Digitala möten i socialtjänsten, stöd med anledning av covid-19

Covid-19 har understrukit behovet av digitala lösningar i socialtjänsten. Även under pandemin behöver socialtjänsten ge råd och stöd, utreda behov och följa upp insatser. För att öka tillgängligheten för invånare, brukare/klienter och minska risken för smitta erbjuds därför digitala möten i större omfattning.

Men att erbjuda möten digitalt är inte alltid enkelt. Flertalet av de digitala lösningar som finns på marknaden saknar lämplig skyddsnivå. Många tjänster har inte stark autentisering (tvåfaktorsautentisering), och erbjuder inte alltid adekvat skydd för överföring av känsliga personuppgifter över internet. Det är inte heller alla typer av möten som passar att genomföra digitalt givet brukarens/klientens behov.

Sveriges Kommuner och Regioner (SKR) har därför tagit fram det här stödmaterialet för att underlätta bedömning om ett digitalt möte kan genomföras, vilka digitala tjänster som kan användas och vad man ska tänka på för att ett digitalt mötet ska ske på ett säkert sätt. Stödet riktar sig främst till verksamhetsansvariga i socialtjänsten och IT-ansvariga.

Inför användning av digitala möten behöver socialtjänsten:

1. Identifiera vilken typ av information som behandlas i olika typer av möten
2. Undersöka vilka tjänster som finns och hur de uppfyller säkerhetskraven
3. Besluta vilka tjänster som ska användas för olika typer av möten
4. Bedöma lämplighet utifrån det enskilda mötet och individens behov/situation

Därför behövs digitala möten

Enligt Folkhälsomyndighetens föreskrifter och allmänna råd ska alla verksamheter i Sverige säkerställa lämpliga åtgärder för att undvika smittspridning av covid-19. En ökad användning av digitala möten är ett sätt för socialtjänsten att omsätta Folkhälsomyndighetens föreskrifter och allmänna råd i praktiken. Möjligheten till digitala möten efterfrågas också av invånare, anhöriga, medarbetare och berörda samverkansaktörer.

Behovet av digitala möten finns inom alla områden i socialtjänsten. Det kan till exempel handla om utredningssamtal med vårdnadshavare, barn, unga eller vuxna, och uppföljningssamtal i särskilda boenden eller vid familjehemsplaceringar. Det kan också handla om möten med samverkansaktörer såsom skolan, Arbetsförmedlingen, Försäkringskassan och hälso- och sjukvården.

Juridiska förutsättningar vid digitala möten

I socialtjänstens möten behandlas normalt uppgifter om brukare/klienter eller annan person som dels är sekretessreglerade enligt offentlighets- och sekretesslagen (OSL) och dels är känsliga personuppgifter enligt dataskyddsförordningen (GDPR). Det gäller oavsett om mötet sker fysiskt eller genom en digital tjänst av typen videokonferens. I grunden gäller alltså samma regelverk för fysiska och digitala möten. Det finns dock några aspekter som skiljer digitala möten från fysiska, och där socialtjänsten behöver vidta särskilda åtgärder.

Bedöm laglighet utifrån dataskyddsförordningen

Ett digitalt möte innebär alltid att det sker en behandling av personuppgifter, bara genom den överföring av ljud och bild som sker mellan deltagarna i samtalet. När sekretessbelagda uppgifter utväxlas finns därmed en risk att dessa röjs. Socialtjänsten måste därför utifrån dataskyddsförordningen bedöma bl.a. laglighet, rättslig grund för behandling av uppgifter och om lagstöd finns för behandling av känsliga personuppgifter. Känsliga personuppgifter enligt dataskyddsförordningen är t. ex uppgifter om hälsa, etniskt ursprung, sexuell läggning, sexualliv, politiska åsikter och religiös eller filosofisk övertygelse.

Det spelar ingen roll om uppgifterna lagras hos någon av deltagarna, hos leverantören av tjänsten eller om all information raderas direkt efter det att samtalet är slut. Även om uppgifterna inte sparas, finns en risk att uppgifterna röjs om själva överföringen i tjänsten inte kan ske tillräckligt skyddat.

Säkerställ identiteten hos motparten

I det digitala mötet behöver socialtjänsten kontrollera motpartens identitet om det handlar om en brukare/klient eller samverkanspart som socialtjänsten inte träffat tidigare eller om det är oklart vem som deltar i mötet. Detta är viktigt för rättssäkerheten. Det säkraste sättet är e-legitimation, men om den möjligheten inte finns kan det räcka att motparten visar personlig legitimation i kameran och att handläggaren noterar att det har gjorts.

