Upprättare: Lisa M Knutsson Fröjd

Fastställare: Johan Sörensson

Informationssäkerhet. Digital kommunikation - videosamtal, telefonsamtal, chatt, delning av skrivbord och videomöte - Rutin. Region Gävleborg

Innehåll

1. Syfte och omfattning

Rutinens syfte är i första hand att skydda informationsförlust genom att användaren använder funktioner på ett oaktsamt eller otillåtet sätt och informationsförlust genom att applikationer hanterar och skickar data som användaren inte hade för avsikt att sprida vidare.

2. Allmänt

Digitala tjänster och tekniska plattformar ska alltid hanteras utifrån ett patient- och informationssäkerhetsperspektiv och följa gällande lagar, förordningar och föreskrifter. All digital kommunikation, som sker synkront eller asynkront, ska hanteras utifrån dessa kriterier och avser exempelvis autentisering av användare, spårbarhet samt säker hantering och lagring av personuppgifter.

För användningen av digital kommunikation, exempelvis röst- eller videosamtal, chatt och videomöte, finns det flera olika program som kan användas. Rutinen gäller oavsett programvara.

Det finns begränsningar i hur känslig information exempelvis sekretessbelagda information, integritetskänsliga personuppgifter och känsliga personuppgifter får kommuniceras i digitala kommunikationskanaler.

Du kan få inbjudningar av andra organisationer till digitala möten som till exempel Microsoft Teams, Zoom och då har du möjlighet att delta via webbläsaren. Se dock alltid till att du **inte kommunicerar känslig information i dessa tjänster om du inte kan säkerställa att lag och säkerhetskrav kan säkerställas**. Se Informationssäkerhet - Direktiv för lagring och kommunikation i digitala kanaler

3. Ansvar och roller

3.1. Stabsdirektör

Stabsdirektören ska årligen eller vid behov fastställa denna rutin.

3.2. Informationssäkerhetsenheten

Informationssäkerhetsenheten skall årligen eller vid behov uppdatera denna rutin.

3.3. Informationsägare

Informationsägaren ansvarar för att denna rutin efterlevs. Rollen som informationsägare är ett chefsansvar och gäller i första hand förvaltningschefer och funktionsansvariga direktörer, verksamhetschefer och avdelningschefer. För mer information se: Informationssäkerhet - Direktiv för ansvar och roller. Region Gävleborg

3.4. IT-förvaltningen

Tillhandahåller digitala kommunikationsverktyg och ansvarar för den IT-tekniska säkerheten i respektive verktyg.

3.5. Medarbetare inom Region Gävleborg

Varje enskild medarbetare på Region Gävleborg ska känna till och tillämpa denna rutin vid digital kommunikation.

4. Beskrivning

Direktivet *Informationssäkerhet - Direktiv för lagring och kommunikation i digitala kanaler* ger en övergripande vägledning för hur olika typer av information får kommuniceras via digitala kanaler.

4.1. Användning av digital kommunikation

Med användning av digital kommunikation avses videosamtal, röstsamtal, chatt, videomöten och delning av skrivbord, exempelvis med Skype Företag - Region Gävleborg.

SMS hanteras inom vården av särskild rutin: *11-138640 Informationssäkerhet - SMS-påminnelser - användning, Hälso- och sjukvård Region Gävleborg*

4.1.1. Chatt (snabbmeddelanden)

De chattfunktioner som tillhandahålls i Region Gävleborg (Skype, Teams etc.), med undantag från Min vård Gävleborg, uppfyller inte de krav på hantering av känsliga uppgifter som ställs i dataskyddsförordningen och patientdatalagen.

Chattfunktionen är inte att likställa informationssäkerhetsmässigt med ett telefonsamtal. Chattkonversationen kan sparas i exempelvis Outlook.

Konfidentiell information, känsliga personuppgifter och integritetskänsliga personuppgifter och information som omfattas av sekretess får inte hanteras i chatten.

4.1.2. Röst- och videosamtal

Röst- och videosamtal är informationssäkerhetsmässigt att betrakta som ett telefonsamtal med rörlig bild i likhet med vanlig telefoni. Olika digitala mötestjänster tillhandahåller olika nivåer av säkerhet som krävs enligt lagar och förordningar.
Innan du genomför ett röst- eller videosamtal ansvarar du att informera dig om den teknik som används och vilken typ av information som kan hanteras där. 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.

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

Inom Region Gävleborg eller mellan olika vårdgivare
Vid röst- eller videosamtal där konfidentiell information, känsliga personuppgifter och integritetskänsliga personuppgifter och information som omfattas av sekretess 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 Gävleborg och patient
Vid röst- eller videosamtal mellan en medarbetare inom Region Gävleborg och patient, ska patienten identifiera sig.
Om samtalet avser en vårdkontakt, så som rådgivning, ersätter ett vanligt besök inom vården måste medarbetare inom Region Gävleborg säkerhetsställa patientens identitet.

