VEJLEDNING

# VEJLEDNING TIL SKÆRMBESØG

## Kommunale sundheds-, ældre- og socialområder

**Senest opdateret den 24. april 2020**

**Indholdsfortegnelse**

# 1 Indledning

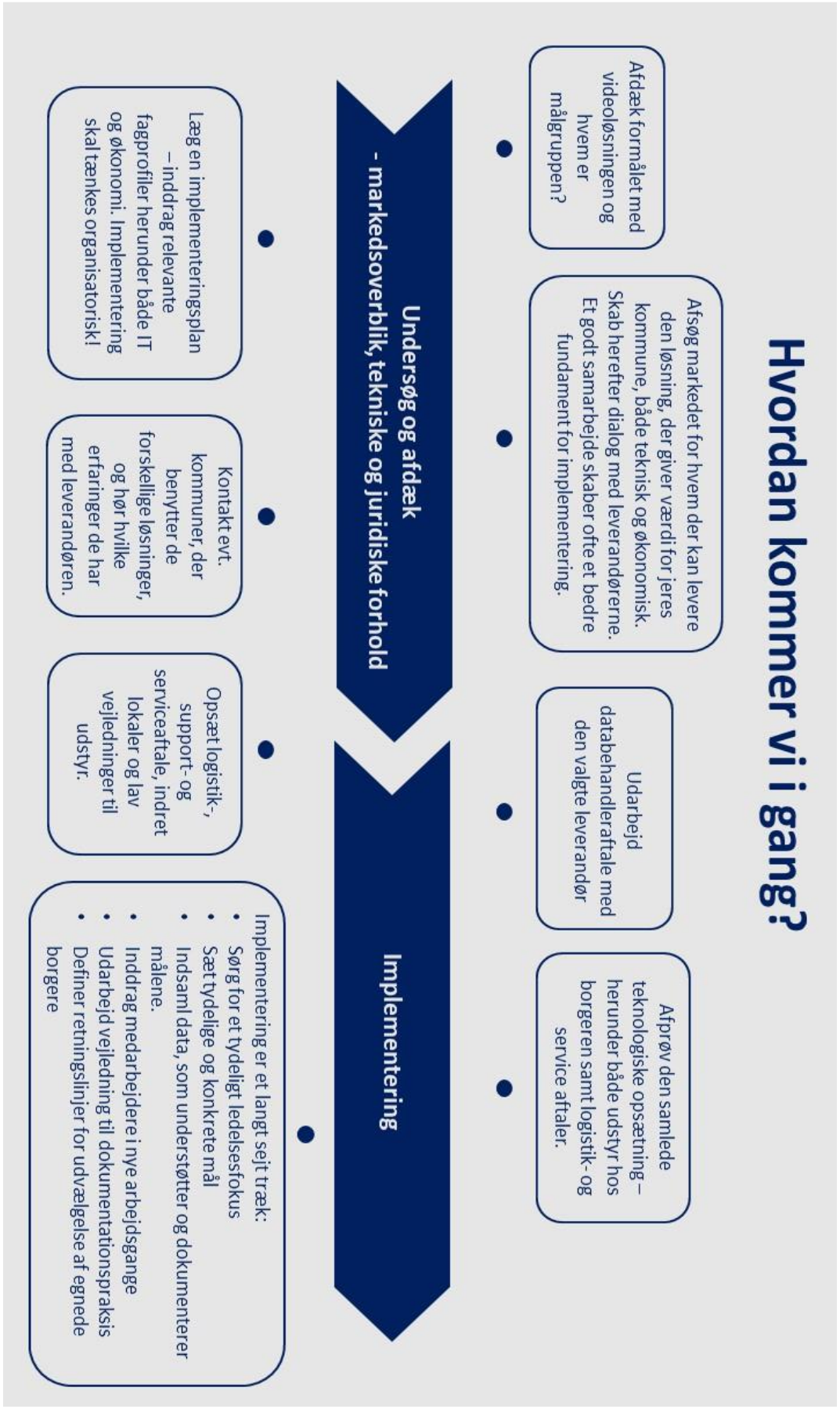
Brugen af skærmbesøg i den kommunale praksis på sundhed-, ældre- og socialområderne giver nye muligheder for udvikling af kvalitet i indsatserne og den daglige arbejdstilrettelæggelse, når det gribes an på en hensigtsmæssig måde. Flere kommuner har arbejdet med dette i en årrække, og rapporter[1,2,3] har dokumenteret, hvordan skærmbesøg medfører en række gevinster for både kommunen, borgere og medarbejdere såsom fleksibilitet i borgerens hverdag og mere fokuserede møder med borgerne.