Säkerställ att mötet sker i ostörd miljö

Vid ett fysiska möte är alla i samma lokal vilket normalt innebär att ingen annan kan höra samtalet. I det digitala mötet befinner sig deltagarna på olika platser. Då är det viktigt att socialtjänsten säkerställer att rätt personer är med i det digitala rummet och att obehöriga inte kan ta del av samtalet.

Dokumentation kan ske på vanligt sätt

Dokumentation av samtalet vid digitala möten görs på vanligt sätt, som vid fysiska möten. Gällande inspelning av samtal gäller särskilda regler som inte tas upp i det här stödmaterialet.

Bedömning av digitala tjänster

Inför användning av digitala tjänster bör socialtjänsten göra en bedömning av vilka krav på säkerhet som ska ställas. En analys bör göras som utgår ifrån:

- verksamhetsbehov
- funktionalitet
- vilken typ av information som ska hanteras i tjänsten
- om tjänsten når upp till säkerhetskraven
- vilka alternativa tjänster som finns
- en sammantagen behovs- och riskanalys

Dessa aspekter ingår i det systematiska informationssäkerhetsarbetet och dataskyddsarbetet som bör finns inom alla kommuner och regioner. Socialtjänsten kan behöva samråda med dataskyddsombudet eller organisationens IT-funktion för att få stöd i bedömningen.

Vid analys av vilken typ av information som kommer hanteras kan socialtjänsten utgå från tidigare fysiska möten – förekommer personuppgifter, känsliga personuppgifter eller sekretessbelagd information? Informationen behöver också säkerhetsklassas – det vill säga värderas utifrån:

- konfidentialitet – hur säkerställs att obehöriga inte kommer åt skyddsvärd/sekretessbelagd information?
- riktighet – hur säkerställs informationen inte ändras/förvanskas?
- tillgänglighet – hur säkerställs att informationen är tillgänglig för behöriga i förväntad utsträckning?

Vid analys av säkerhetskrav bör hänsyn tas till om informationen lagras hos leverantören och om överföringen av information är krypterad.

Informationssäkerhetsarbetet handlar om att vara medveten om riskerna och göra medvetna val. Vid behovs- och riskanalysen behöver hänsyn tas till hur stor risken är i förhållandet till att uppnå en viss säkerhetsnivå. Vilka konsekvenser får det för brukaren/klienten och vilka åtgärder behövs för att minimera riskerna? Här är det också viktigt att väga in konsekvenserna. Vad är alternativet om tjänsten inte kan tillhandahållas?

Viktigt att dokumentera analys och beslut

Det är viktigt att dokumentera både analys och beslut om användning av digitala tjänster. Om avsteg görs och bedömningen är att använda lösningar med en lägre säkerhetsgrad, behöver det beslutet dokumenteras och fattas på rätt nivå, förslagsvis på kommunlednings- eller förvaltningsnivå. Beslutet behöver också tydliggöra vad som gäller i kommunen/organisationen för dessa typer av möten under rådande omständigheter.

Bedömning utifrån typ av möte och individens behov

Vid utredningssamtal mellan socialtjänst och brukare finns det stor risk att känslig information hanteras. Däremot är det inte alltid nödvändigtvis så, till exempel vid vissa uppföljningssamtal. Ibland kan det till och med vara lättare att genomföra samtalet digitalt.

Det kan också vara så att även om informationen inte omfattas av känsliga uppgifter, kan det finnas andra skäl till att mötet bör ske fysiskt. Inför varje möte bör därför ansvarig socialsekreterare/handläggare tillsammans med chef bedöma om det är lämpligt att genomföra mötet fysiskt eller digitalt utifrån mötets karaktär och individens behov/situation. Ibland är fysiska möten nödvändiga. Skyddsbedömningar gällande barn ska till exempel inte ske digitalt.

Checklista om du använder en tjänst utan stark autentisering

Flera kommersiella tjänster som Skype, Teams, Zoom och Facetime kan ha krypterad överföring, men saknar ofta stark autentisering. För möten som inte hanterar känslig information kan det gå bra att använda dessa tjänster, men det måste alltid göras en bedömning om vilken typ av information som kommer att hanteras.

Tänk på följande om du använder tjänster som saknar stark autentisering:

- Gör inte möten offentliga, använd gärna lösenord till mötet eller låt användaren vänta ”utanför” för att bli insläppt.
- Dela aldrig dokument med känslig information via appar eller i chattfunktioner, varken med den enskilde eller andra aktörer.
- Se till att medarbetare som arbetar hemifrån ansluter sig till kommunens VPN, och att de säkerställer att miljön de sitter i tar hänsyn till integritet och sekretess.
- Tänk över hur den enskilde ska identifiera sig (till exempel genom att visa upp sin legitimation i bild vid nybesök).

Mer stöd från SKR

KLASSA – verktyg för informationssäkerhetsklassning, gratis för SKR:s medlemmar

Vägledningar för molntjänster