



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til enhetene	JA/NEI
	Kamera monteres på vegg eller i tak med skruer og nettverkstilførsel. Den kan enkelt skrues ned, men er primært for permanent plassering. Enheten vil etterlate seg skruer i vegg når den monteres ned.	

Tabell 3 – Krav til enhetene

- Krav til applikasjoner og varsler**

Følgende krav til applikasjoner og varsler skal besvares for alle delkonkurranser.

Krav markert med: Dersom dette ikke er på plass pr. d.d., skal Leverandøren dokumentere konkrete planer og tilnærming for at dette er på plass innen teststart. (Med «på plass» menes at løsningen er ferdig utviklet og testet av Leverandør.)*

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til applikasjoner og varsler	JA/NEI
4.1 (M)	Løsningens applikasjon for respons- og varselhåndtering, administrasjon, og konfigurering og drift av enheter, skal leveres som SaaS løsning og er tilgjengelig via et web-grensesnitt ved bruk av vanlige nettlesere. <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet blir ivarettatt.	JA

Leverandørens besvarelse:

Løsningen leveres som en web-applikasjon som kan åpnes fra vanlige nettlesere. Web-grensesnittet består av forskjellige moduler for følgende funksjonalitet: alarmering, videoavspilling, tjenestemottaker, tjenesteutøver og hendelseslogg. Tilgang til de forskjellige modulene er kontrollert av rolle.

Web-grensesnittet er laget med responsivt design og tilpasser seg skjermstørrelsen slik som vist i figurene under.

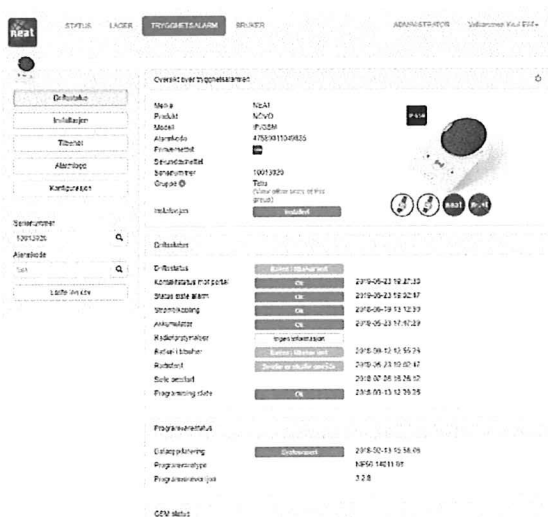


Fra web-grensesnittet vil det for konfigurasjon av gatewayer, sensorer og videokamera lenkes direkte

AMG
ARE



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

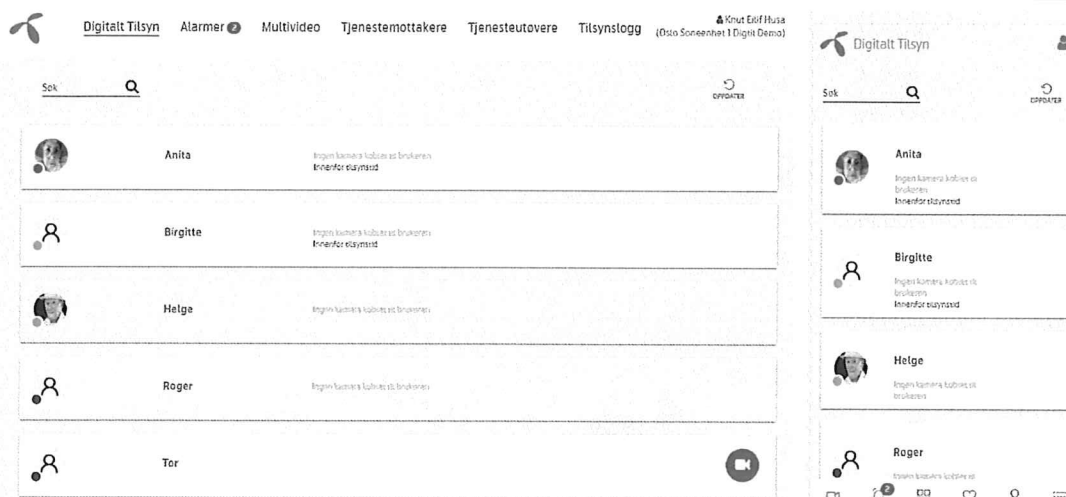
Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til applikasjoner og varsler	JA/NEI
	inn til de bakenforliggende administrasjonsløsningene for enheter uten at man må logge på med ny bruker. I figuren under er det et eksempel hvor en tjenestemottaker har to enheter tilknyttet til seg, en gateway og et videokamera. Ved å klikke på «Konfigurer» under avansert konfigurasjon blir man videresendt til riktig videokamera for å utføre enhetskonfigurasjon. Enheter 10121380 + Legg til Avansert konfigurasjon 10121380 Konfigurer 	
4.2 (M)	Systemet skal fungere på alle arbeidsflater (PC, MAC, nettbrett, mobil) og har et responsivt design slik at de automatisk tilpasser seg ulike enheters skjermformater. <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet blir ivaretatt.	JA
Leverandørens besvarelse: Systemet fungerer på alle arbeidsflater. I figurene under vises skjermbildet for alarmvisning på PC/MAC og mobilterminal. På PC/MAC vil det til venstre i skjerm vises en meny for forskjellige modulene i løsningen. Denne menyen legges på rad nederst i skjermbildet på en mobilterminal. På PC/MAC vil det i digitalt tilsyn funksjonen vises en liste over tjenestemottakere, med knapper for å starte tilsyn. På mobilterminal vil knappene bli større og lettere å betjene med fingrene		

ikke
cut



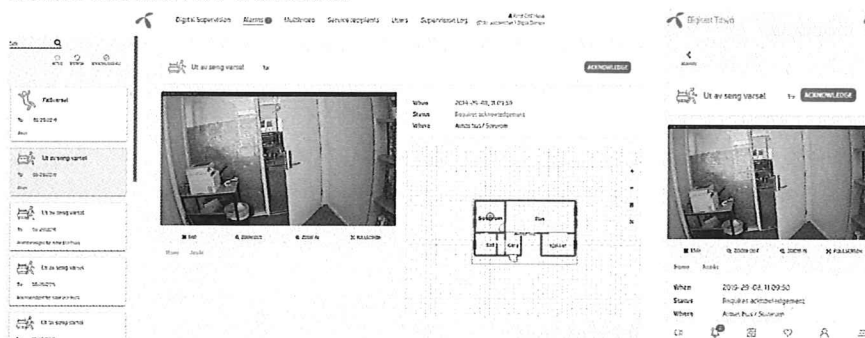
Oslo kommune Helseetaten Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til applikasjoner og varsler	JA/NEI
----------	---	--------



Skjermbilder for digitalt tilsyn

Videre vil man på PC/MAC se listen over alle alarmer samtidig som man kan velge å gå inn i en alarm for å se på video, kart og detaljer. På mobilterminal velger man først alarm, og deretter går man inn i denne alarmen for å avklare.