Øget internethastighed, -dækning og teknologimodenhed de seneste år har introduceret nye spillere og muligheder på markedet. Med dem følger et øget behov for tekniske afklaringer og sammenhænge, ligesom den fornødne jura og sikkerhedsforanstaltninger skal være på plads.

Denne vejledning adresserer primært de tekniske og juridiske aspekter ved arbejdet med skærmbesøg i kommunerne, og har til hensigt at gøre det nemmere at komme godt i gang.

Vejledningen rummer dels en procesmodel (se figur 1 på næste side) med væsentlige trin i implementeringen af skærmbesøg og dels en række tjeklister og anbefalinger til at komme omkring tekniske og juridiske forhold samt leverandører, logistik mm.

[1] Rambøll og Aalborg Kommune, Evaluering: Projekt Online Bostøtte – Oktober 2016
[2] RUC og VIVE, Skærmopkald i hjemme- og sygepleje - 2018
[3] PA Consulting, Analyse af skærmbesøg og virtuelle konsultationer – December 2018




*Figur 1: Hvordan kommer vi i gang? - Illustration af KL's Center for Velfærdsteknologi*

# 2 Teknisk opsætning og fysiske rammer

Følgende afsnit omhandler kommunens tekniske set-up, hardware, samt elementer, som kan påvirke brugeroplevelsen set fra et teknisk synspunkt. Det kan være mobil netværksdækning, integration med kommunens eget AD-system, firewall etc., som skal løses for at skabe den bedste oplevelse for borgere og medarbejdere.

## 2.1 Internetforbindelse

Skærmbesøg og internetforbindelse hænger uløseligt sammen. Kvaliteten af samtalen mellem kommune og borger afhænger bl.a. af hastigheden på internetforbindelsen, og det kan være en stor begrænsning, hvis denne ikke fungerer optimalt. Mobil- og bredbåndsdækning er i størstedelen af landet velfungerende, men i visse kommuner kan dækningen stadig give udfordringer. I nogle set-up ønsker man som kommune at have fuld kontrol over borgerens opkaldsenhed og internetforbindelse. Den typiske løsning er at indkøbe tablets med sim-kort, men løsninger, som benytter sig af sim-kort vil være sårbare over for dårlig mobilbredbåndsdækning. Her vil løsningen i de fleste tilfælde være at sikre, at udstyret kobles op på borgerens egen wi-fi forbindelse.

**Anbefaling:**
Undersøg bredbånds- og mobildækningen i din kommune. Er der områder i kommunen, hvor mobilnetværket ikke fungerer optimalt, kan man benytte sig af en bredbåndsløsning i stedet.

Benyt fx www.tjekditnet.dk, hvor både status for bredbåndsdækningen og mobildækningen i hele landet vises.

## 2.2 Kryptering, firewalls og sikkerhed mm.

For at virtuelle opkald og skærmbesøg kan fungere, er der en række sikkerhedsmæssige foranstaltninger, som skal fungere. Krypterede forbindelser, firewalls, lukkede systemer etc., skal sikre, at det kun er den enkelte borger og kommunens medarbejder, som har adgang til samtalen.

**Anbefaling:**
Skab en god dialog mellem leverandør og IT-afdeling, så de tekniske og sikkerhedsmæssige udfordringer hurtigst muligt kan løses.

I april 2020 har Center for Cybersikkerhed i forbindelse med covid-19 situationen udgivet en kort vejledning i brug af kommunikations- og samarbejdsplatforme. Den kan læses her: https://feddis.dk/cfcs/publikationer/Vejledninger/Pages/kommunikations-og-samarbejdsplatforme.aspx

### 2.2.1 Kryptering

Krypteringen af samtalerne kan fungere på mange måder. Alt efter kommunens egen IT-opsætning, og hvilken leverandør kommunen vælger at benytte sig af, vil det kræve forskellige opsætninger og adgange, der skal konfigureres. Det er derfor vigtigt at skabe en god dialog mellem kommunens IT-afdeling og leverandøren.

