Direktoratet for e-helse

Teknisk anbefaling velferdsteknologi

ANBEFALINGER KNYTTET TIL TEKNISK KRAV FOR TRYGGHETSSKAPENDE TEKNOLOGI

IS-2534

Forord

Stortinget etablerte gjennom RNB 2013 (Prop.149 [2012-2013]) «Nasjonalt program for utvikling og implementering av velferdsteknologi 2014-2020». Sentralt i oppdraget står etablering av en arkitektur og infrastruktur på det velferdsteknologiske området.

I rapporten «Arkitektur for Velferdsteknologi – anbefalinger for utprøving og faser for realisering (IS-2402)» foreslo Helsedirektoratet en arkitektur til utprøving og hvordan denne arkitekturen kan realiseres i faser.

Erfaringer viser at kommunale anskaffelser av trygghetsskapende teknologier i dag baseres på til dels differensierende tekniske spesifikasjoner. En status i markedet viser også at de fleste kommunene i Norge representerer hver for seg små markeder (94 % av norske kommuner har i dag færre enn 500 trygghetsalarmer). Mange små anskaffelser med noe ulike spesifikasjoner gir ikke et godt grunnlag for et bærekraftig leverandørmarked. Ulike spesifikasjoner gir heller ikke grunnlag for likeverdige tjenester til tjenestemottakere.

Formålet med denne rapporten er å utdype anbefalingene i IS-2402 og gi kommuner, leverandører og andre som skal implementere trygghetsskapende teknologi i tjenestene et felles grunnlag for å anskaffe og utvikle løsninger innenfor rammen av den anbefalte arkitekturen. Innholdet erstatter tekniske anbefalinger gitt i IS-2225 «Helsedirektoratets anbefalinger på det velferdsteknologiske området», utgitt 10/2014.

Arbeidet er basert på en erfaringsinnsamling blant et utvalg av kommuner og leverandører som sitter med erfaring i forbindelse med nylig gjennomførte anskaffelsesprosesser.

Standardiseringsarbeidet innenfor velferdsteknologi er ikke ferdig, og gjeldende anbefalinger dekker ikke alle teknologiområder. Velferdsteknologiprogrammet vil derfor måtte forvalte og videreutvikle anbefalingene basert på kommuners og leverandørers løpende erfaringer på området.

Rapporten omtaler ikke håndtering av personvern og informasjonssikkerhet særskilt for trygghetsskapende teknologier, men henviser til **«**Norm for informasjonssikkerhet i helse- og omsorgstjenesten» med tilhørende «Veileder i personvern og informasjonssikkerhet ved bruk av velferdsteknologi»

Oslo, oktober 2016

Direktoratet for e-helse

Innhold

1 Innledning

Dette dokumentet er tatt frem for de som skal anskaffe og de som skal levere trygghetsskapende teknologi i det norske markedet. Dokumentet gir anbefalinger på sentrale krav med fokus på å sikre pålitelig, sikker og effektiv drift av slike løsninger. Krav til pålitelighet og sikkerhet i slike løsninger bør være like over hele landet for å sikre mest mulig lik kvalitet på tjenestene og et mer uniformt marked for leverandører.

Det arbeides nå mot en mer helhetlig ehelse-arkitektur i Norge som skal sikre nødvendig informasjonsflyt mellom systemene for å oppnå en mer effektiv helsetjeneste. Løsninger for trygghetsskapende teknologi må også tilpasse seg denne arkitekturen etter hvert. Dette dokumentet gir anbefalinger knyttet til nødvendig informasjonsflyt mellom den velferdsteknologiske løsningen og kommunens fagsystem/EPJ. Det gis også anbefalinger om kommunikasjonsgrensesnitt.

Denne versjonen av anbefalingene dekker de mest vanlige trygghetsskapende teknologier som trygghetsalarm, fallsensor og lokasjonsteknologi. Anbefalingen vil bli oppdatert etter hvert som erfaringer foreligger fra bruk av andre trygghetsskapende teknologier (f.eks. natt-tilsyn m.m.) og fra medisinsk avstandsoppfølging.

Mange anskaffelsesprosesser er i gang, eller under planlegging, i norske kommuner knyttet til trygghetsskapende teknologier. Det er tidligere anbefalt (IS-2402) at kommuner bør søke samarbeid i disse anskaffelsene. Kompleksitet og utviklingsbehov fremover tilsier at det er behov for et nært samarbeid mellom kommuner og leverandører. Dette oppnås som regel best ved at kontrakten representerer et visst forretningsvolum for leverandøren.

Helsedirektoratet anbefaler at begrepet velferdsteknologi inndeles i følgende teknologiområder (jf. IS-2416):

Trygghetsskapende teknologier *som skal muliggjøre at mennesker kan føle trygghet og gis mulighet til å bo lengre hjemme. I dette inngår løsninger som gir mulighet for sosial deltakelse og motvirke ensomhet.*

Mestringsteknologier *som skal muliggjøre at mennesker bedre kan mestre egen helse og sykdom. I dette inngår teknologiske løsninger til personer med kronisk sykdom/lidelser, personer med psykiske helseutfordringer, personer med behov for rehabilitering og vedlikehold av mobilitet mv. Medisinsk avstandsoppfølging kommer inn under dette teknologiområdet.*