Skjermbilder for alarmvisning

4.3 (M)	Leverandørens enheter og eventuelle APPer skal være integrert i det samme administrasjonssystemet. <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet blir ivarettatt.	JA
---------	---	----

Leverandørens besvarelse:

Alle enhetene kan administreres fra et grensesnitt med én pålogging. Administrasjonssystemet kan brukes fra PC, mobil eller nettbrett. En pålogging per administrator.

are out



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til applikasjoner og varsler	JA/NEI
	Enheter 10121380 + Legg til Avansert konfigurasjon 10121380 Konfigurer	

Administrasjon i løsningen er basert på at man anvender en Digitalt tilsyn applikasjon og administrasjonssystemet til enhetsleverandøren. I Digitalt tilsyn applikasjonen gjør man administrasjon av:

- tjenestemottaker
 - definisjon av tilsynstider
 - tilordning av tjenestemottaker til grupper
 - spesifisere hvilke tjenesteutøvere som skal ha varsel
 - kontrollere hvilke varsel som skal aktiveres for tjenestemottaker
 - tilordning av enheter/utstyr til tjenestemottaker
 - gjøre lenkehopp (ingen innlogging) til aktuelle enheter i utstyrsleverandørens konfigurasjonssystem
- tjenesteutøver
 - endre passord
 - blokkere fra system
 - endre rolle
 - tilordne tjenestemottaker som denne tjenesteutøver kan se

I utstyrsleverandørens konfigurasjonssystem utfører man detaljert konfigurasjon av enheter. Dette innebærer blant annet:

- Gateway
 - Legge til nye sensorer

Arve
Curtis



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til applikasjoner og varsler	JA/NEI
	○ Gjøre detaljert gateway-konfigurasjon som f.eks. styring av volum, lyssignal og forsinkelse ○ Gjøre detaljert sensorkonfigurasjon som f.eks. setting av lokasjon for sensor, styring av radiokoder	
4.4 (M)	Konfigurasjonsendringer, enkel feildiagnose/retting, programvareoppdateringer (firmware) og omstart av enhetene skal enkelt kunne utføres fra sentral driftsløsning/administrasjonssystem (dvs. uten behov for fysisk tilgang til enheten). <u>Utformingskrav</u> Beskriv hva som kan utføres fra sentral driftsløsning/administrasjonssystem, og hva som eventuelt ikke kan utføres fra denne.	JA

Leverandørens besvarelse:

Det er ingen behov for lokal firmware/programoppgraderinger av klientutstyr ettersom serverløsningen gjøres tilgjengelig via web grensesnitt.

Apper må lastes ned fra Google Play, appstore. Telenor kan tilby MDM (Mobile Device Management) hvis dette er ønskelig.

Oppgaver som kan utføres sentralt fra administrasjonsgrensesnittet:

- Konfigurasjon av enhetene (gateway, videokamera, sengesensor, døralarm)
- Se oversikt over batteristatus på enhetene som ikke går på strøm
- Motta varsel fra enheter som ikke er tilgjengelig (kan være nettverksfeil, strømbrudd etc)
- Restart

Kan ikke utføres sentralt:

- Bytte batteri
- Stille inn vinkel på videokamera

Firmware på enheter som er plassert hos tjenestemottaker blir automatisk oppdatert. Gateway vil kontinuerlig synkronisere seg med server for å ha siste firmware installert:

Firmware status

Data update

Firmware type

Firmware version

Synchronized

NE50 14011-01

5.1.38

2019-08-28 10:40:31

For kamera vil tjenesteleverandør ha oversikt over firmware på alle enheter og kunne initiere firmware oppgradering når nye versjoner legges ut. Dette håndteres fra tjenesteleverandørs serverløsning:

Settings / Edit device Digit224 (ACCC8ED351D2)

Device information

Name

MAC address

Model

Firmware version

New upgrade available

Digit224

ACCC8ED351D2

M1065-L

8.40.2.1

Upgrade to 8.40.2.2

Arve
Chis



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til applikasjoner og varsler	JA/NEI
4.5 (E2)	Administrasjonssystemet bør operere smidig og med minst mulig tidsbruk ved oppsett/installasjon, vedlikehold, konfigurasjonsendringer, og feilhåndtering av enheter. <u>Utformingskrav</u> • Beskriv hvordan en standard installasjon med standard oppsett/konfigurering gjøres, inklusiv tidsestimat • Beskriv fremgangsmåte og tidsbruk knyttet til vedlikehold og konfigurasjonsendringer, inklusiv tidsestimat • Beskriv hvordan enkel feildiagnose/retting gjennomføres, inklusiv tidsestimat Leverandøren viser også hvordan kravet oppfylles gjennom demonstrasjon iht. oppgitte demosituasjoner i Vedlegg 1 Beskrivelse av demonstrasjoner.	JA
Leverandørens besvarelse: Generelle forutsetninger for beskrivelsene: • Tjenesteutøver har en gyldig aktiv systembrukerkonto med applikasjonsrolle som har tilgang til aktuell funksjonalitet og tilgang til aktuell tjenestemottaker • Beskrivelsene nedenfor inkluderer ikke innlogging eller fysisk montasje i tjenestemottakers hjem. 1. Standard installasjon med standard oppsett/konfigurering av kamera og gateway – 3min Forutsetning: Kamera og gateway er forhåndsregistrert i løsningen med id/enhetskode/serienummer som del av logistikk og lagerstyringsprossene. Kamera og gateway vil ved første aktivering kunne laste ned oppdatert programvare dersom enheten har vært avslått over lengre tid. Dette er ikke medregnet • Registrer tjenestemottaker med navn og/eller andre identifiserende opplysninger • Legg tjenestemottaker til riktig(e) gruppe(r) • Angi tilsynstid kamera • Legg til kameraenhet og gateway • Kontroller kameraenhet og bilde • Konfigurer gateway ○ Last standardkonfigurasjon – skjer automatisk ○ Legg til én sensor med tidsvindu 2. Vedlikehold og konfigurasjonsendringer – 2 min NB! Kamera og gateway er selv-oppgraderende med ny programvare. Ingen vedlikeholdsoppgaver er nødvendig. Forutsetning: Kamera, gateway og sensorer er allerede montert i tjenestemottakers hjem og fungerer		

Alle
OK



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til applikasjoner og varsler	JA/NEI
som forventet. • Legg til en ny gruppe som skal ha tilgang til å se tjenestemottagers kamera • Endre tilsynstid for kamera • Legge til bevegelsesdeteksjon for kamera • Endre aktivt tidsvindu for sensor 3. Feildiagnose/retting - 2 min Forutsetning: Kamera, gateway og sensorer er allerede montert i tjenestemottakers hjem. Enkelte hendelser er ikke varslet iht ønsket konfigurasjon. • Verifisere kamera og gateway driftsstatus • Verifisere tilsynstid for kamera • Verifisere aktiv varsling fra kamera • Verifisere sonemarkering for kamera • Endre sonemarkering for kamera • Verifisere sensor konfigurasjon og tidsrom • Endre aktivt tidsvindu for sensor		
4.6 (E2)	Løsningen bør gi tydelig og handlingsveiledende tilbakemelding til systembruker ved feilet oppgave/transaksjon og heng/frys i systemet. <u>Utformingskrav</u> Beskriv hvilke feilmeldinger som presenteres til systembruker og ikke. Beskriv også i hvilken grad feilmeldingene har tydelig og beskrivende tekst.	JA
Leverandørens besvarelse: I Digitalt tilsyn applikasjonen er det tydelig tilbakemelding når det oppstår situasjoner som gjør at tjenesteutøver ikke får utført oppgavene sine. I figuren under vises det et par eksempler på dette; når en tjenesteutøver prøver å aksessere et videokamera utenfor tilsynstid og melding til tjenesteutøver hvis videostrømmen er blir brutt.		