### 2.2.2 Browser

En række løsninger giver mulighed for at foretage opkaldet gennem en browser. Da de forskellige løsninger er bygget på forskellige måder, fungerer nogle løsninger bedst i en bestemt browser. Forhør jer hos leverandøren, hvilken browser, der fungerer bedst med deres løsning, så der kan skabes de bedste betingelser for en god oplevelse hos borger og medarbejder.

### 2.2.3 Mobile Device Management-Løsning (MDM)

Hvis man vælger en løsningsmodel, hvor kommunen tager ansvaret for borgerens opkaldsenhed (modsat BYOD), anbefaler flere leverandører, at kommunen benytter sig af en MDM-løsning. MDM betyder ”Mobile Device Management”, hvilket er en software, der gør det muligt at kontrollere enheden – i dette tilfælde kommunens. En MDM-løsning kan bl.a. sørge for, at software altid er opdateret på borgerens enhed og sikre, at retningslinjer og politikker om følsomme data bliver overholdt. Undersøg i samarbejde med den kommunale IT-afdeling, om I skal benytte en MDM-løsning.

MDM-løsningen giver også mulighed for at låse den pågældende enhed, så den kun kan bruge et bestemt program. På den måde sikres det, at borgeren ikke kan benytte enheden til andre handlinger og ændre på software etc.

## 2.3 BYOD-paradigmet (Bring your own device)

Om der skal vælges en BYOD-løsning, altså en løsning hvor borgeren benytter sit eget device, afhænger i høj grad af målgruppen og formålet med skærmløsningen. Det er vigtigt at få afklaret om den valgte leverandørs produkt fungerer på forskellige devices, og hvem og hvordan support-modellen skal opsættes.

Ofte vælges BYOD på bl.a. SEL §85, hvor målgruppen typisk har egne devices og er vant til at bruge dem. Modsat vælges der ofte en løsning med udleveret hardware i hjemmeplejen og -sygeplejen. Ved BYOD findes der nogle overvejelser, man som kommune skal gøre sig. Som hovedregel vil borgeren selv kunne administrere eget device, men i tilfælde af tekniske udfordringer, kan den kommunale medarbejder have svært ved at yde support til et ukendt device. Kvaliteten af opkaldet vil kunne variere yderligere grundet forskellige devices og internetopkoblinger.

## 2.4 Logistik, service og support

Opsætning af logistik-, service- og supportaftaler er altafgørende og vil være forskellige alt afhængig af, hvilken leverandør og opsætning man vælger. Nedenfor er fremhævet to kommunale eksempler på, hvordan man arbejder med supportmodel, opsætning af systemer mm.

**Anbefaling:**
Undersøg forskellige modeller og afprøv dem i sammenhæng fra udlevering, opstart, service, support og hjemtagning.

**Kommunalt eksempel**
**Hjørring Kommune - Support:**
Der arbejdes i Hjørring Kommune udelukkende med BYOD, og der er derfor ikke nogen udfordringer med hverken logistik eller service. Der arbejdes primært med support, som er inddelt på tre niveauer.

1. Level et er medarbejderen hos borgeren (eller en kollega) og løser selv problemstillingerne (nogen steder er det hos en administrativ medarbejder, supporten kan hentes).
2. Level to er i forvaltningens tværgående team i Digitalisering og velfærdsteknologi. Her fås support via telefonen, mail eller fremmøde. Fremmøde kan være hos borger, medarbejders arbejdsplads eller hvor som helst, det kunne give mening for opgaveløsningen. De vurderer også, om der er brug for IT-afdelingen, og kan være behjælpelige med at beskrive udfordringerne sammen med medarbejderne.
3. Level tre foregår i IT-afdelingen. Det er dog sjældent, problemerne rammer dette niveau. IT-afdelingen er sparringspartnere for forvaltningen ved tværgående problemstillinger. Fx ved en opdatering hos Apple, der lagde Skype for Business ned på mobile enheder, som det skete for nogle år tilbage. De skal ligeledes give sparring på det juridiske og forsikringsmæssige.