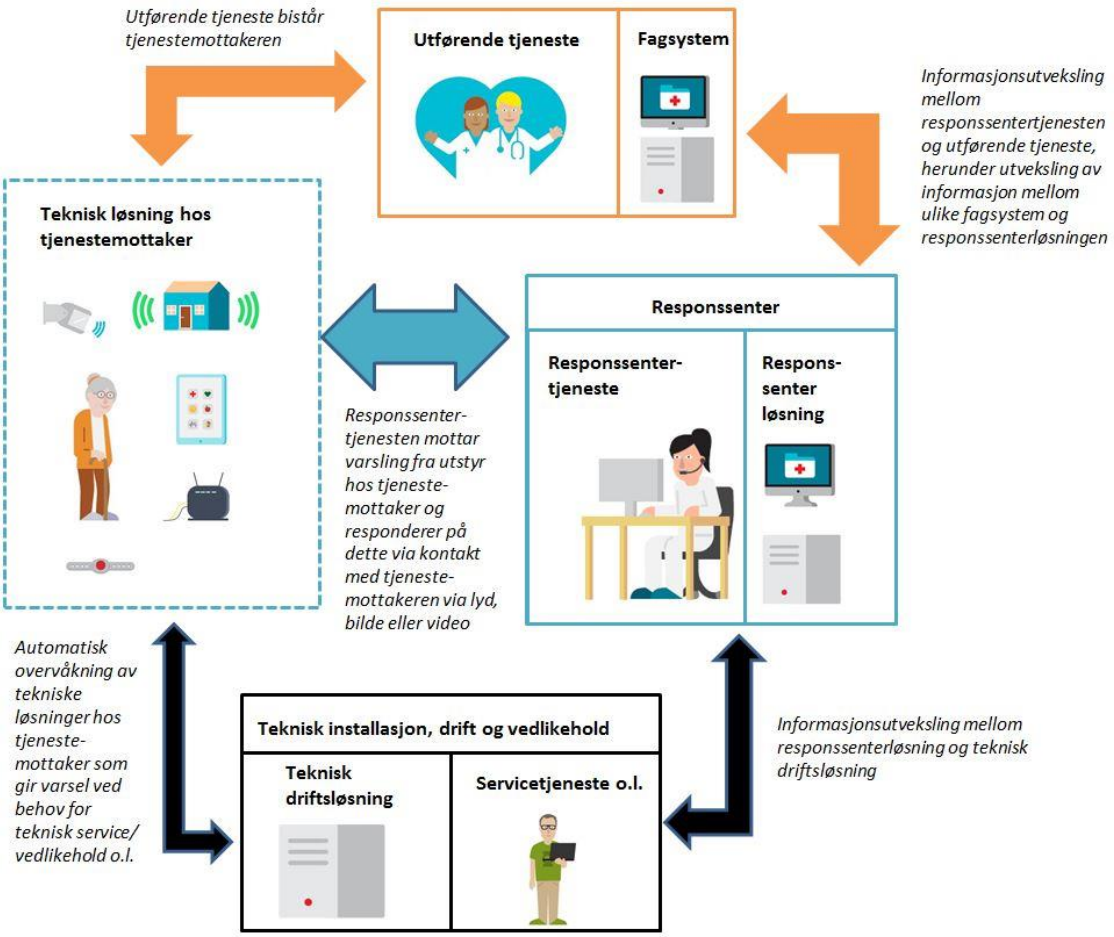
Utrednings- og behandlingsteknologier *som muliggjør avansert medisinsk utredning og behandling i hjemmet – Hospital@home-løsninger. Dette teknologiområdet ble i Helsedirektoratets anbefalinger fra 2014 omtalt som helseteknologier.*

Velværeteknologier *som bidrar til at mennesker blir mer bevisst på egen helse og avhjelper hverdagslige gjøremål uten at nedsatt helsetilstand er årsaken til bruken av teknologi.*

2 Anbefalinger

Figuren nedenfor gir en overordnet oversikt over roller, komponenter og informasjonsflyt i et tjenesteoppsett som benytter trygghetsskapende teknologi. Det er i dette kapittelet gitt anbefalinger på krav til:

- Teknisk løsning hos tjenestemottaker
- Pålitelig kommunikasjonsløsning mellom tjenestemottaker og responssenter
- Responssenterløsning og teknisk driftsløsning
- Informasjonsutveksling mellom responssenter og fagsystem/EPJ



Følgende definisjoner ligger til grunn:

Responssenterløsningen *er en teknisk løsning som skal gi støtte for responssentertjenestens behov for å motta, vurdere, dokumentere og respondere på varslinger fra velferdsteknologiske løsninger. I dette inngår utveksling av informasjon med fagsystemer i helse- og omsorgssektoren.*

Fagsystem *er et elektronisk informasjons-, dokumentasjons- og beslutningsstøttesystem for helse- og omsorgstjenestene som støtter sentrale arbeidsprosesser, som f.eks. saksbehandling, faglig dokumentasjon (journalsystem), arbeidsplanlegging, rapportering mv.*

Teknisk driftsløsning *skal gi støtte for teknisk installasjon, driftsovervåking, teknisk fjernbetjening og teknisk vedlikehold av velferdsteknologiske løsninger som inngår i responssentertjenestens ansvarsområde.*

2.1 Tekniske løsning hos tjenestemottaker

Den tekniske løsningen som tjenestemottaker enten bærer på seg eller som er installert i boligen, er den delen av løsningen som tjenestemottaker forholder seg til daglig. Komplisert betjening og dårlig kvalitet vil medvirke til at tjenestemottaker ikke føler den tryggheten som intensjonen tilsier. Brukervennlighet, målenøyaktighet og robusthet er viktige parametere i denne sammenheng.

2.1.1 Brukervennlighet

Direktoratet for e-helse anbefaler:

- **Teknisk utstyr som krever oppmerksomhet eller handling fra tjenestemottaker skal tilpasses tjenestemottakers behov**

Hver tjenestemottaker har ulike individuelle forutsetninger for å kunne forstå og bruke teknisk utstyr. Hvis tjenestemottaker bruker utstyret feil eller overser viktige signaler, så går dette utover kvaliteten på tjenesten. Utstyret må derfor være utformet slik at denne risikoen er minimal. Utstyr må være utformet på en slik måte at alle personer som blir tilbudt tjenesten kan forstå og benytte det. Grad av krav til universell utforming på utstyret vil være knyttet til hvem kommunen beslutter å tilby tjenestene til. Utstyret må tilpasses personer med ulik grad av funksjonsnedsettelse, herunder demenssykdom, nedsatt syn, hørsel, håndgrep, balanse. I tillegg må det utarbeides gode rutiner for opplæring av tjenestemottakere og tjenesteytere som skal håndtere utstyret. Dette kan gjerne gjøres i samarbeid med leverandørene. Regjeringen har i sin «Handlingsplan for universell utforming[1], identifisert fire tiltak knyttet til velferdsteknologi og hverdagsteknologi (TEK1-4).