cul
are



Oslo kommune
Helseetaten

Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til applikasjoner og varsler	JA/NEI
4.7 (E2)	Systemet bør gi god oversikt over enheter i Oslo Kommune, og kan tilpasses etter Kundens behov. <u>Utformingskrav</u> Beskriv hvordan Kunden kan holde oversikt over sine enheter. Det vil f.eks. telle positivt om det i løsningen fremstilles en oversikt over enheter, som skiller på om en enhet er aktiv og installert hos en tjenestemottaker, eller om en enhet er inaktiv (ikke utplassert hos tjenestemottaker) eller om det er en testenheter. Leverandøren viser også hvordan kravet oppfylles gjennom demonstrasjon iht. oppgitte demosituasjoner i Vedlegg 1 Beskrivelse av demonstrasjoner.	JA
Leverandørens besvarelse: Løsningen har et administrasjonssystem for enhetsstyring og konfigurasjon. I dette grensesnittet det mulig å se hvilken sone (kunde) hvor enhet er installert, hvilken status (aktiv/inaktiv) det har og når man sist har hørt fra enheten. Hvis enheten ikke er utplassert i noen sone, vil dette feltet være tomt. Videre er det mulighet til å bruke abonnementsfeltet til å sette om dette er en testenheter eller produksjonsenhet. I enhetsprofilene kan man spesifisere hvordan innkommende meldinger skal behandles. I enhetsprofilene kan man bla. spesifisere tekniske hendelser man skal rapportere på og hvem som skal motta disse varslene, varslinger ved lavt batterinivå og statistikkhendelser. Man kan også tildele enheten til sone administrasjonssystemet.		

Ch6
Jre



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.

Leverandørens løsningsbeskrivelse – Krav til applikasjoner og varsler

JA/NEI

Enhetsbehandling

Generell

Teknisk

Abonnement

Opprett mange

Aktiver

Deaktiver

Tildel kunde

Sett abonnement

Sett enhetsprofil

Stelt

▼ Vis filter

☐	Navn	Enhets-ID	Type	Abonnement	Enhetsprofil	Siste melding	Kunde
☒	✓	7897253 7897253	Caretech		Standard	2016-08-30 12:52:48	TnO demo
☒	✓	882393254060780 7810374	Caretech		Standard	2017-11-13 09:48:08	TnO demo
☒	✓	Blodsukker 355496041319922	MODZ		Standard	2018-07-18 12:20:09	TnO demo
☒	✓	Blodtrykk 00091f800662	UA-767		Standard	2016-06-28 12:22:27	TnO demo
☒	✓	Blodtrykk-demo 00091f800673	UA-767		Standard	2017-10-25 10:39:14	TnO demo
☒	✓	digitil109 ACCC8E9950C4	AXIS kamera	Digitalt Tilsyn Axis	Standard	Idag, 10:35:39	TnO demo
☒	✓	Digitil211 ACCC8ED25C02	AXIS kamera	Digitalt Tilsyn Axis	Standard		TnO demo
☒	✓	Digitil23 626E640088	Foscam FI9826P	Digitalt Tilsyn Celerway	Standard		TnO demo
☒	✓	Digitil4 11223344	Foscam FI9826P	Digitalt Tilsyn Celerway	Standard	2016-05-11 09:44:28	TnO demo
☒	✓	DigitilTest C4D6553C7C4E	Foscam FI9826P		Standard	2018-06-25 16:26:04	TnO demo
☒	✓	DigitilTest ACCC8E93F0F1	AXIS kamera		Standard	2019-05-16 09:13:17	TnO demo
☒	✓	Edvin iPhone D-95133F99-BS1B-48AF-B51D- 3443771698AB	SmartTracker GPS for iPhone		Standard	2017-07-08 11:28:33	TnO demo
☒	✓	Gateway 7829740	Caretech		TnODeviceProfile	2017-01-24 08:20:25	TnO demo
☒	✓	Johan Android D-5EA9C68F-9B73-4AB4-8DDD- 138771CA3C97	SmartTracker GPS for Android		Standard	2017-07-25 20:52:54	TnO demo
☒	✓	Magnes iPhone D-500D9351-1A93-4BAA-B579- 5A5A5CAD0605	SmartTracker GPS for iPhone		Standard	2017-10-05 10:24:50	TnO demo

1

2 Neste

1 - 15 / 24

4.8 (M)

Løsningen skal jevnlig sjekke at det er kontakt med enhetene.

Utformingskrav

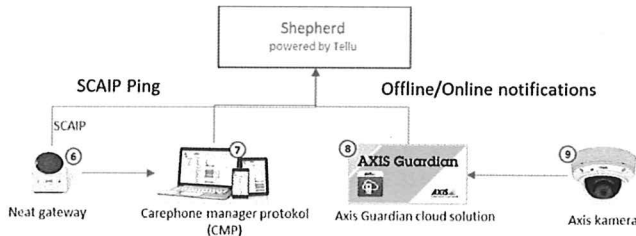
Beskriv hvordan løsningen er satt opp for å sjekke kontakt mellom enheter og applikasjon (f.eks. gjennom at enheter sender «heart-beat» for nedetidsovervåkning). Beskriv også mulighet for å justere frekvens på dette.

JA

oks
vike



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til applikasjoner og varsler	JA/NEI																						
Leverandørens besvarelse: Gateway sender heartbeats til systemet hvert 5 min. Dette intervallet kan justeres. Videokamera sender heartbeats til systemet hvert 3 min. Dette intervallet kan ikke justeres. Sensorer tilkoblet Gateway kan konfigureres for radioovervåkning. Gateway sjekker da radiokontakt med sensor hver 9'ende time og leverer indikasjon om brutt forbindelse til systemet hvis kontakt med sensor ikke oppnås. Intervallet for radiokontaktsjekk kan konfigureres, men hyppigere sjekking vil gå utover batterikapasiteten på sensoren. Hver 9'ende time er valgt som et kompromiss mellom batterikapasitet og behov for varsel om at sensor ikke er tilgjengelig.																								
																								
4.9 (M)	Administrasjonssystemet skal motta varslinger fra enhetene, og alle varsler skal loggføres. <u>Utformingskrav</u> Beskriv hvilke varsler som loggføres og på hvilken måte. Ulike typer varsler kan f.eks. være varsler ved utløst alarm, teknisk svikt som følge av strømbrudd/nettbrudd (om enheter er online eller ikke), lavt batterinivå (inkl. batterinivå), varsler ved testing, og eventuelle andre oppdagede funksjonsfeil.	JA																						
Leverandørens besvarelse: Både tekniske varsler og hendelser ved utløst alarm lagres i hendelsesloggen. Tabellen under viser hvilke hendelser som logges for de ulike enhetene. <table><tr><th>Sensorer</th><th>Videokamera</th></tr><tr><td>Akkumulator lav</td><td>Frakoblet</td></tr><tr><td>Akkumulatorspennings</td><td></td></tr><tr><td>Strøm tilkoblet/frakoblet</td><td></td></tr><tr><td>Manglende «Heartbeat»</td><td>Tilkoblet</td></tr><tr><td>Radioforstyrrelser</td><td></td></tr><tr><td>Batteri i sensorer lavt</td><td></td></tr><tr><td>Batteri i sensorer ok</td><td></td></tr><tr><td>Feil på sekundær eller primærnett</td><td></td></tr><tr><td>Sensor utenfor område</td><td></td></tr><tr><td>GPS koordinater på basestasjon som enheten</td><td></td></tr></table>			Sensorer	Videokamera	Akkumulator lav	Frakoblet	Akkumulatorspennings		Strøm tilkoblet/frakoblet		Manglende «Heartbeat»	Tilkoblet	Radioforstyrrelser		Batteri i sensorer lavt		Batteri i sensorer ok		Feil på sekundær eller primærnett		Sensor utenfor område		GPS koordinater på basestasjon som enheten	
Sensorer	Videokamera																							
Akkumulator lav	Frakoblet																							
Akkumulatorspennings																								
Strøm tilkoblet/frakoblet																								
Manglende «Heartbeat»	Tilkoblet																							
Radioforstyrrelser																								
Batteri i sensorer lavt																								
Batteri i sensorer ok																								
Feil på sekundær eller primærnett																								
Sensor utenfor område																								
GPS koordinater på basestasjon som enheten																								

