**OBS! Utskriven version kan vara inaktuell.**
Senaste versionen hittar du via intranätet under "styrande dokument" eller vårdgivarwebben.

Region Halland

Gäller för: Region Halland

# Videokonferens, distansmöte och chatt

**Hitta i dokumentet**

Syfte
Allmänt
Ansvar
Patientuppgifter och annan sekretessbelagd information
Delta i distansmöte med externa arrangörer
Användning
Övrigt

## Syfte
Rutinen är framtagen som ett stöd för att använda tekniken på ett sätt som uppfyller Region Hallands krav på informationssäkerhet.

## Allmänt
Region Halland tillhandahåller flera applikationer för videokonferens och distansmöten, exempelvis Microsoft Teams, Visiba Care, Platform24 och Cisco Jabber Video.

I applikationerna finns även funktioner för chatt, tal/röst, delning av program/skrivbord, fjärrstyrning, inspelning mm.

## Ansvar
Region Hallands videokonferens- och chattapplikationer är tjänsteverktyg och ska användas med ansvar och sunt förnuft. Användaren ska alltid göra en bedömning och tillämpa tekniken så att grundläggande regler för hantering av allmän handling, arkivering och sekretess tillämpas.

### Personligt ansvar
Varje användare är ansvarig för sitt användarkonto och hur detta används. Det är användarens ansvar att lösenordet är skyddat och hålls hemligt för omgivningen. Det är användarens ansvar att logga ut, alternativt låsa datorn, så att ingen obehörig kan använda tjänsten i någon annans namn. Loggar man in med SITHS-kort ska detta vara under uppsikt.

### Chefsansvar
Verksamhetschefen eller motsvarande är ansvarig för att hanteringsrutiner är kända och efterlevs när applikationerna inkluderas i verksamhetsprocessen. Utifrån det användningsområde som tjänsten ska fylla, är det chefens ansvar att hanteringsrutiner efterlevs och att personalen har tillgång till lämplig utrustning och lokaler.

Vid anställdas missbruk av verktygen har ansvarig linjechef skyldighet att stävja detta enligt arbetsrättsliga regler och lokala rutiner.

Gäller för: Region Halland

## Patientuppgifter och annan sekretessbelagd information

Datatrafiken under ett distansmöte är krypterad, vilket innebär att det är möjligt att utbyta patientuppgifter och annan sekretessbelagd[1] * information över video- och talsamtal.

Chattfunktionen (snabbmeddelande) får **inte** användas för att utbyta patientuppgifter och annan sekretessbelagd information, då denna sparas i konversationshistoriken. Tänk också på att deltagare **som lämnat** en konferens kan exempelvis Teams fortfarande kommer att se chattmeddelanden som skickas i möteschatten.

Presentationsläget (dela skrivbord eller dela program) **får användas**, dock ska man vara särskilt **försiktig** så att inte information visas, som inte är avsedd för alla deltagare. Se rubrik Presentationsläge - visa skrivbord eller program

Inspelningsfunktionen i Teams får **inte** användas för att spela in video- och talsamtal innehållande patientuppgifter eller annan sekretess, se rubrik inspelning.

Transkriberingsfunktionen får **inte** användas när mötet gäller patientuppgifter eller annan sekretessbelagd information då denna sparas hos mötesorganisatören.

## Delta i distansmöten med externa arrangörer

I de fall du blir inbjuden till ett distansmöte med en extern arrangör bör du alltid fråga arrangören om det går att ansluta till mötet via Teams. Det är inte alla applikationer som fungerar att använda när man är uppkopplad på regionens nät, ibland behövs åtgärder för att det ska gå att ansluta.

Utöver de distansmötesapplikationer som Region Halland tillhandahåller finns det flera andra. Dessa har olika säkerhetsgrad och du som mötesdeltagare ansvarar för att kontrollera så att ingen utomstående kan ta del av eventuell sekretessbelagd information via mötet. Du ska endast delta i distansmöten där du fått en personlig inbjudan (dvs. inte offentliga möten).

Nedan listas de applikationer som redan är konfigurerade så att de går ansluta till via regionens nät. Om du blir inbjuden till ett möte i en annan än dessa så bör du testa åtkomsten i god tid och lägga ett ärende till ServiceDesk om det inte fungerar.

- Teams
- Cisco WebEx
- Skype
- Compodium
- Google Meet
- Acano
- Video via digitaltolk
- GoToMeeting

[1] Säkerhetsskyddsklassificerad information (exempelvis försvarssekretess,15 kap 2 §) är inte tillåtet att utbyta i någon form via de här tjänsterna. Mer information kan du få via säkerhetsskyddschefen.

- Zoom
- Platform24

## Användning

Nedan finns ett antal exempel på användningsområden. Läs mer på intranätet om distansmöten (länk).

**Distansmöten, videomöten och konferens**
Kommunikationstjänsten möjliggör möten på distans där ett virtuellt mötesrum skapas. Grundprincipen är att betrakta det digitala mötet som det förlängda mötesrummet och att tillämpa samma förhållningssätt som vid ett fysiskt möte.