**Kommunalt eksempel**
**Ikast-Brande Kommune - Opsætning:**
I Ikast-Brande Kommune er der valgt en videoløsning, som taler sammen med den eksisterende infrastruktur - Cisco Jabber/Teams. IT-afdelingen har lavet en lukket brugergruppe i systemet, så borgerne ikke kan ringe til andre medarbejdere end bostøtten. Endvidere har IT-afdeling lavet en MDM-løsning som lukker alle andre funktioner end videoløsningen ned på borgerens tablet. På den måde sikres det, at borgeren ikke installerer andre apps og ændrer i tablettens opsætning. I Ikast-Brandes indkøbsmodul er det muligt at bestille en "borger tablet". Det betyder, at medarbejderen ikke længere skal forbi IT og have den kodet. I praksis fungerer det ved, at IMEI-nummeret bliver registreret i IT ved køb, og så snart tabletten tændes og kobles på nettet henter den selv MDM-løsningen, og så er den klar til brug.

## 2.5 Fysiske rammer

Optimale fysiske rammer er en klar forudsætning for at skærmbesøg kan lykkes. Det er vigtigt, at det udstyr der benyttes til opkald, er af en ordentlig kvalitet, så billede og lyd ikke bliver en udfordring for samtalen.

Det skal være muligt at føre samtalen i fortrolighed. Derfor er det vigtigt at indrette et rum, hvor opkaldene kan foretages i fred og ro, hvor der er udstyr til rådighed heriblandt webcam, skærm, head-set med mikrofon. Af hensyn til borgeren kan det også være en ide at have et set-up, hvor der ikke er forstyrrelser i baggrunden. Det kan være forvirrende, hvis der går folk rundt, eller hvis andre folks stemmer kan høres. Benyt derfor headset med mikrofon for at give borgeren den bedste oplevelse.
Nogle borgere, bl.a. indenfor socialpsykiatrien, sætter også pris på, at medarbejderne drejer kameraet rundt i lokalet, så man kan se, at der ikke er andre end medarbejderen til stede.

**Anbefaling:**
- Gør lokaler egnede til video: Overvej belysning, gardiner til at skærme for sollys, udstyr af god kvalitet (mikrofon, headset, skærm, kamera mm.).
- Overvej om der skal indrettes særlige videorum, hvor man ikke forstyrres af forbipasserende.

Videoløsninger bidrager også til, at medarbejderne kan arbejde mere fleksibelt og ikke er afhængige af kontoret. Flere kommuner angiver, at medarbejdere benytter sig af videoopkald til borgerne fra mange andre steder end på kontoret. Eksempelvis hvis man kører mellem to besøg, og en borger pludselig har brug for at blive ringet op. Uanset om man er på farten eller på et kontor, skal samtalen stadig kunne føres i fortrolighed. Hvis der akut er brug for at foretage et kald fra en bil, må forbipasserende naturligvis ikke kunne se, hvem der tales med, ligesom de heller ikke må kunne høre, hvad der tales om. Også her skal det sikres, at der er tale om en sikker forbindelse. Det vil IT-afdelingen kunne hjælpe med at sikre.

## 2.6 Den tekniske tjekliste

Den nedenstående liste giver et overblik over de områder I, som kommune, skal overveje. Listen kan benyttes i samtale med leverandører og internt i kommunen.