only
file



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til applikasjoner og varsler	JA/NEI																																																																																																											
	<table><tr><td>kommuniserer med</td><td></td></tr><tr><td>ICCID på SIM-kort</td><td></td></tr><tr><td>Feil i konfigureringen</td><td></td></tr><tr><td>Mislykket brukeranrop</td><td></td></tr><tr><td>Signalstyrke 4G/GSM nett</td><td></td></tr><tr><td>Nettverksinformasjon</td><td></td></tr><tr><td>Produkttype</td><td></td></tr><tr><td>Firmwareversjon</td><td></td></tr></table> I figuren under vises hendelsesloggen i løsningen. Det indikeres om dette er et varsel eller en teknisk hendelse som logges. I tilfelle varsler vises det hvilken modul (regel) som er kilde til varselet. Videre vises det også hvilket objekt varselet gjelder. Tekniske hendelser kan også varsles hvis det skal reageres på dem umiddelbart. Varsler om tekniske hendelser kan sendes til tjenesteutøver og/eller vedlikeholdspersonell umiddelbart de mottas av systemet. Utilgjengelighet av enheter vil varsles ved uteblitt heartbeat med tider som beskrevet i krav 4.8. Det kan varsles ved vanlig varslingsmekanisme som beskrevet i krav 4.12. Hendelseslogg Fra 2019-03-25 16:43 til 2019-05-29 00:47 Last ned ▼ Vis filter 2019-05-29 00:47 2019-05-29 16:43 <table><tr><th></th><th>Tidspunkt</th><th>Hendelse</th><th>Melding</th><th>Kilde</th><th>Objekt</th><th></th></tr><tr><td></td><td></td><td></td><td>Start</td><td></td><td></td><td></td></tr><tr><td>🕒</td><td>Idag, 22:47:14</td><td>Alarm</td><td>Manglende «Heartbeat»</td><td>🔧 Regel</td><td>👤 Per 68 år</td><td>🔔</td></tr><tr><td>🔧</td><td>Idag, 22:44:21</td><td>sensorFeil</td><td>Sensor utenfor område</td><td>🔧 TnODeviceProfile</td><td>🏠 Gateway</td><td>🔔</td></tr><tr><td>🔧</td><td>Idag, 22:42:48</td><td>lavBatt</td><td>Akkumulator lav</td><td>🔧 TnODeviceProfile</td><td>🏠 Gateway</td><td>🔔</td></tr><tr><td>🔧</td><td>Idag, 22:41:48</td><td>sensorFeil</td><td>Sensor utenfor område</td><td>🔧 TnODeviceProfile</td><td>🏠 Gateway</td><td>🔔</td></tr><tr><td>🔧</td><td>Idag, 22:34:42</td><td>lavBatt</td><td>Akkumulator lav</td><td>🔧 TnODeviceProfile</td><td>🏠 Gateway</td><td>🔔</td></tr><tr><td>🔧</td><td>Idag, 22:28:19</td><td>sensorFeil</td><td>Sensor utenfor område</td><td>🔧 TnODeviceProfile</td><td>🏠 Gateway</td><td>🔔</td></tr><tr><td>🔧</td><td>Idag, 22:28:15</td><td>batteryLow</td><td>Akkumulator lav</td><td>🔧 TnODeviceProfile</td><td>🏠 Gateway</td><td>🔔</td></tr><tr><td>🕒</td><td>Idag, 16:25:24</td><td>Alarm</td><td>Bevegelse Per 68 år</td><td>🔧 Bevegelse orange</td><td>👤 Per 68 år</td><td>🔔</td></tr><tr><td>🕒</td><td>Idag, 16:24:55</td><td>Alarm</td><td>Alarm Seng digitil - Anne 77 år demo Fornebu</td><td>🔧 Axis bevegelse ved seng</td><td>👤 digitil - Anne 77 år demo Fornebu</td><td>🔔</td></tr><tr><td>🕒</td><td>2019-05-27 21:52:28</td><td>Alarm</td><td>Alarm Seng digitil - Anne 77 år demo Fornebu</td><td>🔧 Axis bevegelse ved seng</td><td>👤 digitil - Anne 77 år demo Fornebu</td><td>🔔</td></tr><tr><td>🕒</td><td>2019-05-27 21:50:27</td><td>Alarm</td><td>Alarm Seng digitil - Anne 77 år demo Fornebu</td><td>🔧 Axis bevegelse ved seng</td><td>👤 digitil - Anne 77 år demo Fornebu</td><td>🔔</td></tr></table>	kommuniserer med		ICCID på SIM-kort		Feil i konfigureringen		Mislykket brukeranrop		Signalstyrke 4G/GSM nett		Nettverksinformasjon		Produkttype		Firmwareversjon			Tidspunkt	Hendelse	Melding	Kilde	Objekt					Start				🕒	Idag, 22:47:14	Alarm	Manglende «Heartbeat»	🔧 Regel	👤 Per 68 år	🔔	🔧	Idag, 22:44:21	sensorFeil	Sensor utenfor område	🔧 TnODeviceProfile	🏠 Gateway	🔔	🔧	Idag, 22:42:48	lavBatt	Akkumulator lav	🔧 TnODeviceProfile	🏠 Gateway	🔔	🔧	Idag, 22:41:48	sensorFeil	Sensor utenfor område	🔧 TnODeviceProfile	🏠 Gateway	🔔	🔧	Idag, 22:34:42	lavBatt	Akkumulator lav	🔧 TnODeviceProfile	🏠 Gateway	🔔	🔧	Idag, 22:28:19	sensorFeil	Sensor utenfor område	🔧 TnODeviceProfile	🏠 Gateway	🔔	🔧	Idag, 22:28:15	batteryLow	Akkumulator lav	🔧 TnODeviceProfile	🏠 Gateway	🔔	🕒	Idag, 16:25:24	Alarm	Bevegelse Per 68 år	🔧 Bevegelse orange	👤 Per 68 år	🔔	🕒	Idag, 16:24:55	Alarm	Alarm Seng digitil - Anne 77 år demo Fornebu	🔧 Axis bevegelse ved seng	👤 digitil - Anne 77 år demo Fornebu	🔔	🕒	2019-05-27 21:52:28	Alarm	Alarm Seng digitil - Anne 77 år demo Fornebu	🔧 Axis bevegelse ved seng	👤 digitil - Anne 77 år demo Fornebu	🔔	🕒	2019-05-27 21:50:27	Alarm	Alarm Seng digitil - Anne 77 år demo Fornebu	🔧 Axis bevegelse ved seng	👤 digitil - Anne 77 år demo Fornebu	🔔	
kommuniserer med																																																																																																													
ICCID på SIM-kort																																																																																																													
Feil i konfigureringen																																																																																																													
Mislykket brukeranrop																																																																																																													
Signalstyrke 4G/GSM nett																																																																																																													
Nettverksinformasjon																																																																																																													
Produkttype																																																																																																													
Firmwareversjon																																																																																																													
	Tidspunkt	Hendelse	Melding	Kilde	Objekt																																																																																																								
			Start																																																																																																										
🕒	Idag, 22:47:14	Alarm	Manglende «Heartbeat»	🔧 Regel	👤 Per 68 år	🔔																																																																																																							
🔧	Idag, 22:44:21	sensorFeil	Sensor utenfor område	🔧 TnODeviceProfile	🏠 Gateway	🔔																																																																																																							
🔧	Idag, 22:42:48	lavBatt	Akkumulator lav	🔧 TnODeviceProfile	🏠 Gateway	🔔																																																																																																							
🔧	Idag, 22:41:48	sensorFeil	Sensor utenfor område	🔧 TnODeviceProfile	🏠 Gateway	🔔																																																																																																							
🔧	Idag, 22:34:42	lavBatt	Akkumulator lav	🔧 TnODeviceProfile	🏠 Gateway	🔔																																																																																																							
🔧	Idag, 22:28:19	sensorFeil	Sensor utenfor område	🔧 TnODeviceProfile	🏠 Gateway	🔔																																																																																																							
🔧	Idag, 22:28:15	batteryLow	Akkumulator lav	🔧 TnODeviceProfile	🏠 Gateway	🔔																																																																																																							
🕒	Idag, 16:25:24	Alarm	Bevegelse Per 68 år	🔧 Bevegelse orange	👤 Per 68 år	🔔																																																																																																							
🕒	Idag, 16:24:55	Alarm	Alarm Seng digitil - Anne 77 år demo Fornebu	🔧 Axis bevegelse ved seng	👤 digitil - Anne 77 år demo Fornebu	🔔																																																																																																							
🕒	2019-05-27 21:52:28	Alarm	Alarm Seng digitil - Anne 77 år demo Fornebu	🔧 Axis bevegelse ved seng	👤 digitil - Anne 77 år demo Fornebu	🔔																																																																																																							
🕒	2019-05-27 21:50:27	Alarm	Alarm Seng digitil - Anne 77 år demo Fornebu	🔧 Axis bevegelse ved seng	👤 digitil - Anne 77 år demo Fornebu	🔔																																																																																																							
4.10 (M)	Administrasjonssystemet skal motta varslinger om strømbrudd og nettbrudd. Utformingskrav Leverandøren beskriver hvordan kravet oppfylles.	JA																																																																																																											

