern part hanterar personuppgifter ska personuppgiftsbiträdesavtal upprättas.
Ingen känslig information (K2 eller K3) ska lagras i molntjänster utan noggrann riskanalys. I de fall personuppgifter lagras är patientnämnden personuppgiftsansvarig och reglerna i datskyddsförodningen ska följas.

Avvikelser

Incidenter och avvikelser ska skrivas i förvaltningens avvikelsesystem. Det är informationssäkerhetssamordnaren som ska ansvara för att avvikelser analyseras och åtgärdas.

Utbildning

Alla anställda ska få utbildning i informationssäkerhet. Utbildningen bör följas upp årligen.

Uppföljning och övervakning

Genomförda riskanalyser, avvikelser och utvärdering av skyddsåtgärder ska användas i uppföljning av informationssäkerheten. Omvärldsanalysen ska bl a omfatta it-utveckling, ny eller förändrad lagstiftning, standarder, marknadskrav och utveckling av teknik.

Patientnämnden
Box 17535, 118 91 Stockholm
Hornsgatan 15

Telefon 08-690 67 14
Fax 08-690 67 18

E-post: registrator@pan.sll.se
www.pan.sll.se

Anvisningar för informationssäkerhet

Bakgrund:

Följande anvisningar grundas på Riktlinjer för informationssäkerhet inom Stockholms läns landsting och patientnämndens lokala riktlinjer.

Skyddade personuppgifter

Säkerheten är extra viktig då personuppgifter är skyddade. För information, se rutin 'Hantering av uppgifter om skyddad identitet', Rutiner/rutiner/allmänna rutiner/skyddad identitet.

Förteckning över förvaltningen informationstillgångar:

Förvaltningens informationstillgångar ska vara dokumenterade i en förteckning som uppdateras årligen av informationssäkerhetssamordnaren. Dessa tillgångar ska omfatta fysiska tillgångar (datorer, skrivare mm), programvara, informationstillgångar (databaser, datafiler och dokumentation), avtal, immateriella tillgångar (patent och varumärken) och nyckelpersoner. I denna förteckning framgår också hur tillgångarna klassificerats och de skyddsåtgärder som vidtagits utifrån klassificeringen. Se 'Förteckning över informationstillgångar'.
Eftersträvad skyddsnivå kontrolleras genom rutiner, stickprov och avvikelser.
Riskhantering ska vara en kontinuerlig process och riskanalyser ska genomföras i samband med förändringar i verksamheten, processerna och informationssystemen eller motsvarande. De verksamhetskritiska systemen (se klassificering) ska granskas och årligen analyseras av systemägare och informationssäkerhetssamordnare. Analyserna ska kompletteras med en uppföljning av att systemen följer interna och juridiska krav i samråd med förvaltningsjuristen.

Utbildning

Landstingets grundläggande interaktiva utbildning i informationssäkerhet (DISA) ska genomföras av nyanställd tidigt i introduktionen och ska följas upp tillsammans med informationssäkerhetssamordnaren. DISA bör repeteras vart tredje år av alla anställda. Även tillfälligt anställda ska få utbildning och information.

Roller, ansvarsfördelning och behörighet

För aktuella behörigheter, se bilaga 'Förteckning över informationstillgångar'. Det är förvaltningschefen som tilldelar behörighet utifrån arbetsuppgift och beslutet ska omprövas årligen. Det gäller både anställda och

konsulter.
Systemägaren har utsett systemförvaltare för förvaltningens egna informationssystem. De ska upprätta en systemförvaltningsplan i enlighet med de övergripande riktlinjerna. Planen ska uppdateras årligen och vid incident.
Dessa planer ska innehålla noggrann information om:
- system- drift- och användardokumentation, såsom källkod, programvara, kravspecifikation och ägarförhållande
- säkerhetsfunktion
- utvecklingsplan i förhållande till lagar och regler
- gallringsplan
- hantering av störningar och avvikelser
- uppföljning och uppdatering (t ex säkerhetsuppdatering och ändringshantering).
Se systemförvaltningsplaner för Focus, Intranätet, den externa webbplatsen och CMC Motion.

Personal

E-tjänstekort med pin-kod ska användas för att säkerställa behörigheten. Administratörsbehörigheter ska begränsas till ett fåtal personer som har personliga användaridentiteter.
Lösenord, passerkort och e-tjänstekort ska tilldelas, dessa är personliga och får inte lånas ut. En sekretessbekräftelse ska undertecknas, se checklista vid nyanställning (Rutiner/introduktion/nyanställd personal).
Vid avslutande av anställning görs på motsvarande sätt så att passerkort, e-tjänstekort och övrig utrustning återlämnas samt åtkomsträttigheter upphör, se checklista vid entledigande (Rutiner/personalrutiner/anställning). Material som ägs av arbetsgivaren får inte kopieras eller tas med när anställning upphör. Material som ägs av arbetsgivaren är till exempel all information i CMC Motion.

Bisysslor

Anställda får inte ägna sig åt bisysslor som hindrar dem att vara opartiska i sin yrkesutövning. Information om landstingets regler för bisysslor finns att ta del av på landstingets intranät och i förvaltningens rutiner (se Rutiner/personalrutiner/anställning). Information om riktlinjer för bisyssla ska ges vid nyanställning av personal och ska redovisas minst vartannat år.

Sekretess

I 25 kapitlet 4 § offentlighets- och sekretesslagen anges: sekretess gäller i ärenden hos en nämnd med uppgift att bedriva patientnämndsverksamhet enligt lagen (2017:372) om stöd vid klagomål mot hälso- och sjukvården för uppgift om en enskilds hälsotillstånd eller andra personliga förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde el-

ler någon närstående till denne lider men. Känslig information får inte diskuteras på allmän plats eller där det finns risk för att någon kan ta del av vad som sägs. Om någon röjer sekretessbelagda uppgifter och/eller tar del av information om en anmälare, stödperson eller patient utan giltigt skäl kan det betraktas som brott mot tystnadsplikten och/eller dataintrång. Detta kan polisanmälas och kan föranleda samtal med förvaltningschefen, skriftlig varning, uppsägning eller avsked. Bristande efterlevnad av gällande regler för informationssäkerhet och sekretess kan även vara misskötsel, vilket kan vara ett brott mot anställningsavtalet.

Lagring i extern lagringstjänst

I de fall information lagras i sk molntjänster ska det säkerställas genom t ex biträdesavtal att samma säkerhet som i förvaltningens system kan garanteras. Beslut om lagring fattas efter dokumenterad riskanalys.

Incidenshantering

Vid allvarliga incidenser t ex virusutbrott anmäls detta till landstingets itsupport och förvaltningschef beslutar i samråd med förvaltningens informationssäkerhetssamordnare om vilka åtgärder som bör vidtas för att begränsa skadan. Åtgärderna kan omfatta avstängning av datorer eller epostkonton. Till stöd har förvaltningen landstingets SOC-funktion som bevakar incidenser och som återför risker och händelser. Information om risker lämnas på förvaltningens funktionsbrevlåda registrator.pan@sll.se och vidarebefordras till informationssäkerhetssamordnare och/eller dataskyddsombud.

Uppföljning

Informationssäkerhetssamordnaren ska ansvara för att instruktioner efterföljs och att orsaker till avvikelser analyseras.