Det anbefales at det stilles følgende minimumskrav til universell utforming på utstyr hos tjenestemottaker:

- **Få og store knapper**
- **Intuitive fargevalg med god kontrast på knapper og lysvarsel**
- **Store og intuitive symboler med god kontrast**
- **Store og enkle tekster/ledetekster med god kontrast**
- **Tydelig kvitteringsvarsel som viser at varsel har nådd frem til responssenterløsningen**
- **Bruk av både lys og lyd ved kvittering og andre varsler som kan justeres i styrke etter individuelle behov og ønsker, for eksempel vibrasjon**
- **Høyttalervolum og mikrofonfølsomhet som kan justeres fra responssenter**
- **Alternativ trykkmotstand og knappestørrelse på trygghetsalarmer**
- **Batteridrevet utstyr bør angi behov for ladning eller batteribytte**

[1] Regjeringens handlingsplan for universell utforming 2015-2019, Q-1233 B, Barne-, likestillings- og inkluderingsdepartementet

- **Enkelt og intuitivt ladeutstyr for utstyr som trenger ladning**
- **Enkelt å koble til ladere eller annet tilleggsutstyr, eller bytte batterier**
- **Bruk av standardbatterier (som er enkle å få tak i)**
- **Enkle brukerveiledninger med gode illustrasjoner og lite tekst**
- **Utstyr som bæres rundt halsen må ha bruddsikring for å unngå struping**

2.1.2 Målekvalitet

Direktoratet for e-helse anbefaler:

- **Målenøyaktigheten på sensorer må oppgis fra leverandør, enten i utstyrsspesifikasjonen eller sammen med måleresultatet som oversendes til responssenterløsningen (f.eks. posisjonsmåling)**
- **Målefølsomheten må kunne justeres for personlig tilpasning på sensorer som kan virke forskjellig fra person til person (f.eks. fallsensorer).**

Nødvendig målenøyaktighet til utstyret hos tjenestemottaker må vurderes ut fra behov. Det er derimot viktig at nøyaktigheten er kjent for tjenestepersonellet slik at situasjonen kan vurderes ut fra dette. Om en posisjonsmåling utendørs har en nøyaktighet på 10 meter eller 1 km kan ha stor betydning for eventuelle videre aksjoner. Tjenesteyter må vurdere risikoen med for eksempel å sette opp et virtuelt gjerde (geofence) i nærheten av trafikkert vei opp mot den nøyaktigheten på posisjonsmålingen som vanligvis oppnås i dette området. Målenøyaktigheten til et GPS basert utstyr vil være avhengig av mottaksforholdene for satellittsignalene der målingene blir tatt.

Det anbefales at målenøyaktigheten på sensorer oppgis fra leverandør, enten i utstyrsspesifikasjonen eller sammen med måleresultatet som oversendes til responssenterløsningen (f.eks. posisjonsmåling).

Erfaringer så langt har avdekket utfordringer med kvaliteten til fallsensorer. Personer faller på forskjellige måter slik at det er vanskelig å fastsette et absolutt nøyaktighetskrav til en fallsensor. Det er heller ikke identifisert noen internasjonale standarder som definerer hvordan dette kan måles.

Det anbefales at fallsensorer må kunne justeres av tjenesteyter tilpasset tjenestemottaker for å oppnå størst mulig nøyaktighet for akkurat denne personen.

2.1.3 Robusthet

Direktoratet for e-helse anbefaler:

- **Utstyret må tåle de mekaniske belastningene det må forventes å bli utsatt for i de tjenestene de skal benyttes.**
- **Utstyret må følge Norske og Europeiske standarer satt for slikt utstyr (CE merking).**
- **Utstyr som krever tilkobling til strømnettet må fungere minimum 24 timer ved strømbrudd.**

Utstyr som tjenestemottaker kontinuerlig skal bære med seg innendørs, som for eksempel alarmutløser for trygghetsalarm, må tåle fall på gulvet og i vann (vasken/do og dusj). Utstyr som skal bæres med utendørs må i tillegg tåle store temperatursvingninger, regn og støv/jord/sand.

Det anbefales at utstyr som skal bæres innendørs oppfyller følgende minimumskrav:

- **IP 67 i henhold til IEC 60529 (EN NEK 60529), komplett beskyttelse mot støvgjennomtrengning og ingen skadelig virkning ved kortvarig neddykking i vann (15 til 100 cm i inntil 30 minutter).**
- **Tåle fritt fall fra 1.5 meter og ned i stein/betonggulv.**

Det anbefales at utstyr som skal bæres utendørs oppfyller følgende minimumskrav:

- **Bør helst oppfylle IP 67 i henhold til IEC 60529 (EN NEK 60529), som for utstyr som skal bæres innendørs. Som et minimum bør det oppfylle IP 64 (komplett beskyttelse mot støvgjennomtrengning og at vannsprut fra alle kanter ikke skal ha skadelig virkning).**
- **Fungere i temperaturområdet – 20 til + 40 grader Celsius**
- **Tåle fritt fall fra 1.5 meter ned på stein/betonggulv i – 20 grader Celsius**

2.1.4 Kommunikasjonsgrensesnitt

Direktoratet for e-helse anbefaler:

- **All datakommunikasjon baseres på IP og talekommunikasjon baseres på IP eller mobil**
- **Nytt utstyr bør støtte IPv6**
- **Kommunikasjonsgrensesnittet mellom teknisk løsning hos tjenestemottaker og responssenterløsning må følge de nasjonale anbefalingene gitt i IS-2402, «Arkitektur for velferdsteknologi – anbefaling for utprøving og faser for realisering»), eller senere utgaver.**

Forslag til europeisk spesifikasjon, og etterhvert standard, for IP protokoll knyttet til trygghetsskapende teknologier er under utarbeidelse i CENELEC TC79. Inntil denne er på plass så anbefales det å benytte den svenske standarden SIS/STD-101762, «Digital social alarm - Social Care Alarm Internet Protocoll (SCAIP)». Det er viktig å være klar over at denne standarden ikke krever kryptering av informasjonen som overføres og må derfor ikke benyttes ved overføring av sensitive opplysninger. SCAIP-standarden har mangler som spesielt gjør seg gjeldende for mobile trygghetsalarmer. Eksempler på slike mangler er overføring av lokasjonsinformasjon fra mobilnettverket, kryptering, tjenesteoppsett av tids- og områdestyrte lokasjonsalarmer. I tillegg er det komplisert å implementere kostnadseffektivt og med lavt batteriforbruk på små enheter ved bruk av SCAIP.