**Tabel 1: Den tekniske tjekliste**

| Område | Beskrivelse | Hvad skal vi overveje? |
|---|---|---|
| **Devices**<br>*Der refereres her til de devices, som borger og medarbejder benytter til at udføre skærmbesøg* | | |
| **BYOD eller indkøbt device** | De to mest benyttede muligheder ift. borgerdevices er enten, at borgeren benytter sit eget (BYOD), eller at der indkøbes devices gennem kommunen. | ☐ Hvilke krav til devices har leverandøren?<br><br>☐ Skal vi benytte en BYOD-løsning? Er der retningslinjer i kommunen vedr. anvendelse af BYOD-løsninger? Og giver leverandøren mulighed for dette?<br><br>☐ Skal vi indkøbe devices til borgerne? Og evt. hvor mange?<br><br>☐ Fungerer leverandørens løsning på de eksisterende devices, som vores medarbejdere anvender? Eller skal der indkøbes devices til medarbejdere? Og evt. hvor mange?<br><br>☐ Skal der indkøbes anden hardware til opsætning af call-center? |
| **Tablet/PC/Begge** | Her refereres til de enheder, som medarbejderne skal benytte. Dette kan enten være indkøbte devices, stationære callrooms eller andre kombinationer. | |
| **Software og brugerflade**<br>*Den borgerrettede brugerflade og opkaldsmuligheder varierer fra udbyder til udbyder. Man skal derfor overveje hvilken løsning, der passer bedst til målgruppe og kommunalt set up.* | | |
| **Dedikeret app** | En app, der downloades på samme måde som andre apps til en hardware. Oftest findes de både til IOS og Android. | ☐ Er der retningslinjer i kommunen vedr. anvendelse af hhv. dedikeret app, browser eller låst tablet?<br><br>☐ Hvilken målgruppe af borgere skal anvende løsningen? Hvor IT-kyndige er de? (fx vil en låst tablet være mest optimal, når det drejer sig om borgere, der er mindst IT-kyndige)<br><br>☐ Hvilke muligheder tilbyder leverandøren?<br><br>☐ Hvis det giver mest mening at anvende en låst tablet, hvilken MDM-løsning kan så anvendes? Har kommunen i forvejen en MDM-løsning? Skal der indkøbes en MDM-løsning? Tilbyder leverandøren en MDM-løsning, som en service? |
| **Browser** | Opkaldene foregår gennem en browser. Valget af browser kan variere fra udbyder til udbyder. | |
| **Låst tablet** | Udbyderen har også mulighed for at installere softwaren på en tablet, så den kun kan bruges til skærmbesøg. Dette kræver et MDM-modul, så der er kontrol med, hvad der findes på den pågældende tablet. | |

| | | |
|---|---|---|
| **Sikkerhed, hosting, mm.**<br>*Der er en række punkter omkring teknik, hosting og sikkerhed, som skal overvejes i forbindelse med implementering af en skærmløsning.* | | |
| **Hosting muligheder** | Der findes flere forskellige muligheder for hosting. Det er vigtigt at afdække hvilke i samarbejde med IT-afdeling og leverandør. Klarlæg om leverandøren selv hoster, eller om leverandøren har en 3. parts hostingløsning. I alle tilfælde skal der benyttes en databehandleraftale. | □ Hvilke hostingmodel ønsker vi? Hoster leverandøren selv, eller benyttes der en tredjeparts hosting?<br>□ Hvilke garanterede oppetider har leverandøren. og passer de med vores behov? |
| **On-premise/egen lagring** | On-premise betyder, at al indsamlet data lagres på egne servere, som kommunen selv stiller til rådighed. | □ Foregår hosting i en cloud-løsning? Kan leverandøren garantere, at data kun vil være på en EU-baseret cloud? Hvis ja, kan leverandøren dokumentere dette? |
| **Kryptering af samtaler** | Den sikring, der skal foregå mellem de forskellige enheder | □ Har vi i kommunen en standard for, hvad en databehandler aftale med eksterne leverandører skal indeholde? Eller er det en forudsætning, at man anvender leverandørens standard databehandleraftale, som er ens for alle deres kunder?<br>□ Hvordan sikrer leverandøren kommunikationssikkerheden? |
| **Andet**<br>*Andre overvejelser ved implementering af skærmløsning.* | | |
| **Kan eksportere data til journalisering** | Som nævnt her i guiden er data utrolig vigtigt. Både i implementeringsregi, men også til overblik og udvikling når løsningen er gået i drift. | □ Hvilke muligheder for indsamling af data giver løsningen?<br>□ Kan løsningen integreres i journaliseringssystemet? |
| **Mulighed for at indkøbe/udvikle egen løsning** | Enkelte løsninger giver mulighed for at designe og udvikle eget kommunalt design og set up. | □ Er det muligt at indkøbe og udvikle løsningen? |

# 3 Markedsoverblik

Tabellen nedenfor er et overblik over kendte løsninger rettet mod sundheds-, ældre- og socialområdet. Listen er ikke udtømmende. Alle løsninger på listen lever ifølge leverandørerne op til de krævede sikkerhedsstandarder.