chls
Ave



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til applikasjoner og varsler	JA/NEI									
Leverandørens besvarelse: Ved strømbrydd vil gateway sende melding til administrasjonssystemet når ekstern strømforsyning tilkobles og frakobles. Varsling kan da sendes slik som beskrevet i krav 4.9. Ved nettbrudd vil en eller flere av følgende hendelser inntreffe: 1. heartbeats fra enheter uteblir og det varsles om dette slik som beskrevet i krav 4.9. 2. en alarm blir ikke levert via nettforbindelse. Gateway går da over til reserveløsning og gjør oppringning til predefinert(e) telefonnummer(e) 3. Telenor operasjonssentral sender informasjon til kunder om nettproblemer. Denne informasjonen kan også legges inn som driftsmeldinger i administrasjonssystemet											
4.11 (M)	Dersom enheter er batteridrevne, skal administrasjonssystemet motta varslinger om lavt batterinivå på enheter. <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet oppfylles.	JA									
Leverandørens besvarelse: Administrasjonssystemet vil motta informasjon om batteristatus fra enheter hvis batterinivået blir lavt. Videre kan det da sendes et varsel om dette til personell, enten via SMS, e-post eller som en alarm gjennom web-grensesnittet.											
4.12 (E3)	Varslinger bør nå fram raskt/umiddelbart til varselmottaker slik at Helsedirektoratets anbefalinger* til svartid kan overholdes med god margin. <u>Utformingskrav</u> Beskriv hvor raskt varsler når varselmottaker (spesielt utløste alarmer). Varsler som når fram raskere enn 5 sekunder vil telle positivt. <i>*Helsedirektoratet anbefaler at minimum 95 % av alle varsler skal besvares av varselmottaker innen 60 sekunder.</i>	JA									
Leverandørens besvarelse: Løsningen er konfigurert med hensyn på hvordan tjenstemottaker skal bli varslet. Det tilbys varsling via web-grensesnitt, SMS, e-post, mobil push abonnement og automatisk oppringing. I forhold til garantert responstid på varling er automatisk oppringing og varsling i web-grensesnitt som gir en garantert responstid. De andre metodene vil kunne variere avhengig av nettverkstrafikk og lokale innstillinger på terminal. Under er en tabell som oppsummerer typiske responstider ved ulike type varslinger:											
<table><tr><th>Type varsel</th><th>Responstid (sek)</th><th>Forklaring</th></tr><tr><td>Web-grensesnitt</td><td>1-2</td><td>Varsel sendes via web-socket til klient. Krever at klient er pålogget</td></tr><tr><td>SMS</td><td>4-80 (typisk)</td><td>Avhengig av trafikk hos SMS leverandør</td></tr></table>			Type varsel	Responstid (sek)	Forklaring	Web-grensesnitt	1-2	Varsel sendes via web-socket til klient. Krever at klient er pålogget	SMS	4-80 (typisk)	Avhengig av trafikk hos SMS leverandør
Type varsel	Responstid (sek)	Forklaring									
Web-grensesnitt	1-2	Varsel sendes via web-socket til klient. Krever at klient er pålogget									
SMS	4-80 (typisk)	Avhengig av trafikk hos SMS leverandør									

Ohla
Ake



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til applikasjoner og varsler	JA/NEI
e-post	5-160(typisk)	Avhengig av mailserver(e) og lokale innstillinger i mailklient
Mobil push abonnement	2-60(typisk)	Avhengig av dvaletilstand på terminal
Automatisk oppringing	1-2	Sikker responstid
4.13 (E3)	Enhetene bør sende identifiserbare varsler med en beskrivende tekst til varselmottaker, f.eks. ved utløst alarm, teknisk svikt som følge av strømbrudd/nettbrudd, lavt batterinivå (inkl. batterinivå), testing, og eventuelle andre oppdagede funksjonsfeil. <u>Utformingskrav</u> Beskriv i hvilken grad ulike typer varsler er identifiserbare og har en beskrivende tekst for systembruker. Leverandøren viser også hvordan kravet oppfylles gjennom demonstrasjon iht. oppgitte demosituasjoner i Vedlegg 1 Beskrivelse av demonstrasjoner.	JA
Leverandørens besvarelse: Varsler sendes med informasjon som indikerer årsak til varsel og hvem varslet angår. Det er imidlertid viktig at informasjonen ikke er personsensitiv da denne informasjonen vil kunne sendes på kanaler som kan være usikre. Det blir imidlertid lagt ved en lenke som man kan åpne og dermed måtte autentisere for å få tilgang til mer informasjon. Typisk tekst i melding kan være: «Person forlatt seng på rom 12». Man unngår i dette tilfellet å eksponere personsensitiv informasjon samtidig som personell kan reagere raskt på varsel.		
4.14 (E3)	Systemet bør ha god funksjonalitet knyttet til å holde oversikt over og håndtere varsler, samt se sanntidsstatus på både teknisk status og status relatert til tjenestemottaker i systemet. <u>Utformingskrav</u> Beskriv hvordan systemet er lagt til rette for å gi en oversikt over sanntidsstatus på varsler. Dette kan f.eks. være en dashboard-løsning eller lignende som fremstiller varsler/status relatert til både tekniske varsler/status, samt relatert til tjenestemottaker (helsevarsler/utløste alarmer). Beskriv også hvordan Kunden kan ha oversikt over og håndtere varsler/kvittere ut varsler på ulike arbeidsflater. Leverandøren viser også hvordan kravet oppfylles gjennom demonstrasjon iht. oppgitte demosituasjoner i Vedlegg 1 - Beskrivelse av demonstrasjoner.	JA
Leverandørens besvarelse: Løsningen har et alarmmottak hvor alle varsler for tjenestemottakere, både helsevarsler/alarmer og tekniske varsler, vises i sanntid. Dette mottaket har mulighet for illustrasjon med både innendørs og utendørs kart for raskt å kunne se tilhørende lokasjon til varslet.		