Det anbefales at kommunikasjonsgrensesnittene mellom teknisk løsning hos tjenestemottaker og responssenterløsning oppfyller følgende minimumskrav:

- **SCAIP (SIS/STD-101762) standarden skal følges på stasjonære trygghetsalarmer.**
- **Leverandørspesifikke protokoller kan benyttes i tillegg til SCAIP der det er hensiktsmessig.**
  Nødvendige tilpasninger kan være leverandørspesifikk transport av SCAIP-alarmer over HTTPS (TLS 1.2) med en egnet autentiseringsmekanisme, samt tilpassede meldinger for manglende funksjonalitet. **OBS!** Leverandørspesifikke grensesnitt vil ikke nødvendigvis uten videre kunne videreføres dersom responssenterløsningen byttes ut.
- **Leverandører som leverer tilpassede grensesnitt må åpne sine spesifikasjoner slik at andre leverandører kan benytte samme grensesnitt uten begrensninger.**

2.1.5 Installasjon

Direktoratet for e-helse anbefaler:

- **Teknisk løsning hos tjenestemottaker må kunne tilpasses hver enkelt person og omgivelsene den skal fungere under.**
- **Kartlegging av personlige og lokale forhold, og sammensetting og test av løsning, må gjøres før installasjon hos tjenestemottaker.**

Sammensetning og konfigurasjon av teknisk løsning hos tjenestemottaker er knyttet til det tjenestevedtaket som kommunen har gjort for hver enkelt tjenestemottaker. Løsningsoppsettet kan derfor variere fra gang til gang. Tjenestemottakerne må føle seg trygge på at de tekniske løsningene de skal forholde seg til fungerer som de skal. En viktig faktor for å oppnå dette er at installasjonen og idriftsettelsen gjennomføres uten problemer, og at det blir gitt god opplæring.

Det anbefales at installasjon av teknisk løsning hos tjenestemottaker følger følgende minimumskrav:

- **Utstyr må i størst mulig grad være konfigurert før installasjon ute hos tjenestemottaker.**
- **Ved bruk av trådløse forbindelser mellom utstyr som inngår i løsningen hos tjenestemottaker må kvaliteten på slike forbindelser kunne måles og eventuelt forbedres med bruk av lokale signalforsterkere.**
- **Det bør foreligge standard testprosedyrer som verifiserer at utstyret er konfigurert riktig og at forbindelsen til responssenterløsningen fungerer.**

2.1.6 Drift

Direktoratet for e-helse anbefaler:

- **For å være sikker på at utstyret virker, og for å skape trygghet hos tjenestemottaker, bør hjemmetjenesten og tjenestemottaker regelmessig sammen verifisere at utstyret virker.**
- **Øvrig teknisk overvåkning, feilretting, vedlikehold, programvare-oppdateringer og konfigurasjonsendringer bør i hovedsak kunne gjennomføres sentralisert og i minst mulig grad kreve innsats fra tjenestemottaker.**

En forutsetning for å kunne ta ut gevinstene med bruk av velferdsteknologi er at alle kan stole på at de tekniske løsningene fungerer og at det blir gitt rask beskjed hvis de ikke fungerer. Det er nødvendig at tjenestemottaker prøver teknologien sammen med hjemmetjenesten med jevne mellomrom for å skape trygghet. Teknisk fjernovervåkning av løsningen er nødvendig for å kunne oppdage eventuelle tekniske uregelmessigheter tidlig. Løsningen vil etter hvert, som andre digitale løsninger, kreve programvareoppdateringer. Et lengre tjenesteforløp vil sannsynligvis også kreve endringer av løsningskonfigurasjonen. Slike oppdateringer og endringer må kunne gjennomføres fra sentrale løsninger (teknisk driftsløsning og responssenterløsning) uten tjenestemottakers medvirkning. Det vil etter hvert bli installert avanserte løsninger ute hos mange tjenestemottakere med forskjellige konfigurasjoner og forskjellige programvareversjoner. Det er nødvendig at alle løsningene registreres i et felles utstyrsadministrasjonssystem for å holde oversikten.

Det anbefales at det settes følgende minimumskrav til drift av teknisk løsning hos tjenestemottaker:

- **Konfigurasjonsendringer, enkel feildiagnose/retting, programvareoppdateringen og omstart må kunne utføres fra sentral driftsløsning uten behov for lokal medvirkning**
- **Det skal ikke være mulig for tjenestemottaker å endre konfigurasjonsoppsettet på utstyret**
- **Løsningen må kunne gi informasjon om at den fungerer til teknisk driftsløsning med gitt tidsintervall (keep alive/heart beat). Det bør være mulig å justere dette tidsintervallet for å kunne optimalisere batterilevetid og kommunikasjonsmengde i forhold til kritikalitet.**

- **Løsningen må automatisk kunne varsle sentral løsning ved tekniske tilstander som kan påvirke løsningens pålitelighet (som f.eks. dårlig dekning, spenningsbortfall, lavt batterinivå, ved ladefeil, kritiske funksjonelle feil).**
- **Løsningen må starte automatisk etter avbrudd uten behov for lokal assistanse.**
- **Løsningskomponentene bør kunne registreres i et felles utstyrsadministrasjonssystem hvor hvert utstyrselement har en unik ID og hvor bl.a. informasjon om utstyrstype, plassering, programvareversjon, konfigurasjon, kommunikasjonsleverandør, forventet gjenstående batterilevetid og feilmeldinger blir holdt oppdatert.**

2.2 Pålitelig kommunikasjon

Direktoratet for e-helse anbefaler:

- **Mobilkommunikasjon brukes som primærkanal for kommunikasjon mellom teknisk løsning hos tjenestemottaker og responssenterløsning.**
- **Fast bredbånd brukes som en redundant kommunikasjonskanal der dette er mulig.**
- **Fast bredbånd kan brukes som primærkanal hvis tjenesteyter eier, eller har kontroll over, abonnementet.**
- **Planlegg for skifte fra 2G til 4G/LTE mobilkommunikasjon.**

Kommunikasjonen mellom teknisk løsning hos tjenestemottaker og responssenterløsning er en kritisk komponent. Fungerer ikke denne så vil ikke varsler fra tjenestemottaker nå frem til responssentertjenesten og den tekniske fjernovervåkningen av teknisk løsning hos tjenestemottaker vil opphøre.

