Riktlinje
Process: Hantera personuppgifter/informationssäkerhet
Område: Administrativt stöd
Giltig fr.o.m: 2016-10-21
Giltig t.o.m: 2018-10-21
Faktaägare: Ann-Katrin Axelsson, Informationssäkerhetsstrateg
Fastställd av: Jan Cserpes, IT-direktör
Revisions nr: 1
Identifierare: 63533

REGION KRONOBERG

Internetbaserad kommunikation - videosamtal, telefonsamtal, chatt, delning av skrivbord och videomöte

Gäller för: Region Kronoberg

Innehållsförteckning

Det är varje användares ansvar att det personliga *Skype Företags*-kontot från Region Kronoberg, används utifrån dessa riktlinjer och med gott omdöme.

1 Inledning

Dokumentens syfte är i första hand att skydda mot följande:

- Informationsförlust genom att användaren använder funktioner på ett oaktsamt eller otillåtet sätt.
- Informationsförlust genom att applikationer hanterar och skickar data som användaren inte hade för avsikt att sprida vidare.

För användningen av ***Internetbaserad kommunikation*****,** exempelvis röst- eller videosamtal, chatt och videomöte, finns det flera olika program som kan användas. Exempel på program är Skype, Skype Företag, Lync och Facetime.

Skype Företag - Inom Region Kronoberg används för närvarade *Skype Företag* för dessa ändamål. Programvaran kan komma att ändras över tid och flera kan komma att bli godkända, men riktlinjerna gäller oavsett programvara. I detta dokument används *Skype Företag* som exempel på programvara.

Skype Företag är en virtuell anslutning mellan dig och den/de du arbetar med, som gör det möjligt att prata, skicka snabbmeddelande (chatt), videomöte, dela skrivbord och program samt samarbeta i realtid direkt från datorn eller någon annan mobil enhet.

Om inte kommunikationen lever upp till kraven på stark autentisering och krypterade överföring medför detta att det finns begränsningar i hur känsliga uppgifter som är sekretessbelagda, exempelvis patientuppgifter, personuppgifter eller andra sekretessbelagda uppgifter får hanteras i denna lösning.

2 Ansvar

Verksamhetschefen har ansvar för informationsbehandlingen inom sin verksamhet. I det ingår att information och utbildning ska ges till verksamhetens personal för användning av aktuell programvara.

När man använder sig av *Skype Företag* uppträder man som representant för Region Kronoberg.

Det är varje användares ansvar att det personliga *Skype Företag*-kontot från Region Kronoberg används utifrån dessa riktlinjer och med gott omdöme.

3 Informationssäkerhet

3.1 Känslig information

Vad som är känslig information beror på situationen och verksamheten. Det kan exempelvis röra sig om patientuppgifter, personalärenden, upphandling eller annan information som inte andra än de som direkt berörs ska ha tillgång till.

3.2 Krav på säkerhetslösningarna

Informationsklassificering – Beroende på vilken information som ska hanteras blir kraven olika. Om känsliga personuppgifter ska hanteras så ställer det högre krav på säkerhetslösningarna.

Riskanalys – Inför att en ny eller förändrad tjänst eller programvara för internetbaserad kommunikation ska användas inom Region Kronoberg ska en riskanalys genomföras.

Legitimering - Om ett videosamtal eller videomöte ska ersätta ett vanligt fysiskt besök i vården ska patienten identifiera sig först, exempelvis med mobilt bank-id. På motsvarande sätt som patienten identifierar sig med en fysisk legitimation vid det vanliga besöket.

4 Användning av Internetbaserad kommunikation

Exempelvis *Skype Företag*, som är den programvara som IT-avdelningen tillhandahåller inom Region Kronoberg för närvarande.

4.1 Chatt (snabbmeddelanden)

Chattfunktionen i *Skype Företag* uppfyller inte de krav på hantering av känsliga uppgifter som ställs i personuppgiftslagen och patientdatalagen. Chattfunktionen är heller inte att likställa informationssäkerhetsmässigt med ett telefonsamtal.

Chattkonversationen kan sparas i Outlook.

Patientuppgifter och andra sekretessbelagda uppgifter får inte hanteras i chatten.

4.2 Röst- och videosamtal

Röst- och videosamtal är informationssäkerhetsmässigt att betrakta som ett telefonsamtal med rörlig bild i likhet med vanlig telefoni och videokonferenser. Tekniken i *Skype Företag* är tillräckligt säker för att hantera känsliga uppgifter, men precis som vid telefoni måste man försäkra sig om att man inte lämnar ut uppgifter till en person som inte är behörig att ta del av den.