alts
are



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til applikasjoner og varsler	JA/NEI
----------	---	--------



Digitalt Tilsyn

Alarmer 

Multivideo

Tjenestemottakere

Tjenesteutøvere

Tilsynslogg

 Knut Eilif Husa
(Oslo Soneenhet 1 Digital Demo)

Prioritet	Tjenestemottaker	Når	Status
 Fallvarsel	Tor	29.08.2019	Aktiv
 Ut av seng varsel	Tor	29.08.2019	Aktiv
 Ut av seng varsel	Tor	29.08.2019	Kvittert av: Knut Eilif Husa
 Ut av seng varsel	Tor	29.08.2019	Kvittert av: Knut Eilif Husa
 Ut av seng varsel	Tor	29.08.2019	Kvittert av: Knut Eilif Husa
 Ut av seng varsel	Tor	29.08.2019	Kvittert av: Knut Eilif Husa
 Ut av seng varsel	Tor	29.08.2019	Kvittert av: Knut Eilif Husa

Kvittering av varsel skjer ved å velge aktuelt varsel og deretter kvittere varslet med kommentarer.

Ved stort volum av varsler er det mulig å sette på filtre i løsningen slik at man bare ser varsler knyttet til en spesifikk tjenestemottaker, eller bare varsler av en spesifikk type, f.eks. kun se tekniske varsler.

Chlo
HKE



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til applikasjoner og varsler	JA/NEI
Man kan også filtrere slik at man bare ser aktive alarmer. Visning av varsler er tilgjengelig både fra pc/stasjonær datamaskin, og mobile enheter som nettbrett eller mobiltelefon. Visning av varsler på ulike arbeidsflater er beskrevet i krav 4.2.		
4.15 (E3)	Det bør kunne defineres varselmottaker for henholdsvis tekniske varsler og helsevarsler (direkte relatert til tjenestemottakere). <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet oppfylles. Leverandøren viser også hvordan kravet oppfylles gjennom demonstrasjon iht. oppgitte demosituasjoner i Vedlegg 1 Beskrivelse av demonstrasjoner.	JA
Leverandørens besvarelse: Varsel ved tekniske hendelser kan rutes til andre varselmottakere enn mottakere av helsevarslene. Ruting av tekniske varsler settes typisk opp i enhetsprofiler som lytter på all informasjon som sendes fra enhetene. Se krav 4.7.		
Administrering av systembrukere og tjenestemottakere		
4.16 (M)	En systembruker skal kun kunne registreres én gang (unik bruker). <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet blir ivaretatt.	JA
Leverandørens besvarelse: Systembrukerens identifikator (enten dette er kommunal identitet, fnr, e-postadresse eller annet) er unik innenfor en konto/tjeneste. Enkelte kommuner velger å benytte flere kontoer for å organisere sin Digitalt tilsyn tjeneste. Samme brukeridentifikator kan derfor benyttes i flere kontoer/tjenester. Vi tror dette er sannsynlig konfigurasjon også for Oslo kommune, se videre besvarelse i kap. 4. Shepherd tjeneste og integrasjonsplattform er en fler-konto plattform som leverer en rekke tjenester i tillegg til Digitalt tilsyn, f.eks. medisinsk avstandsoppfølging mm. Samme brukeridentifikator kan derfor benyttes i flere kontoer/tjenester.		
4.17 (M)	En tjenestemottaker skal kun kunne registreres én gang, og har 11-sifret p.nr eller D-nr som identifikator. <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet blir ivaretatt.	JA

okt
Ake



Oslo kommune
Helseetaten

Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til applikasjoner og varsler	JA/NEI
Leverandørens besvarelse: Telenors Digitalt tilsyn tjeneste kan benyttes som en pseudonymisert eller personidentifiserende tjeneste. Enhetene kan også være koblet til lokasjon (adresse/rom) ikke person. Dersom kommunen velger å benytte fnr/dnr som identifikator, registreres dette som «ekstern identifikator», denne må være unik og kan kun registreres en gang per konto/tjeneste. Som kommentert til krav 4.16 så er Shepherd tjeneste og integrasjonsplattform er en fler-konto plattform som leverer en rekke tjenester i tillegg til Digitalt tilsyn, f.eks. medisinsk avstandsoppfølging mm. Samme eksterne identifikator fnr/dnr kan derfor benyttes i flere kontoer/tjenester i parallell.		
4.18* (M)	Systembrukere skal kunne inaktiveres og aktiveres igjen. <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet blir ivaretatt.	JA
Leverandørens besvarelse: I administrasjonssystemet for Shepherd kan administrator deaktivere og aktivere en systembrukers tilgang til en konto. En brukerkonto som er deaktivert vil ikke kunne brukes for å aksessere Digitalt tilsyn for kundekontoen, og vil ikke ha tilgang til pasientdata i kontoen. En brukerkonto som blir aktivert vil ha samme tilganger som den hadde før den ble deaktivert.		
4.19 (M)	Tjenestemottakere skal kunne inaktiveres og aktiveres igjen. <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet blir ivaretatt.	JA
Leverandørens besvarelse: I grensesnittet for Telenor Digitalt tilsyn kan administrator deaktivere en tjenestemottaker på detaljsiden for tjenestemottakeren. For en deaktivert tjenestemottaker vil tilknyttede enheter bli deaktivert, og det vil ikke lenger være mulig å benytte kameraet for den deaktiverte tjenestemottakeren. Det vil heller ikke bli generert varsler for tjenestemottakeren. Når en tjenestemottaker blir aktivert, vil tilknyttede enheter også bli aktivert, varsler vil kunne bli generert, og alle innstillinger vil være de samme som før tjenestemottakeren ble deaktivert.		