Denne kommunikasjonen kan løses på to måter:

- Mobilt bredbånd
- Fast bredbånd hvis løsningen er fast installert i en bolig

Mobilt bredbånd gir kommunikasjon der hvor utstyret er, også utendørs, og kommunikasjonen kan enkelt leveres med løsningen slik at ansvaret for løsning inkludert kommunikasjon er samlet. Kommunikasjonsabonnementet håndterer da kun kommunikasjonsbehovet til den spesifikke løsningen. Løsninger som kun benytter mobilt bredbånd er avhengig av at det er dekning på stedene løsningen benyttes.

Fast bredbånd gir kommunikasjon kun til fast bolig og leveres stort sett som et privat abonnement. Dette betyr at kommunikasjonsabonnementet gjerne også benyttes til andre formål (Internett, TV, smarthusløsninger etc.). Dette betyr at endringer kan skje som vil påvirke kvaliteten på kommunikasjonen uten at tjenesteyter har kontroll over dette.

Mobilnettene i Norge er i stadig utvikling og dekningen og kvaliteten blir bedre og bedre. Telenor hevder at målt på landsbasis vil en bruker oppleve at mobilnettet har en oppetid på ~ 99,9% og ~99,5% suksess-rate for å sette opp en samtale. Selv om ytelsene i både 2G- og

3G-nettet er svært gode, yter 4G-nettet bedre. Mobiloperatørene investerer betydelig beløp årlig i utbygging av 4G-nett. Nye frekvenskonsesjoner blir brukt til 4G. Eksempler på dette er nye frekvensblokker i 800 MHz båndet som gir langt bedre flatedekning og dekning innendørs. Det forventes at 4G-dekningen vil passere 2G-dekningen i 2018. 4G gir også langt bedre båndbredde enn 2G noe som er nødvendig ved bruk av for eksempel video. Telenor hevder at de vil opprettholde 2G-dekningen på dagens nivå til 2025. 3G-nettet vil sannsynligvis bli avviklet før det. I 4G-nettet er både tale og data basert på IP. I kombinasjon med svært høy kapasitet gir dette en vesentlig bedre trafikkavvikling og kapasitetsutnytting sammenlignet med de andre teknologiene. Som en ekstra sikring av fremkommelighet for tale så blir 4G tale prioritert om det skulle bli kapasitetsutfordringer.

Det er nødvendig at velferdsteknologiske løsninger utvikler seg mot å benytte 4G/LTE som kommunikasjonsteknologi. I dag er det en utfordring at 4G-modulene som kan benyttes i ulike velferdsteknologiske løsninger er relativt kostbare, krever mye strøm og er store. Med nye standarder innenfor LTE-teknologi (f.eks. LTE Cat-1 og Cat-M) og etterhvert Narrow Band IOT, så vil kostandene for disse modulene reduseres dramatisk, samt at også batterilevetid forlenges (med levetid i størrelsesorden 1-10 år) og ikke minst vil modul-størrelsen reduseres. Vi vil sannsynligvis se de første løsningene med denne teknologien på markedet medio 2017. Denne teknologien vil legge til rette for en migrasjon fra gammel 2G teknologi til ny 4G teknologi. Det anbefales at det hoppes over LTE Cat-0 og at det fokuseres direkte på LTE Cat-M1 i utstyret da operatørene høyst sannsynlig vil droppe implementering av LTE Cat-0

Det faktum at det er variabel dekning i Norge og at det kan forekomme feil i mobilnettene medførte at vi tidligere[2] har anbefalt å benytte abonnement som kan veksle mellom alle tilgjengelige mobilnett i Norge (nasjonal roaming) der det er nødvendig. Telenor har kommentert dette:

(Sitat Telenor): Det er ingen planer om nasjonal roaming i Norge. Det er forbundet med svært store investeringer og det er ikke sikkert det vil kunne fungere i en oppstått situasjon. Ved feil hos Telenor kan det være komponenter i Telenors nett som feiler som bidrar til at det ikke er mulig å overføre trafikk. Det har også med kapasitet hos mottakende operatør, det er ikke sikkert at mottaker er i stand til å ta imot hele eller deler av trafikken. Roaming innebærer å være gjest. Tanken er at det skal gi økt sikkerhet og økt oppetid ved å ha to operatører å velge mellom. Telenor og Telia deler ofte infrastruktur og kun radiodelen utgjør forskjellen. Går strøm eller samband går begge nettene ned. Problemer for utstyr kan ofte relateres til 2G teknologien – eksempelvis kapasitet, lang responstid eller kjernenettet. Slike problemer løses ikke nødvendigvis ved roaming da mobilutstyret vil oppleve at den har tilgang til nettet og ikke vil søke etter annet nett. Verdikjeden for roaming er også langt mer kompleks og trafikken rutes ut av Norge og hjem igjen til Norge over internett for å nå kundens server – via en internasjonal carrier. Dette gir en større sannsynlighet for brudd og

[2] Helsedirektoratet (2014): IS-2225 «*Helsedirektoratets anbefalinger på det velferdsteknologiske området*»

feil. Er feilen hos hjemme-operatøren, internasjonal carrier - eller på veien til eller fra hjemme-operatøren? Er det en alvorlig feil hos internasjonal carrier går alle enhetene ned samtidig. Roaming innebærer et oppsplittet ansvarsforhold og i en feilsituasjon så er feilsøking, feillokalisering vanskeligere og må rettes mot hjemme-operatøren. Avslutningsvis så er roaming en mer kostbar måte å produsere konnektivet på. Hvem dekker denne kostanden?(Sitat Telenor slutt).

Med bakgrunn i dette, og utviklingen vi ser innen 4G/LTE, så er ikke anbefalingen om nasjonal roaming gjentatt her. Dette betyr ikke at nasjonal roaming frarådes, men at ønsket effekt sannsynligvis ikke er så stor som tidligere vurdert.