**Tabel 2: Overblik over tekniske løsninger**

| Navn | Beskrivelse | Leverandør |
|---|---|---|
| **Dedikerede løsninger udviklet til videokommunikation mellem borgere og kommunale medarbejdere** | | |
| **Appinux** | Appinux skærmbesøgsmodul er video med en meget enkel brugergrænseflade, hvor en tablet anvendes i kioskmode (kræver MDM-modul) eller installeres som en egen app/link på lige fod med andre apps/browsere på hardwaren. Der er mulighed for BYOD-løsning samt udleveret tablet. | Appinux |
| **HejDoktor** | HejDoktor tilbyder en dedikeret skærmløsning. Løsningen downloades som en app og kan derfor benyttes uafhængigt af hardware. Løsningen fungerer enten som BYOD-løsning eller på udleverede tablets. Der er desuden mulighed for integration til Cura. | HejDoktor |
| **KMD Nexus Video** | KMD Nexus Video er en videoløsning, som integrerer og understøtter videokonsultationer i fagsystemet Nexus. Videoapplikationen downloades som en applikation og kan derfor benyttes ved både BYOD-løsning, men også til udleverede tablets. | KMD |
| **Life-Manager** | Modulopbygget platform, som kan tilpasses kommunens eget udstyr. Bygger på videoløsning med fokus på hjemmeplejen, sygeplejen og specialiserede socialområde. Life-manager installeres som applikation/software og fungerer uafhængigt af hardware. Der er altså mulighed for BYOD-løsning samt udleveret tablet. | Life-Partners |
| **Tunstall Health** | Tunstall leverer en række forskellige virtuelle løsninger. Tunstall Health understøtter det, virksomheden kalder "omsorgskald", hvor borgeren får udleveret en tablet med indbygget software, så kommunen kan kontakte borgeren. Tunstall Health giver både mulighed for BYOD-løsning samt udlevering af tablet. | Tunstall A/S |
| **Viewcare** | Dedikeret løsning, som understøtter både medarbejdere og borger med end-to-end løsning. Fungerer ved download af applikation til de forskellige enheder. Fungerer både på borgeres eget device (BYOD), samt ved udlevering af tablet. | Viewcare A/S |
| **VitaComm** | VitaComm er en bred kommunikationsplatform, hvor videosamtaler bl.a. er en mulighed. Løsningen fungerer gennem en applikation, som downloades til det enkelte device. Fungerer både ved indkøbt hardware og på borgeres eget device. VitaComm samarbejder med SundhedsEkspressen om implementering af teknologien. | Applikator |

| | | |
|---|---|---|
| **Tværsektorielle møderum** | | |
| **VDX (Pexip)** | Fællesoffentlig og tværsektoriel videoinfrastruktur for stat, regioner og kommuner. Tilbyder dedikeret løsning for en-til-en eller flerpartsvideomøder.<br><br>VDX giver mulighed for samarbejde om en decentral videokonferenceserver. Man har som kommune mulighed for at designe egen kommunal løsning oven på VDX-infrastrukturen, som samtidig kan benyttes i den borgerettede kommunikation. VDX har udviklet en række API'er, som kan skabe integration med bl.a. de kommunale EOJ-systemer. Løsningen vil som udgangspunkt være finansieret på forhånd, da MedCom er drevet af fællesoffentlige midler. | MedCom |
| **Andre løsninger** | | |
| **Cisco webex teams og Jabber** | Generisk bred video- og hardwareinfrastruktur til video- og audiokonferencer, som inkluderer både den underliggende infrastruktur samt nødvendige softwareklienter til en bred vifte af enheder. Cisco har to løsninger, Jabber og Webex Teams, der giver mulighed for videokald. | Cisco |
| **IBG Video** | IBG Video er en del af IBG-platformen og fungerer som et modul, der kan tilføjes. Løsningen downloades gennem en applikation og fungerer herfra. | IBG |
| **Microsoft Teams** | Microsoft Teams er en samarbejdsplatform med en indbygget videosamtaleløsning. Løsningen er ikke målrettet ydelser på social og sundhedsområdet, men de tidligere sikkerhedsudfordringer, som har været ved brugen af Skype for Business er løst heri. Teams fungerer ved, at der via mail sendes et anonymt krypteret link til borgeren, som på denne måde kan tilgå det virtuelle møderum. Teams er en del af Microsoft 365 pakken.<br><br>**Skype for business**<br>Ifølge Microsoft udvikles der ikke mere på Skype for Business, og det vil over de næste år blive udfaset. Den præcise tidshorisont er endnu uvis. | Microsoft |
| **Shareplan** | Sensum Shareplan er en kommunikations-, struktur- og planlægningsplatform. Løsningen er målrettet bosteder og specialtilbud. Indeholder en videoløsning, som kan benyttes til samtale mellem borger og medarbejder. | E.G. |
| **TDC NetDesign** | NetDesign leverer kommunikationsløsninger samt underliggende infrastruktur og arkitektur for flere regioner og kommuner. NetDesign kan levere en dedikeret videoløsning samt den underliggende infrastruktur. | TDC NetDesign |
| **Zoom** | Zoom er en videokonferencetjeneste, der bruges til både møder, online undervisning og meget andet. Zoom er kendt for at have svag kryptering, og efter sigende findes der mange kompromitterede konti til salg, så det kan ikke anbefales at bruge tjenesten til behandling af personfølsomme informationer. | Zoom Video Communications |