delg
ACE



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til applikasjoner og varsler	JA/NEI
4.20* (M)	Løsningen skal forenkle administrasjon og vedlikehold i løsningen ved å gruppere både systembrukere, tjenestemottakere og andre brukere av løsningen i soner. Administrasjon og vedlikehold kan dermed også gjøres gruppevis, og ikke kun enkeltvis på tjenestemottakere eller systembrukere. Løsningen tilbyr hierarkisk soneinndeling som støtter at: • Systembrukere og tjenestemottakere kan grupperes i soner • Det kan opprettes ubegrenset antall nivåer av soner med undersoner • Systembruker og tjenestemottaker kan tilordnes et hvilket som helst nivå i sonehierarkiet (Se «SSA-K_Bilag 1 - Vedlegg 3 - Spesifikasjon rollebasert tilgangskontroll») <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet blir ivaretatt.	JA
Leverandørens besvarelse: Hierarkisk soneinndeling realiseres igjennom kontoer og grupper. Basert på Telenors nåværende forståelse av Oslo kommunes behov og bruksscenarier er vår antagelse at Oslo kommune er mest tjent med å organisere tjenesten med en konto per soneenhet, dette beskrives også under krav 4.22. En soneenhet som skal driftes og administreres uavhengig av andre soneenheter bør etableres som egen konto. Inn under en soneenhet brukes "grupper". I løsningen brukes den generiske termen «grupper», som kan representere enten geografiske soner eller annen gruppering, f.eks. etter diagnose eller andre kriterier. Det kan opprettes et ubegrenset antall grupper for å representere et hierarki. • Systembrukere kan legges til grupper. En systembruker kan legges til et ubegrenset antall grupper/nivåer. • Tjenestemottakere kan legges til grupper. En tjenestemottaker kan legges til et ubegrenset antall grupper/nivåer. • Systembrukere får kun tilgang til de tjenestemottakere som er lagt til de grupper som systembruker er medlem i.		
4.21 (E1)	Tilbudt(e) løsning(er) bør ha mulighet for å gruppere tjenestemottakere (utover gruppering i soner), slik at det kan settes opp standardoppsett for en gruppe tjenestemottakere. Dette kan f.eks. være relevant dersom man ønsker å deaktivere en spesifikk funksjon for en gitt gruppe tjenestemottakere, eller at det ønskes å endre varselmottakere for en gruppe i en gitt periode. <u>Utformingskrav</u> Leverandøren beskriver hvordan tjenestemottakere kan grupperes, og hvilke innstillinger/tilpasninger som kan gjøres på gruppenivå for tjenestemottakere.	JA

Ans
Ans



Oslo kommune
Helseetaten

Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til applikasjoner og varsler	JA/NEI
Leverandørens besvarelse: I løsningen brukes den generiske termen «grupper», som kan representere enten geografiske soner eller annen gruppering, f.eks. etter diagnose eller andre kriterier. Det kan opprettes et ubegrenset antall grupper. Mottak av varsler styres av tilgangsstyringsmekanismene og av dataabonnement. Dersom varsler for en spesifikk gruppe tjenestemottakere skal rutes til andre mottakere enn øvrige tjenestemottakere vil det være naturlig å ta disse tjenestemottakerne ut av gruppen de tidligere har vært medlem i, og tilordne de til en ny gruppe, f.eks. for en spesifikk lokasjon som en omsorgsbolig e.l. Det vil da kun være systembrukere som får tilgang til denne nye gruppen som mottar varsler for de aktuelle tjenestemottakere. Ved varsling til eksterne alarmsystem vil det være enten tilgangsrettighetene til alarmsystemets systembruker og/eller dataabonnementets konfigurasjon som avgjør ruting av alarmvarsler. Et dataabonnement kan f.eks. konfigureres til kun å abonnere på varsler for en spesifikk gruppe, eller unntatt en spesifikk gruppe, selv om systembrukeren har tilgangsrettigheter til å lese alarmer for de aktuelle tjenestemottakere. For gateway gjøres innstillinger på gruppenivå ved å etablere en gruppespesifikk mal som anvendes på alle gatewayer/sensorer for gruppen. Alle innstillinger på gateway kan settes igjennom malen. Telenor har hittil ikke hatt forespørsler om å gjøre innstillinger på gruppenivå for konfigurasjon av digitalt tilsyn kameraer. Kundene har bevisst ønsket å konfigurere disse individuelt mtp tilsynsvindu etc. Dersom Oslo kommune har konkrete innstillinger/funksjoner man ønsker å kunne sette på gruppenivå vil Telenor ta dette inn i veikart/produktkø for videreutvikling. Se også svar på krav 4.20.		
4.22* (M)	Løsningen skal sikre at en soneenhet (eksempelvis en bydel) kan administrere sine egne ansatte og tjenestemottakere, uten innsyn i andres soner. <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet blir ivarettatt.	JA
Leverandørens besvarelse: Basert på Telenors nåværende forståelse av Oslo kommunes behov og bruksscenarier er vår antagelse at Oslo kommune er mest tjent med å organisere tjenesten med en konto per soneenhet. Overordnet organisering i ulike kontoer vil være det viktigste tiltaket for å sikre mot innsyn i andre enheters soner. For hjemmeboende antar vi det vil være bydel, for institusjoner antar vi det vil være per institusjon. Telenor har allerede en rekke kunder på tjenesten Digitalt tilsyn som har organisert sin bruk på denne måten. Innenfor hver soneenhet/konto vil administrator for soneenheten/kontoen forvalte aktuell gruppestruktur for tilgangsstyring iht hvordan enheten er organisert.		

aks
AKC



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til applikasjoner og varsler	JA/NEI
4.23 (M)	Løsningen skal ivareta at alle systembrukere tildeles minimum én rolle i løsningen ved opprettelse (eksempler på typiske roller kan være: administrator, operatør, pårørende). Rollen avgjør hva systembruker kan endre og se i løsningen (hvilke tilganger og rettigheter systembruker har). Rollestyringen skal forenkle administrasjon og sikre at person- og helseopplysninger kun presenteres for autorisert personell med tjenstlig behov. (Se «SSA-K_Bilag 1 - Vedlegg 3 - Spesifikasjon rollebasert tilgangskontroll») <u>Utformingskrav</u> Leverandøren beskriver hvordan det er sikret at alle systembrukere tildeles minimum én rolle i løsningen ved opprettelse.	JA
Leverandørens besvarelse: Når systembruker opprettes i Digitalt tilsyn applikasjonen må det angis applikasjonsrolle, som igjen styrer hvilken funksjonalitet systembrukeren får tilgang til i løsningen. Eksempler på roller er: Administrator – kan administrere systembrukere, administrere grupper, administrere tjenstemottakere, aktivere/inaktivere tjenstemottakere mv. Tjenesteansvarlig – kan administrere tjenstemottakere, gjennomføre tilsyn mv, men kan ikke opprette systembrukere eller gi systembrukere tilgang til grupper. Tjenesteutøver – kan motta, se og lukke varsler, gjennomføre tilsyn og se hendelseslogg Tekniker – kan konfigurere kamera og motta, se og lukke varsler, men kan ikke opprette eller slette tjenstemottaker eller gjøre endringer på tjenstemottakers konfigurasjoner grupper. Pårørende (kan være familie, venn, frivillig, nabo etc) - kan motta, men ikke kvittere, varsler, samt gjennomføre tilsyn via kamera og se hendelseslogg. Dersom kommunen tilbyr pårørende appen Tryggi kan også varsler mottas her.		
4.24	Systembrukers rettigheter skal administreres i en rollemal og ikke for den enkelte systembruker. En rollemal beskriver hvilke tilganger de som opptrer i rollen skal ha og hvilke kategorier av informasjon de som innehar rollen normalt skal gis tilgang til når det ytes helsehjelp. <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet blir ivaretatt.	JA