4.1.3. 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 e-post 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” där konfidentiell information, känsliga personuppgifter och integritetskänsliga personuppgifter och information som omfattas av sekretess delas ska man noggrant kontrollera att alla som har tillgång till det delade skrivbordet är behöriga att ta del av informationen. 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 annan sekretessbelagd information för personer som inte behöver dem för att utföra sina arbetsuppgifter och således inte är behöriga att ta del av informationen.

4.1.4. Överlåta kontrollen (fjärrstyrning)

Det är endast tillåtet att överlåta kontrollen av applikationer eller skrivbord till mötesdeltagare inom Region Gävleborg. 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 konfidentiell information, känsliga personuppgifter och integritetskänsliga personuppgifter och information som omfattas av sekretess. Endast i undantagsfall får extern person ha kontroll över datorer inom Region Gävleborg. Sådana fall kan handla om support från externa organisationer. I dessa fall ska det finnas personuppgiftsbiträdesavtal mellan Region Gävleborg och den externa organisationen.

4.1.5. Videomöte

4.1.5.1. Möte utan känslig information

Vid möten utan känslig information ska de tjänster (programvaror) som IT-förvaltningen tillhandahåller för distansmöten användas. När du deltar i möten som en extern part bjudit in till är det viktigt att du inte kommunicerar känslig information.

4.1.5.2. Möte med känslig information

Vid ett distansmöte där känslig (konfidentiell information, känsliga personuppgifter och integritetskänsliga personuppgifter och information som omfattas av sekretess) 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 någon av dessa tjänster nyttjas som IT-förvaltningen tillhandahåller:

- Skype för Företag – Region Gävleborg

- Min vård Gävleborg – ska i första hand användas för möte med patienter.

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. För att tillfredsställande sekretess ska erhållas, ska inga personuppgifter (personnummer) diskuteras via videomöten.

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

När det finns tvivel på att uppkopplingen är säker eller att någon deltagare inte sitter i ett utrymme som säkerhetsställer att utomstående inte kan höra vad som avhandlas är rekommenderat att endast använda video utan ljud för att istället ringa upp mötesdeltagaren via telefon för den muntliga kommunikationen.

4.1.5.3. Vårdrelaterade videomöte

Vårdgivare ska följa gällande lagar och förordningar för patientsäkerhet oavsett om vården sker fysiskt eller digitalt.

För vårdrelaterade videomöten ska punkt 4.1.5.2 beaktas.
Samtal som kan ersättas eller kompletteras av vårdande möte via nätet:

- Återbesök och behandling
- Uppföljning (medicinering, vårdplan)
- Föräldrastöd
- SIP
- Skolkonferens

För att tillfredsställande sekretess ska erhållas, ska man minimera de personuppgifter som diskuteras när webbsamtal används, personnummer ska inte förekomma.

4.1.5.4. 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 Gävleborg tillhandahållen teknik.

Det måste finnas rutiner på vårdenheten hur distansmöten får och ska användas i kontakt med patient och/eller anhörig.
Säkerhetsställ att:

- Patienten är den som samtycker 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.

När det finns tvivel på att uppkopplingen är säker eller att någon deltagare inte sitter i ett utrymme som säkerhetsställer att utomstående inte kan höra vad som avhandlas är rekommenderat att endast använda video utan ljud för att istället ringa upp mötesdeltagaren via telefon (ej högtalarfunktion) för den muntliga kommunikationen.

4.1.5.5. Inbjudan till videomöte med patienter och/eller anhöriga

Inbjudan kan skickas från medarbetarens personliga Region Gävleborg e-postadress.

Inbjudans rubrik och text ska formuleras neutralt och det får inte förekomma känsliga personuppgifter i inbjudan. Inbjudan ska därför hållas på en övergripande nivå, exempelvis: *Klicka för att delta i ditt bokade hälso- och sjukvårdsbesök.*

4.1.6. Inbjudan till möten som anordnas av andra organisationer

Det finns flertal olika mötesplattformer och olika organisationer använder olika verktyg/lösningar. Om medarbetare på Region Gävleborg blir inbjuden till ett möte av en annan organisation ansvarar man för att kontrollera att mötesplattformen har rätt nivå av säkerhet som krävs enligt lagar och förordningar. Vid osäkerhet ska man undvika att diskutera sekretessbelagd information, känsliga personuppgifter eller på annat vis konfidentiell information. Vid behov av stöd och rådgivning kontakta informationssakerhet@regiongavleborg.se eller it-support@regiongavleborg.se.

5. Plan för kommunikation och implementering

Rutinen kommer att spridas genom informationssäkerhetsrådet och publiceras på Plexus.

6. Dokumentinformation

Rutinen har tagits fram av informationssäkerhetsenheten och granskats av juridikavdelningen och säkerhet- och beredskapsavdelningen. IT-förvaltningen har varit delaktig i framtagande av innehåll. Hälso- och sjukvårdsförvaltningen har varit delaktig i framtagande av beskrivningen under 4.1.5.3 - 4.1.5.5.

7. Referenser

Dokumentnamn	Plats
Informationssäkerhet - Direktiv för ansvar och roller. Region Gävleborg.	Platina
Informationssäkerhet - Direktiv för lagring och kommunikation i digitala kanaler	Platina