Inom Region Kronoberg eller mellan olika vårdgivare

Vid röst- eller videosamtal rörande patient- eller personuppgifter eller vid upphandling där sekretessbelagda uppgifter avhandlas ska man noggrant kontrollera att alla deltagare i konferenssamtalet är igenkända och att varje part kontrollerat att dörrar till konferensrum eller motsvarande är stängda. Patient och/eller anhöriga som ska delta i röst/videosamtal ska samtycka till detta.

Mellan Region Kronoberg och patient

Vid röst- eller videosamtal mellan en medarbetare inom Region Kronoberg patient, kan patienten behöva identifiera sig.

Om samtalet avser en vårdkontakt, så som rådgivning, ersätter ett vanligt besök inom vården **ska** patienten identifiera sig.

Inspelning av röst- eller videosamtal är inte tillåtet om patientuppgifter eller andra sekretessbelagda uppgifter hanteras i samtalet.

4.3 Dela skrivbord eller applikation

Vid användning av funktionen ”dela skrivbord” kan det vara bra att tänka på att mötesdeltagarna ser lika mycket som om de stod bredvid dig och tittade på din skärm. Om du till exempel får en aviseringsruta som visas när du får mail kan de övriga mötesdeltagarna se detta. För att undvika detta kan du istället för att dela skrivbord dela enbart det program som du vill visa. Övriga saker du eventuellt har uppe på skrivbordet kommer då inte synas.

Vid ”dela skrivbord” rörande patient- eller personuppgifter eller vid upphandling där sekretessbelagda uppgifter avhandlas ska man noggrant kontrollera att alla som har tillgång till det delade skrivbordet är behöriga. Var noga med hur skärmar är placerade så att inte obehöriga kan ta del av informationen utanför rummet.

Det är inte tillåtet att använda funktionen dela skrivbord eller dela applikation för att tillgängliggöra och visa patientuppgifter eller andra sekretessbelagda för personer som inte behöver dem för sina arbetsuppgifter.

4.4 Överlåta kontrollen (så kallad fjärrstyrning)

Det är endast tillåtet att överlåta kontrollen av applikationer eller skrivbord till deltagare inom Region Kronoberg. Du har ett fortsatt ansvar för vad som sker på datorn och i program om även om du lämnat över kontrollen till någon annan

Det är inte tillåtet att överlåta till annan person att fjärrstyra en dator med öppna/inloggade applikationer som innehåller/visar patientuppgifter eller andra sekretessbelagda uppgifter

4.5 Videomöte

4.5.1 Möte utan känslig information

Vid möten utan känslig information ska de tjänster (programvaror) som IT erbjuder för distansmöten användas.

4.5.2 Möte med känslig information

Vid ett distansmöte där känslig information diskuteras/presenteras måste mötesdeltagarna se till att endast de som har rätt till och direkt behov av uppgifterna har möjlighet att ta del av uppgifterna.

Vid möten med känslig information ska de tjänster (programvaror) som IT erbjuder för distansmöten användas.

Om sekretessbelagd information lämnas till mötesdeltagare från andra vårdgivare/organisationer ska den som lämnar ut uppgifterna ha gjort en men-/sekretessprövning för att se att det inte föreligger sekretess gentemot övriga mötesdeltagare. Detta gäller oavsett om utlämnandet sker muntligen eller skriftligen.

Använd en plats där inga andra än deltagarna kan se och höra vad som avhandlas.

4.5.3 Deltagande av patient och/eller anhörig (t ex samordnad vårdplanering)

När patient och/eller anhörig ska delta på distansmöten, detta kan vara aktuellt vid en samordnad vårdplanering. Samma lagstiftning, såsom offentlighets- och sekretesslagen, gäller oavsett om mötet sker fysiskt, via telefon eller via av Region Kronoberg tillhandahållen teknik.

Det är viktigt att det finns rutiner på vårdenheten hur distansmöten får och ska användas i kontakt med patient och/eller anhörig.

Tänk på att

- ✓ Patienten är den som kan samtycka till att en anhörig får delta på ett distansmöte till exempel vid en vårdplanering.

- ✓ Efter att patienten pekat ut vilken/vilka anhöriga som ska delta ska de anhöriga få information om hur de ansluter till distansmötet.

- ✓ Det är viktigt att den anhöriga får information om förutsättningarna för mötet och om det kommer att diskuteras uppgifter som omfattas av sekretess. Den anhöriga har ingen tystnadsplikt men det är viktigt att den anhöriga förstår att hen ska använda en plats där inga andra än deltagarna kan se och höra vad som avhandlas.

- ✓ Inför mötet är det viktigt att ha rutiner hur patient och/eller anhörig identifieras så att det är säkerställt att det är rätt personer som deltar i mötet. Patienten kan t.ex. identifiera sig genom att sitta tillsammans med hälso- och sjukvårdspersonalen eller att patienten sedan tidigare är känd. Patienten får sedan i sin tur identifiera de anhöriga som ansluter till mötet.