RUTIN

Rutin för användning av videofunktion i Teams för digitala vårdmöten

Version 01.00
Denna rutin gäller under tiden som kommunen befinner sig i den extraordinära händelsen utifrån Covid-19, dock som längst till 2020-12-31.

Informationsklass: **Intern**
Ansvarig: Tobias Ander
Dokumentet är endast giltigt vid utskriftstillfället. Senaste giltiga versionen finns på intranat.orebro.se/informationssakerhet

Sammanfattning

Teams, en av applikationerna inom Office 365, är en lösning för att möjliggöra bland annat videosamtal, telefonsamtal, chatt och delning av skrivbord, applikationer och dokument. En analys visar att Teams har god säkerhet i stort men inte lever upp till kravet om stark autentisering.[1]

Detta medför att det finns begränsningar i hur uppgifter som är sekretessbelagda, exempelvis patientuppgifter, personuppgifter eller andra sekretessbelagda uppgifter får hanteras i denna lösning.

Inga filer med sekretessuppgifter får delas eller sparas i Teams. Chattfunktionen kan inte användas för sekretessuppgifter eftersom detta sparas i Teams. Däremot kan videosamtal användas, då samtalets innehåll inte sparas någonstans. Det är viktigt att notera att det går att se att ett samtal ägt rum mellan två parter, men inte vad som sägs i samtalet. Detta dokument innehåller instruktioner för användning av Teams i arbete som omfattas av sekretess. Tillämpning av dessa instruktioner tillfaller verksamhetschefer till personal som arbetar med sekretessuppgifter.

Omfattning/tillämpningsområde

Gäller för verksamheter inom Social välfärd som hanterar vårdmöten där sekretessuppgifter diskuteras.

Ansvar

Verksamhetschefen har ansvar för informationsbehandlingen och informationssäkerheten 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 Teams uppträder man som representant för Örebro kommun.

Det är varje användares ansvar att det personliga Teams-kontot används utifrån dessa instruktioner och med gott omdöme.

Avvikelser och personuppgiftsincidenter

Avvikelser och personuppgiftsincidenter hanteras enligt Örebro kommuns riktlinjer.

[1] Stark autentisering betyder att det måste finnas inloggningslösningar som ställer krav på att identiteten kontrolleras på minst två olika sätt, exempelvis:

1. med någonting användaren kan – t.ex. lösenord eller pinkod
2. med någonting användaren har – t.ex. certifikat, engångskoder eller mobiltelefon
3. med hjälp av användaren själv – t.ex. fingeravtryck

Riktlinje för användning av Teams

Chatt (snabbmeddelanden)

Chattfunktionen i Teams uppfyller inte de krav på hantering av känsliga uppgifter som ställs i patientdatalagen och Dataskyddsförordningen. Chattkonversationen sparas i Office 365, och får därför inte användas för sekretessklassade uppgifter.

Riktlinje: Patientuppgifter och andra sekretessbelagda uppgifter får inte hanteras i chatten.

Röst och videosamtal

Röst- och videosamtal är informationssäkerhetsmässigt att betrakta som ett telefonsamtal med rörlig bild i likhet med vanlig telefoni och videokonferenser. 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. och att varje part kontrollerat att dörrar till konferensrum eller motsvarande är stängda. Ett sätt att säkerställa att personen är den hen utger sig för är att hålla upp legitimation i bild och därmed kan mötesorganisatören verifiera att alla är kända. Patient och/eller anhöriga som ska delta i röst/videosamtal ska samtycka till detta. Samtycket kan ske muntligt vid mötets uppstart.
Vid användning av Teams så hamnar alla deltagare utanför Örebro kommun i en lobby och behöver släppas in i mötet. Detta är ett sätt att säkerställa att ingen kan smyga in obemärkt i mötet.
Riktlinje: Inspelning av röst- eller videosamtal är inte tillåtet om patientuppgifter eller andra sekretessbelagda uppgifter hanteras i samtalet.
Vid röst eller videosamtal rörande patient- eller personuppgifter där sekretessbelagda uppgifter avhandlas ska man noggrant kontrollera att alla deltagare i konferenssamtalet är igenkända.

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.

Riktlinje: Det är inte tillåtet att använda funktionen dela skrivbord eller dela applikation för att tillgängliggöra och visa patientuppgifter eller andra sekretessbelagda uppgifter.

Överlåta kontrollen (så kallad fjärrstyrning)

Det är endast möjligt att överlåta kontrollen av applikationer eller skrivbord till deltagare inom Örebro kommun.

Riktlinje: 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.

Att tänka på inför, under och efter ett Teamsmöte

Möteskallelse

När man bokar ett Teamsmöte antingen via Outlook eller direkt i Teams så kommer mötesbokningen sparas. Använd gärna ord som ”avstämning” eller ”uppföljning” i ämnes raden.

Riktlinje: Inga personuppgifter eller andra känsliga uppgifter ska kunna utläsas i kallelsen.

Mötet bokas i Outlook och genomförs sedan i Teams. Se filmen nedan för att se hur du gör för att boka, bjuda in och hålla i mötet.

SE FILMEN HÄR – Boka möte i Outlook

Mötets start

Alla deltagare utanför Örebro kommun hamnar först i en ”lobby”. Det betyder att du behöver släppa in dem i mötesrummet innan samtalet kan påbörjas. Detta är en åtgärd för att säkra att ingen obehörig omärkt ska kunna komma in i samtalet, samt att mötesorganisatören kan verifiera att samtliga personer i samtalet är identifierade.

Att tänka på under mötet:

- Sitt i ett enskilt rum och utan störande ljud. Gäller samtliga deltagare på mötet.
- Säkerställ att samtliga deltagare är kända i mötet. Har man träffats förut räcker det med att man noterar att personen är i rummet. Är det första gången man träffas så kan man visa en legitimation i bild för att verifiera att man är den man utger sig för.
- Stäng av mikrofonen när du inte pratar, så undviker du rundgång i mötet.
- Tänk på att om du delar din skärm ser mottagaren allt som du ser. Var noga med att du visar rätt saker och stänga ner så många program som möjligt i bakgrunden.
- All dokumentation sker i journalsystem, INTE i Teams

Ej tillåtet under mötet
Det är inte tillåtet att föra konversationer med sekretessuppgifter i chatten under mötet – eftersom chatten sparas

Det är inte tillåtet att dela skärm där patientuppgifter eller annan sekretessbelagd uppgift visas – eftersom det inte går att kontrollera om annan deltagare tar kopia

Det är inte tillåtet att spela in mötet – eftersom denna inspelning sparas och skulle kunna visas igen av obehöriga

Att tänka på efter avslutat möte:

- Säkerställ att mötet är avslutat genom att trycka på röd telefonlur.