**Fordele og ulemper ved de forskellige løsninger**
Som markedsoverblikket antyder er der store forskelle mellem de forskellige løsninger. Disse må derfor overvejes i den kommunale organisation, inden man påbegynder indkøb og implementering af skærmbesøg. Vælger man en af de dedikerede løsninger, vil man som kommune ofte

kunne drage fordel af et større samarbejde med leverandøren. Her bl.a. i form af sparring, rådgivning og projekt-/procesledelse ved implementering samt mulighed for flere og tilgængelige data.

Ved de kommercielle løsninger er det lige omvendt. Her vil sparringen med leverandøren være mindre og kan derfor kræve en større implementeringsindsats fra kommunen selv. Derfor vil prisen også ofte være lavere.

#### 3.1.1 Disse løsninger er ikke sikre

Der findes en række løsninger, som kan være lette at tilgå, da borgerne ofte har disse løsninger på deres enheder i forvejen. Det drejer sig bl.a. om sociale platforme som, i den version de eksisterer i dag, ikke lever op til sikkerhedskravene og derfor er ulovlige at bruge til formålet.

**Benyt ikke sociale platforme som fx:**
- Facebook Messenger
- FaceTime
- Almindelig Skype
- WhatsApp

## 4 Juridiske forhold

### 4.1 Databehandleraftaler

Hos de fleste leverandører vil det være en forudsætning at udarbejde en databehandleraftale, før løsningen tages i brug. Både kommuner og leverandører er efterhånden vant til det, men hvis der er brug for inspiration, kan man med fordel læse mere hos Datatilsynet: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2018/feb/ny-skabelon-skal-hjaelpe-virksomheder-og-myndigheder-med-at-blive-klar-til-databeskyttelsesforordningen/.

I praksis vil det ofte være en leverandør/databehandler, som udformer databehandleraftalen, og i mange tilfælde ønsker leverandørerne at anvende deres egen skabelon. Det er dog stadig den dataansvarlige, som har ansvaret for, at lovkravene i aftalen er opfyldt.

### 4.2 BYOD-sikkerhed

Som tidligere beskrevet er der flere forskellige forhold, der spiller ind, hvis man vælger at bruge borgers eget device til at kommunikere via skærm. GDPR-forordningen medfører bl.a., at de dataansvarlige skal kontrollere databehandlernes måde at håndtere data på. Det betyder, at det skal sikres, at data ikke krydser en server uden for EU. Det kan være svært at tage stilling til som fagpersonale, om en forbindelse er sikker nok, og det er ikke hensigtsmæssigt, at der skal foretages et risikobaseret skøn i hver enkel situation, så det er bedst at have på plads på forhånd. Særligt hvis der en dag er brug for at have kontakt ud af kommunen fx til andre myndigheder.

Hvis borgers udstyr bryder sammen, som følge af de apps/kommunikationsløsninger kommunen har installeret, vil der være tale om en potentiel erstatningssag. Hvis borgers udstyr bryder sammen af anden årsag, fx fordi det er gammelt eller får en vandskade, vil det være borgers eget ansvar, og ikke kommunens at skaffe nyt udstyr. I mellemtiden må besøget leveres på anden vis, eksempelvis som fysisk besøg. Der er til gengæld intet til hinder for at have en politik om, at man hjælper med reparationer i tilfælde, hvor det er særligt vigtigt at kunne levere et besøg via en skærm.

### 4.3 Standard ISAE 3402

ISAE 3402 er en international standard, som anvendes til revision og erklæringsopgaver med høj grad af sikkerhed om kontroller hos serviceleverandører, herunder it-serviceleverandører. Det er ikke alle leverandører, der er certificerede, men standarden er en garant for, at leverandøren som service provider overholder standarden for sikkerhed, drift og arbejdsgange. Desuden er erklæringen en sikkerhed for, at leverandørens tjenester håndterer alt data korrekt.