Samtliga mötesdeltagare ansvarar för att det bara är behöriga deltagare vid mötet. För att mötet ska bli givande för alla deltagare är det väsentligt att varje deltagare befinner sig i en ostörd miljö. Ljudkvaliteten vid ett virtuellt möte är en grundläggande framgångsfaktor, därför rekommenderas headset med mikrofon.

Medarbetare som arbetar på distans ska även beakta rutin:
Distansarbete – informationssäkerhet

**Snabbmeddelande/chatt**
Snabbmeddelanden/chatt är en enklare form av mejl och följer samma grundprinciper. Funktionen är endast avsedd för information av tillfällig art som inte ska arkiveras. Det är användarens ansvar att radera konversationshistoriken alternativt arkivera och diarieföra konversationer, om det faller inom ramen för allmän handling som ska diarieföras. I Teams kan man endast radera sina egna inlägg.

**Presentationsläge - visa skrivbord eller program**
Användare som presenterar information/material ansvarar för att endast visa information som deltagarna är behöriga att se, eftersom samtliga deltagare kan göra en skärmdump av det som presenteras på mötet. Välj i första hand att bara dela ut aktuellt dokument eller program istället för att dela skrivbord. Om skrivbordet visas ska program och dokument som inte är relevanta under mötet stängas ner. Ingår externa deltagare i mötet och informationen kan sparas ner av dem är det att betrakta som ett utlämnande av handling.

Tänk på att om du delar skrivbordet - kan mötesdeltagarna se lika mycket som om de står bredvid dig och tittar på din datorskärm. Om du till exempel får en aviseringsruta varje gång du får ett mejl kan alltså mötesdeltagarna se ämne och de första orden i mejlet.

Säkerställa att det är rätt deltagare som är anslutna till mötet innan man delar skärm/program.

**Överlåta kontroll, fjärrstyrning av annan dator**
I Teams finns möjlighet att överlåta kontroll, vilket innebär att datorn kan fjärrstyras av en annan deltagare. Det är endast möjligt att överlåta kontroll av program eller skrivbord till deltagare internt inom Region Halland.

*Även om kontrollen överlåts till annan deltagare, är den inloggade användaren ansvarig och ska därför övervaka det som sker.*

**Bifoga filer**
Användaren ansvarar för att endast skicka filer som mottagaren eller mottagarna är behöriga att ta del av. Bifogade filer lagras lokalt där ingen backup tas. Det är användarens ansvar att flytta filerna till lämplig lagringsyta.

*I de flesta fall är det mer lämpligt att hänvisa till en fil lagrad på exempelvis gemensam filyta genom att bifoga en länk till filen.*

**Inspelning**
För de användare som har presentationsmöjligheter finns även inspelningsfunktion. Utgångsläget är att inspelning inte ska göras. Finns behov av att spela in och lagra mötet eller presenterat material, ska detta klart framgå.

Om man vill spela in ett möte ska det tydliggöras för samtliga deltagare om att en inspelning av mötet görs. Inspelningens syfte och orsak ska vara tydligt redogjort för alla deltagare.

Det är användarens ansvar att flytta inspelningen till lämplig lagringsyta. Inspelningar som görs är att betrakta som allmän handling och ska hanteras enligt gällande dokumenthanteringsplan.

*Konversationer innehållande patientuppgifter eller annan sekretess får inte spelas in.*

## Övrigt

**Hot**
Kontakta ansvarig chef om meddelande innehåller hot eller liknande. Ta inte bort konversationen. Avsändaren kan eventuellt spåras.

**Privat användning**
Privat användning av Teams får ske endast undantagsvis och i begränsad omfattning för att lösa arbetstagarens personliga behov, på samma sätt som exempelvis tjänstemobil får användas för att exempelvis lösa ett hastigt uppkommet problem i skolan eller annan familjeangelägenhet. Övriga distansmötestjänster får inte användas privat överhuvudtaget.

Teams får däremot inte användas regelmässigt för privat bruk. Användningen får naturligtvis inte heller ske på sådana tider eller i sådan omfattning att det inkräktar på arbetet.

Gäller för: Region Halland

Servicedesk tillhandhåller ingen support eller stöd för privat användning.

Tänk på att Region Halland ingår i avsändaradressen. Var därför noggrann med hur du uttrycker dig för att inte ge intryck av att du representerar Region Halland vid privat användning. Din användning kan också innebära att uppgifter kan komma att betraktas som allmän handling.

**Hantering vid missbruk**
Missbruk av Regionens IT-resurser kommer att beivras genom arbetsrättsliga åtgärder. Det kan röra sig om att användaren har använt sitt konto på ett sätt som strider mot lag eller Region Hallands riktlinjer. Om det finns misstanke om brott är Region Hallands förhållningssätt att polisanmäla det inträffade.

## Uppdaterat från föregående version

Lagt till att:

- Transkriberingsfunktion inte får användas när mötet behandlar patientuppgifter eller annan sekretess.
- Förtydligat avsnitt om privat användning.
- Tagit bort referenser till Skype
- I övrigt mindre redigeringar för att öka tydlighet och läsbarhet.

Ersätter version 2021-07-06