Innehåll:

Bakgrund
Styrning och planering, legala krav
Organisation, roller och ansvar
Bedömning och hantering av risker
Kontinuitetsplanering
Kommunikation
Avvikelser
Uppföljning och övervakning

Bakgrund:

Föreliggande dokument utgör patientnämndens förvaltnings lokala riktlinjer och utgår från ’Riktlinjer för informationssäkerhet inom Region Stockholm’ som antogs av regionstyrelsen 2020 (RS 2020-0148). Övergripande dokument är Policy för verksamhetsskydd (RS 2020-0147).

Styrning och planering

Den övergripande policyn och de övergripande riktlinjerna är styrande för all informationshantering i Region Stockholm. Ansvar för informationssäkerhet är kopplat till verksamhetsansvar.

Legala 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 kapitlen
- Offentlighets- och sekretesslagen (2009:400) och då särskilt 4-6 kapitlen 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 (2017:725)

- Förvaltningslagen (2017:900)
- Lag (2007:1091) om offentlig upphandling
- Lag om kommunal redovisning (1997:614)
- Lag (2017:372) om klagomål mot hälso- och sjukvård
- Lag (1991:1128) om psykiatrisk tvångsvård vad gäller stödpersoner
- Lag (1991:1129) om rättspsykiatrisk vård vad gäller stödpersoner
- Smittskyddslagen (2004:168) vad gäller stödpersoner
  Till ovan nämnda lagar kan det finnas förordningar och föreskrifter som är tillämpliga.

Organisation, roller och ansvar samt utbildning

Patientnämnden

Patientnämnden är personuppgiftsansvarig och ytterst ansvarig för informationssäkerheten i nämnd och förvaltning. Nämnden ska utse dataskyddsombud och informationssäkerhetssamordnare. Patientnämnden är ansvarig för att de krav som regionen 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

Ansvar för informationssäkerhet är kopplat till verksamhetsansvar. Förvaltningen är systemägare för ärendehanteringssystemet CMC Motion och ansvarig för information på hemsidan och intranätet. Förvaltningschef ska:
- fatta beslut om användares åtkomsträttigheter så att behörighet ges beroende på arbetsuppgifter. Uppföljning av behörighetstilldelningen ska göras årligen.
- besluta om införande, utveckling och avveckling av it-system och ska vid behov utse systemförvaltare. Behovet av skyddsåtgärder ska omprövas regelbundet.
- ansvara för att kontinuitetsplan finns framtagen och uppdateras årligen eller efter incidenter
- tillse att det finns en uppdaterad inventarieförteckning.

Dataskyddsombud

Dataskyddsombudet ska se till att personuppgifter behandlas korrekt och lagligt och ska sammanställa en förteckning över vilka personuppgiftsregister som finns. Förteckningen ska arkiveras, men

en kopia av förteckningen ska finnas tillgänglig i förvaltningens lokaler. Dataskyddsombudet ska anmäla till Integritetsskyddsmyndigheten om missförhållanden uppdagas och inte åtgärdas efter att förvaltningschefen har blivit informerad om dessa missförhållanden. Behandling av personuppgifter ska anmälas till dataskyddsombudet som också ska tillse att personuppgiftsbiträdesavtal upprättas i de fall extern part hanterar personuppgifter. Dataskyddsombudet deltar regelbundet i nätverk för dataskyddsombud inom regionen.

Informationssäkerhetssamordnare
Informationssäkerhetssamordnaren ska
- regelbundet granska informationssäkerheten och analysera hur den förhåller sig till författningar, policy, riktlinjerna inom regionen och förvaltningens rutiner
- ansvara för den lokala efterlevnaden av rutiner
- sprida kunskap om regler, genomföra riskanalyser och kontrollera efterlevnaden i form av loggar i datasystemen vid särskilda händelser och då särskilt Vårdsynpunkter och Stödpersoner
- vara kontaktperson mot regionens informationssäkerhetschef och vara representant i informationssäkerhetsrådet
- föreslå rutiner för klassificering av informationstillgångar.

Årligen ska samordnaren rapportera granskningar, skyddsåtgärder, riskanalyser och förbättringsåtgärder till förvaltningschefen. Informationssäkerhetsasamordnaren ska årligen genomföra ledningens genomgång med förvaltningens ledning och där planera för en handlingsplan de närmaste åren.

Systemförvaltare
Förvaltningschefen ska vid behov utse systemförvaltare över förvaltningens informationssystem CMC Motion, hemsidan och intranätet. 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 skrivas.

Personal

Rutiner ska finnas för att säkra informationssäkerheten i samband med rekrytering, nyanställning och avslutande av anställning. Regionens datoriserade utbildning för informationssäkerhet genomförs kort efter anställning (DISA). 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 sekretesslagen (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).

Bedömning och hantering av risker

Riskbedömning ska genomföras för de viktigaste informationssäkerhetsaspekterna och ska dokumenteras i complianceportalen och i risk- och sårbarhetsanalyser. Grundregeln är att information inte ska lämnas oskyddad.

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.

Kommunikation

Informationssäkerhet kommuniceras via uppdaterade rutiner, återföring av avvikelser, information på möten och e-post vid behov.

Avvikelser

Incidenter och avvikelser ska skrivas i förvaltningens avvikelsesystem. Det är informationssäkerhetssamordnaren som ska ansvara för att avvikelser analyseras och åtgärdas. Har dataskyddsombud anmält personuppgiftsincident till Integritetsskyddsmyndigheten ska det också anmälas till Regionens CERT.

Uppföljning och övervakning

Genomförda riskanalyser, avvikelser och utvärdering av skyddsåtgärder ska användas i uppföljning av informationssäkerheten genom ledningens genomgång som genomförs en gång årligen. Omvärldsanalysen ska bl a omfatta it-

utveckling, ny eller förändrad lagstiftning, standarder, marknadskrav och utveckling av teknik.

Patientnämndens förvaltning
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