Læs evt. mere her:
https://www.stil.dk/administration-og-infrastruktur/systemrevision-af-studieadministrative-systemer/isae-3402-standarden

## 4.4 Standard ISO 27001

En række leverandører er ISO 27001 certificerede. Formålet med leverandørens efterlevelse af ISO 27001-bestemmelsen er at sikre, at leverandøren kan dokumentere opfyldelsen af kontrakters krav til leverandørens ledelsessystem for informationssikkerhedsstyring. Dette vil blandt andet indebære, at leverandøren har truffet de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre myndighedens data og information mod tab af fortrolighed, tilgængelighed og integritet.

Med andre ord vil en ISO 27001 certificeret leverandør bl.a. skulle leve op til:

- At data og information kun kan tilgås af det personel, som har et arbejdsrelateret behov for dette.
- At relevant data og information kan genfindes efter behov, eksempelvis i sammenhæng med revision eller anmodning om aktindsigt.
- At data og information er pålideligt, så det kan danne basis for beslutningsgrundlag.

Myndigheden skal dog være opmærksom på, at certificeringen vil være udtryk for, om leverandørens egen sikkerhed stemmer overens med leverandørens interne forhold. Bestemmelsen er således ingen garanti for total sikkerhed, da der kan være uoverensstemmelser mellem leverandørens sikkerhedsbehov og kundens.

## 4.5 Rådgivning hos Datatilsynet

Siden maj 2018 har datatilsynet vejledt og rådgivet om spørgsmål vedrørende databeskyttelse. Det betyder, at man kan henvende sig til dem med spørgsmål vedrørende databeskyttelse og igangværende sager. De har desuden en række generelle vejledninger liggende, hvor man kan finde svar på en række spørgsmål. Læs mere her: https://www.datatilsynet.dk/kontakt/.

# 5 Journalisering

Der findes i øjeblikket ikke en fælleskommunal standard for, hvordan kommunerne skal dokumentere, at en indsats leveres helt eller delvist via en skærm. Dette medfører en stor forskellighed i dokumentationspraksis på tværs af kommunerne.

**Anbefaling:**
Sørg for at stille krav om, at data på de foretagne opkald er en del af produktet. På den måde kan I følge med i udviklingen og optimere arbejdsgangene omkring skærmbesøg.

Flere leverandører af skærmløsninger har rapporter med data-træk fra deres log-systemer om opkaldstidspunkter og opkaldslængde som en fast del af produktet. Det giver jer mulighed for at følge udviklingen og tilpasse arbejdstilrettelæggelsen. Hvis ikke leverandøren tilbyder disse rapporter, anbefales det, at I efterspørger det allerede ved indkøb af løsningen.

**Kommunale eksempler**

**Viborg Kommune – Journalisering:**
I Viborg Kommune registreres skærmbesøg på sundhedslovsindsatserne i EOJ-systemet KMD Nexus som en selvstændig indsats. Dette betyder, at der kan trækkes statistik på disse.
I forhold til servicelovens indsatser er der ikke selvstændige indsatser, hvilket betyder, at der ikke kan trækkes statistik på disse. Årsagen til dette er, at kommunen på et tidspunkt var begrænset af de tekniske muligheder vedrørende pakkemodellen. Der arbejdes i øjeblikket med en alternativ løsning, hvor driften noterer skærmbesøg i kommentarfeltet på køreruten.

**Holbæk Kommune – Journalisering:**
Holbæk Kommune benytter sig ligeledes af KMD Nexus og har struktureret måden, hvorpå skærmbesøgene registreres. I omsorgsnotat registreres det, hvis en borger er egnet til video, og om borgeren er blevet tildelt et device. Her skrives også borgers brugernavn og password.
Herefter planlægges besøget som normalt i kørelisten, men skærmbesøget kategoriseres ”planlagt skærmbesøg” frem for standarden ”planlagt besøg”. Dette giver en anden farvekode i kalender. Der skrives ”skærmbesøg” i kommentarfelt på kørelisten, for medarbejdere, der kun ser kørelisten. Ved at skærmbesøget har en anden kategori, kan der trækkes data på, hvor mange skærmbesøg de leverer i omsorgssystemet.