Det anbefales å sette følgende minimumskrav for å sikre pålitelig kommunikasjon mellom teknisk løsning hos tjenestemottaker og responssenterløsning:

- **Valg av mobiloperatør bør tilpasses lokale dekningsforhold der hvor løsningen skal benyttes.**
- **I områder med begrenset mobildekning bør det være mulig å benytte utstyr som kan tilkobles ekstern antenne og/eller mulighet for å benytte simkort fra annen nettverksleverandør (bytte SIM kort eller dual-SIM).**
- **Der det er mulig bør fast bredbånd benyttes som en alternativ kommunikasjonskanal**
- **Det bør avtales en utviklingsplan med løsningsleverandør om en gradvis overgang fra 2G til 4G/LTE med støtte for minimum 800 MHz båndet.**

2.3 Responssenterløsning og teknisk driftsløsning

2.3.1 Pålitelighet

Direktoratet for e-helse anbefaler:

- **Sentral responssenterløsning og teknisk driftsløsning skal fungere minimum 99,9 % av tiden målt 24/7 per måned. Dette inkluderer ikke planlagt vedlikeholdsvindu.**
- **Driftsoppsett for responssenterløsning og teknisk driftsløsning må inneholde profesjonelle driftsrutiner med tilhørende kvalitetskrav.**
- **Formaliser samarbeid med leverandøren om tiltak som reduserer risikoen for kvalitetsbrudd og reduserer konsekvensene ved brudd.**
- **Etabler beredskapsrutiner for aksjon hvis de tekniske løsningene ikke fungerer.**
- **Planlagt vedlikehold må avtales og tilpasses tjenestens belastning.**

Både responssenterløsning og teknisk driftsløsning er sentrale kritiske komponenter i tjenesten. Slutter disse løsningene å fungere så mottas ingen varsler fra noen av de påkoblede løsningene hos tjenestemottakerne. Da mange tjenesteytere kun kan komme i kontakt med hjelp via sin alarmknapp vil det kunne få alvorlige følger om systemet i fungerer.

Ustabile systemer medfører at kommunene må ha ekstra beredskap som medfører merarbeid og redusert effektiviseringsgrevinst. Det er derfor viktig at disse løsningene fungerer til enhver tid. Flere leverandører opererer i dag med 99,9 % oppetid målt 24/7. Dette utgjør ca. 45 minutter nedetid totalt per måned. Planlagt vedlikehold på systemet er forutsigbart og kan kompenseres med planlagt beredskap i tjenesten. Planlagt vedlikehold bør allikevel resultere i minimal nedetid for systemet og bør legges i tid der det gir minst belastning for tjenesten. Er det behov for lengre servicevinduer må det planlegges med to parallelle løsninger der den ene alltid er tilgjengelig. Det er nødvendig at det identifiseres og arbeides med tiltak som reduserer risiko og konsekvens i samarbeid med leverandøren.

Skulle det allikevel skje at løsningen slutter å fungere må det være etablert beredskapsrutiner i tjenesten som kan iverksettes. I slike situasjoner er det er spesielt viktig at responssentertjenesten har mulighet til å kommunisere med utførende enheter selv om ikke responssenterløsningen fungerer. For eksempel må alternative kommunikasjonsløsninger kunne benyttes hvis valgt mobilnett er nede. Andre mobiloperatører eller nødnett kan være slike alternativer.

Minimum 99,9 % oppetid på sentrale løsninger setter strenge krav til driftsoppsettet av sentrale komponenter i løsningene. Det må tas høyde for systemfeil, strømstans, kabelbrudd, vannskader, brann, innbrudd, mm.

Det anbefales at det gjennomføres en risiko- og sårbarhetsanalyse (ROS) før idriftsettelse. En slik analyse bør bl.a. omfatte behandling av følgende spørsmål:

- **Hva kan feile i løsningen hos tjenestemottaker?**
- **Hva kan feile i kommunikasjonsløsningen?**
- **Hva kan feile i sentrale løsninger (responssenterløsning og teknisk driftsløsning)?**

Hvis sannsynligheten vurderes som høy og konsekvensene store må det identifiseres tiltak som kan redusere sannsynlighet og risiko. Det anbefales at risikobildet og tiltak følges opp i et månedlig driftsmøte mellom innkjøper og leverandør.

Eksempler på tiltak som bør vurderes:

- Beredskapsrutiner i responssentertjenesten hvis løsningen er nede
- Redundans for sentrale komponenter
- Automatisk re-ruting til alternativt mottak hvis løsningen er nede
- Gode rutiner for backup og vedlikehold
- Reservedelslager

Det anbefales at det settes følgende minimumskrav til driftsoppsett for sentrale løsninger:

- **Kvalitetsavtale (SLA) som omfatter oppetid, feilrettingstid knyttet til kritikalitet på feil og rutiner for vedlikehold og oppdateringer.**
- **Nødstrømsforsyning for langvarig bortfall av strømnettet (minimum 1 ukes varighet).**

- **Daglig sikkerhetskopiering av logger, data og konfigurasjoner.**
- **Fortløpende dokumentasjon av tilgjengelighet, innmeldte feil med kritikalitetsnivå, feilrettingstid.**
- **Driftslokalene må holde korrekt klima for server utrustningen og personalet.**
- **Driftslokalene må være utstyrt med slukningsutstyr som raskt kan slukke brann i lokalet.**
- **Driftslokalet må være tilkoblet et brannvarslingssystem som er i direkte kontakt med det lokale brannvesenet.**
- **Driftslokalene må ha et adgangskontrollsystem som sikrer at kun godkjent personale får adgang.**
- **Driftslokalene må være best mulig sikret mot innbrudd og være tilkoblet innbruddsalarm som er i direkte kontakt med et vaktselskap.**

2.3.2 Funksjonalitet

2.3.2.1 Responssenterløsning

Direktoratet for e-helse anbefaler:

- **Responssenterløsningen skal gi nødvendig støtte for gjennomføring av arbeidsoppgavene i responssentertjenesten omfattet av; tilpasse tjenesteoppsett, motta varsler, logge hendelser, dialog med tjenestemottaker, vurdere hendelser, beslutte aksjon, overlevering til utførende enhet og avslutning og dokumentasjon av hendelser.**
- **Løsningen skal kunne betjenes både fra faste og mobile terminaler.**
- **Responssenterløsningen skal gi fortløpende oversikt over resultater og statistikker knyttet til avtalte kvalitetsparametere - som for eksempel svartid og avklaringsgrad**

Responssenterløsningen er primærverktøyet for responssentertjenesten. Verktøyet skal understøtte tjenestens arbeidsforløp – motta varsel om hendelse, logge hendelse, dialog med tjenestemottaker, vurdere hendelse, beslutte aksjon, overlevering til utførende tjeneste ved behov og avslutning av hendelse. I tillegg må løsningen støtte oppsett og endring av tjenesten i henhold til vedtak. Responssenterløsningen må legge til rette for at relevant informasjon knyttet til hendelser kan vises i IT-verktøy som benyttes i utførende tjeneste.

Det anbefales at det settes følgende minimumskrav til funksjonalitet i responssenterløsningen[3]:

- **Oppdatert relevant informasjon om tjenestemottaker må kunne vises for tjenesteoperatøren når en hendelse oppstår (se kapittel nedenfor om informasjonsutveksling).**

[3] Informasjonsbehandling forutsetter nødvendig rettslig grunnlag (ref. Norm for informasjonssikkerhet i helse- og omsorgstjenesten)

- **Teknisk løsningskonfigurasjon hos tjenestemottaker må kunne registreres. Gjennomføringen av selve konfigurasjonen kan gjøres ved hjelp av teknisk driftsløsning.**
- **Hendelser må kunne tildeles et saksnummer og lagres i en logg. Følgende informasjon må minimum kunne lagres per hendelse: Tjenestemottaker, type hendelse, tidspunkt for varsel og kritikalitet der det er nødvendig.**
- **Ved varsel skal det automatisk opprettes en toveis tale- og/eller videokommunikasjon med løsning hos tjenestemottaker.**
- **Alle samtaler mellom tjenestemottaker og responssentertjenesten skal lagres automatisk. Lydloggen skal oppbevares forsvarlig i minimum 6 måneder.**
- **Gi mulighet for å integrere beslutningsstøtte etter behov.**
- **Gi mulighet for raskt å kontakte utførende tjeneste og gi denne den nødvendige informasjon, eventuelt viderekoble tale/video forbindelsen med tjenestemottaker. (se kapittel nedenfor om informasjonsutveksling).**
- **Sette regler for varsling og ruting av spesifikke hendelser knyttet til spesifikke tjenestemottakere til alternative mottakere (for eksempel lokasjonsvarsler fra «Anna» rutes til pårørende).**
- **Logge kvalitetsdata som svartid, reaksjonstid, responstid for responssentertjenesten og silingsgrad, og produsere grafiske fremstillinger av resultater i flere tidsintervaller (time, dag, uke og måned).**
- **Gi tydelig varsel om et innkommende varsel ikke blir besvart innen gitte krav til svartid.**
- **Løsningen bør kunne betjenes fra både faste og mobile terminaler.**

2.3.2.2 Teknisk driftsløsning

Direktoratet for e-helse anbefaler:

- **Teknisk driftsløsning skal gi nødvendig støtte for teknisk overvåkning, feilretting, vedlikehold, programvareoppdatering og konfigurasjonsendringer av den tekniske løsningen hos tjenestemottaker (se underkapittel «Drift» i kapittelet «Teknisk løsning hos tjenestemottaker»).**
- **Teknisk driftsløsning skal gi støtte for en filtrering av tekniske varsler slik at kun varsler fra de tekniske hendelsene som har betydning for tjenestens kvalitet blir sendt videre til responssenterløsningen.**
- **Teknisk driftsløsning kan bestå av flere leverandørspesifikke løsninger tilpasset det utstyret som benyttes hos tjenestemottakerne.**

Teknisk driftstjeneste må både respondere på tekniske varsler og utføre planlagte vedlikehold (for eksempel programvareoppdatering). Denne funksjonen skal også utgjøre et effektivt filter mot responssentertjenesten for tekniske varsler. Kun tekniske hendelser som kan ha betydning for kvaliteten på responssentertjenesten skal varsles. Det finnes i dag ingen standarder som dekker alle funksjonene som en slik teknisk driftsløsning skal utføre for alle varianter av løsninger hos tjenestemottaker. De beste driftsløsningene leveres ofte av

utstyrsleverandørene selv. Det er hensiktsmessig at disse benyttes inntil dette området eventuelt blir mer standardisert. Et sentralt driftsoppsett kan derfor bestå av like mange driftsløsninger som det er utstyrsleverandører. Det er derimot viktig at kvaliteten på den tekniske overvåkningen og filtreringen av varsler er mest mulig lik.

Det anbefales at det settes følgende minimumskrav til funksjonalitet i teknisk driftsløsning:

- **Motta tekniske varsler fra løsning hos tjenestemottaker i henhold til anbefalingene gitt i underkapittel «Drift» i kapittelet «Teknisk løsning hos tjenestemottaker».**
- **Støtte for fjern-konfigurering av tjenesteregler og tekniske varsler i løsning hos tjenestemottaker.**
- **Filtrere varsler og videresende til responssenterløsningen kun varsler om de tekniske hendelser som har betydning for tjenestens kvalitet.**
- **Støtte for konfigurering av ruting av varsler til alternativt mottak ved feil på responssenterløsningen.**
- **Løsningen bør kunne betjenes fra både faste og mobile terminaler.**
- **System for utstyrsadministrasjon hvor hvert utstyrselement har en unik ID og hvor bl.a. informasjon om utstyrstype, plassering, programvareversjon, konfigurasjon, kommunikasjonsleverandør, forventet gjenstående batterilevetid og feilmeldinger blir holdt oppdatert.**

2.3.3 Brukervennlighet

Direktoratet for e-helse anbefaler:

- **Responssenterløsningen må ha enkle og intuitive brukergrensesnitt.**
- **Skjermgrensesnitt bør følge IKT-forskriftens henvisning til WCAG 2.0 (Web Content Accessibility Guidelines) nivå AA (ISO/IEC 40500:2012) eller tilsvarende.**
- **Brukergrensesnittene må tilpasses både faste og mobile terminaler.**

Responssenterløsningen må være utformet på en slik måte at operatørene kan ekspedere innkomne saker så raskt som mulig uten å miste oversikt. Responssenterløsningen skal kunne betjenes av personell med ulike fysiske forutsetninger og variabel erfaring med IT. Det er viktig at både de skjermbaserte og fysiske brukergrensesnittene i responssenterløsningen er så enkle og intuitive som mulig.

Difi publiserer krav til nettløsninger/skjermbaserte systemer på: https://uu.difi.no

2.3.4 Kommunikasjonsgrensesnitt

Direktoratet for e-helse anbefaler:

- **Responssenterløsningen må støtte tilsvarende kommunikasjonsgrensesnitt som angitt i underkapittelet «Kommunikasjonsgrensesnitt» i kapittelet «Teknisk løsning hos tjenestemottaker» (kap. 2.1.4).**
- **Responssenterløsningen må integreres mot relevante grensesnitt (APIer) knyttet til e-helse løsninger (for eksempel kommunale fagsystem, helsenorge.no) når disse foreligger.**
- **Teknisk driftsløsning kan benytte leverandørspesifikke grensesnitt mot løsning hos tjenestemottaker.**

Responssenterløsningen skal kommunisere med løsning hos tjenestemottaker gjennom de grensesnittene som er anbefalt for dette. Teknisk driftsløsning kan kommunisere med løsning hos tjenestemottaker gjennom leverandørspesifikke grensesnitt. Kommunikasjonsgrensesnitt mellom responssenterløsning og andre e-helse løsninger (for eksempel kommunalt fagsystem/EPJ) er ennå ikke klart definert i den nasjonale e-helse arkitekturen. Inntil videre anbefales det at leverandørene av fagsystemene lager spesifikke grensesnitt (APIer) for håndtering av noen spesifiserte basis informasjonselementer. Responssenterløsningen må integreres mot disse APIene når de foreligger. Se kapittelet «Informasjonsutveksling» for nærmere informasjon om informasjonselementene.

2.3.5 Sikkerhet og informasjonshåndtering

Direktoratet for e-helse anbefaler:

- **Alle løsningene må følge krav satt i «Norm for informasjonssikkerhet i helse- og omsorgstjenesten» med tilhørende «Veileder i personvern og informasjonssikkerhet ved bruk av velferdsteknologi»**

«Veileder i personvern og informasjonssikkerhet ved bruk av velferdsteknologi» (https://ehelse.no/veileder-i-personvern-og-informasjonssikkerhet-ved-bruk-av-velferdsteknologi) belyser regelverk, ansvarsforhold og informasjonssikkerhet og inneholder eksempler på brukerhistorier ved bruk av velferdsteknologi. Revidert versjon av denne veilederen forventes å være tilgjengelig ila 2016.

2.4 Informasjonsutveksling

Direktoratet for e-helse anbefaler:

- **Det må være tilrettelagt for effektiv informasjonsutveksling mellom responssenterløsning og kommunalt fagsystem/EPJ.**
- **Leverandører av kommunale fagsystem/EPJ må presentere hvordan denne informasjonsutvekslingen kan gjennomføres, og leverandører av responssenterløsning må tilpasse seg dette.**
- **Direktoratet for e-helse vil arbeide med en nasjonal tilnærming på dette som bør følges.**

Riktig og relevant tilgang til informasjon er nødvendig for at hvert ledd i tjenestekjeden skal kunne utføre sine oppgaver best mulig. Eksempler på dette er vist nedenfor.

Som ansatt i responssentertjenesten ønsker jeg …

- … å kunne se informasjon om bruker som kan være av betydning for vurdering og oppfølging av utløst varsel, slik at jeg kan gjøre en best mulig vurdering av hvordan tjenestemottaker bør følges opp i det enkelte tilfelle.
- … å bruke kun responssenterløsningen for å dokumentere hendelsen, slik at jeg slipper å drive «dobbeltregistrering» i to systemer.
- … å kunne videreformidle hendelsesinformasjon til utførende tjeneste i de tilfeller hvor det er mest hensiktsmessig at de tar aksjon.

Som ansatt i utførende tjeneste ønsker jeg …

- … å kunne få informasjon om hendelsen når responssentertjenesten beslutter at utførende tjeneste må ta aksjon.
- … å få et varsel om det har inntruffet hendelser som det er viktig å vite om før neste planlagt besøk.

I samarbeid med representanter fra helse- og omsorgstjenesten i flere kommuner er det kartlagt et minimum sett av informasjon som må utveksles mellom responssenterløsningen og kommunalt fagsystem/EPJ. Det arbeides nå videre i Direktoratet for e-helse med å se på dette behovet i sammenheng med andre behov for informasjonsutveksling med kommunale fagsystem/EPJ. Det er behov for at responssenteroperatøren har tilgang til oppdatert informasjon om tjenestemottaker – personalia, helseopplysninger, besluttede vedtak og tiltak, og daglig besøksplan. Når en hendelse registreres i responssenteret er det behov for at informasjon kommer inn i fagsystemet/EPJ uten behov for dobbeltregistrering – informasjon om hendelsen (tid, sted, beskrivelse, data fra utstyr hos tjenestemottaker), og besluttet videre aksjon. Det er også behov for at responssenteroperatøren skal kunne legge inn kommentarer med forslag til endringer i tiltak.

3 Oppfølging av anbefalingene

Følgende tiltak igangsettes i Direktoratet for e-helse knyttet til disse anbefalingene:

1) Ressurser vil være tilgjengelig for diskusjoner og rådgivning knyttet til anskaffelsesaktiviteter

2) Dialog med leverandørene av kommunale fagsystem for å stimulere til at de etablerer APIer til sine løsninger som dekker behovet for informasjonsutveksling med responssenterløsning i henhold til definert basis nivå av informasjonselementer

3) Videreutvikle anbefalingene når ny kunnskap og erfaring foreligger

Direktoratet for e-helse

Besøksadresse
Verkstedveien 1
0277 Oslo

Postadresse
Postboks 6737
St. Olavs plass
0130 OSLO