Åke
Chh



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til applikasjoner og varsler	JA/NEI
Leverandørens besvarelse: Digitalt tilsyn applikasjonsroller er spesifikt definert for denne tjenesten basert på Shepherd tjeneste- og integrasjonsplattform generelle rollemodell. For hver av applikasjonsrollene i Digitalt tilsyn, eksemplifisert i svar til krav 4.23, har Telenor gjort en vurdering av aktuelle tilgangsrettigheter for rollen, og valgt inn/ut detaljerte brukerrettigheter til denne rollen ut i fra den generelle underliggende rettighetsmodell. Dette har flere fordeler: • Alle funksjoner i løsningen tilbys også igjennom åpne veldokumenterte API og API'ene benytter samme detaljerte rolle og tilgangsmodell som applikasjonen. • Det er svært enkelt og medfører lav risiko å definere tilgangsrettigheter til nye applikasjonsroller ved videreutvikling. • Det er svært enkelt og medfører lav risiko i å legge til nye funksjoner i tjenesten og tilordne tilganger til disse til eksisterende roller. • Det er svært enkelt å legge til/trekke fra tilgangsrettigheter for en rolle, dersom det skulle være behov for dette.		
4.25* (M)	Det skal være mulig å opprette flere roller/rollemaler i systemet enn de som er standard. <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet blir ivaretatt.	JA
Leverandørens besvarelse: Shepherd tjeneste- og integrasjonsplattform har en svært detaljert underliggende tilgangsmodell. Ut i fra denne tilgangsmodellen konfigureres aktuelle applikasjonsroller som gir tilgang til ulik grad av funksjonalitet i applikasjonen og via API. Nye applikasjonsroller/rollemaler kan enkelt opprettes ved å definere et navn og krysse av for hvilke detaljerte tilgangsrettigheter rollen skal gi. For tilgang via API vil nye systembrukere med denne applikasjonsrollen umiddelbart være operasjonelle. For tilgang via applikasjonen forutsetter Telenor at nye applikasjonsroller ikke introduseres utenfor en kontrollert endringsprosess, da endring av tilgangsrettigheter som regel bør verifiseres og tilpasses i applikasjonen med tanke på visning/skjuling av brukergrensesnittelementer og andre aspekter som påvirker løsningens brukskvalitet. Se også svar til krav 4.24		
4.26* (M)	En systembruker skal kunne ha flere roller, men kun være aktiv i én rolle av gangen. Systembruker skal kunne bytte mellom roller basert på hvilke oppgaver som skal utføres. Bytte mellom roller kan f.eks. gjøres ved pålogging eller i egen funksjon for å skifte rolle. <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet blir ivaretatt.	JA

AKO
24/6



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til applikasjoner og varsler	JA/NEI
Leverandørens besvarelse: I dagens løsning støtter systemet at en systembruker kan ha én rolle per konto. En systembruker kan ha forskjellige roller og tilganger i forskjellige kontoer. I en fremtidig versjon av Telenor Digitalt tilsyn som skal være klar før 1. oktober 2019, vil systembrukere kunne ha flere roller innenfor samme konto. Det vil fortsatt være slik at systembruker alltid jobber med én aktiv rolle, og systembrukers tilganger vil være styrt av den aktive rollen. Bytte av aktiv rolle kan gjøre av systembruker med en funksjon for å skifte rolle, og systemet vil huske sist anvendte rolle ved neste innlogging.		
4.27* (M)	En systembruker skal kunne knyttes til en eller flere soner/organisatoriske enheter. Systembruker skal kunne ha ulike roller i ulike soner. (Noen ansatte jobber f.eks. i flere bydeler og har ulike roller i de ulike bydelene). <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet blir ivarettatt.	JA
Leverandørens besvarelse: Som beskrevet i svar til krav 4.22 er Telenors antagelse, basert på Telenors nåværende forståelse av Oslo kommunes behov og bruksscenarier, at Oslo kommune er mest tjent med å organisere tjenesten med en konto per soneenhet. Det opprettes da en systembruker per soneenhet/konto, med samme eksterne identifikator for alle systembrukerne. Hver av systembrukerne for den aktuelle ansatte administreres i en konto, uavhengig av de andre kontoene. En ansatt kan således ha rolle som Administrator med tilhørende tilgangsrettigheter i en soneenhet/konto, men ha rolle som Operatør med andre tilgangsrettigheter i en annen soneenhet/konto. Som beskrevet i svar til krav 4.26 vil tjenesten utvides slik at systembruker kan ha flere ulike roller innenfor samme konto/soneenhet. Systembruker kan da ha en rolle, administrator, i en del av en soneenhet, og en annen rolle i en annen del av en soneenhet, for eksempel operatør.		
4.28* (E3)	Løsningen bør tilby ulike roller med tilhørende muligheter og begrensninger knyttet til hva systembruker kan endre og/eller se (f.eks. rettigheter/tilganger knyttet til sikkerhetsinnstillinger, sikkerhetstilganger og tilganger til funksjonalitet). <u>Utformingskrav</u> Beskriv løsningens ulike roller og hvilke funksjonelle muligheter/begrensninger som kan legges i disse. Beskriv f.eks. i hvilken grad ansatte med en gitt rolletilgang kan endre innstillinger, aktivere/deaktivere enheter/funksjoner, styre varslingskjeder, stille inn tidsintervaller og gjøre andre individuelle tilpasninger per tjenestemottaker.	JA

Wise
CMA



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til applikasjoner og varsler	JA/NEI
----------	---	--------

Leverandørens besvarelse:

Tabellen nedenfor viser overordnet roller med tilhørende tilgangsrettigheter. Rollene merket med NY er roller under etablering som del av videreutvikling og vil være etablert til oppstart av tjenesten for Oslo kommune. Kryss indikerer at rollen har tilgang til funksjonen dersom den er aktuell/konfigurert i bruk for den aktuelle tjenestemottaker/systembruker.

ROLLEBESKRIVELSE DIGITALT TILSYN

	Opprette tjenestemottakere	Endre tjenestemottakere	Slette tjenestemottakere	Se video/bilde	Motta varsler	Se varsler	Kvittere varsler	Se hendelseslogg	Opprette systembruker	Endre systembruker	Slette systembruker	Endre passord*	Blokkere tilgang	IP filter	Tofaktor autentisering	Konfigurere gateway og sensorer
Administrator	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
NY Tjenesteansvarlig	X	X	X	X	X	X	X	X					X	X	X	X
Tjenesteutøver				X	X	X	X	X						X	X	
NY Tekniker				X	X	X	X	X						X	X	X
NY Pårørende				X	X	X		X							X	

* gjelder andre brukeres passord. Alle kan endre eget passord

Kommentarer til funksjoner:

- Endre tjenestemottaker - gruppetilhørighet, tidsvinduer mv.
- Motta varsler – opprette abonnement og motta varsler på de tilgjengelige kanaler som, mobil pushmelding eller e-post.
- Se varsler - se varsler i mobil- eller webapplikasjon.
- Endre passord - gjelder andre brukeres passord. Alle kan endre eget passord.
- Blokkere tilgang – blokkere gjeldende brukersesjon for eksempel ved mistet mobiltelefon e.l.

Kommentarer til roller

- Tekniker kan utføre en rekke funksjoner kun med tilgang til kamera, uten tilgang til personopplysninger om tjenestemottaker.
- Pårørende autentiseres vha ID-porten, endre passord og IP-filter er ikke aktuelt.

4.29 (E2)	Løsningen bør tilby mulighet for å hente ut tekniske rapporter og teknisk informasjon. <u>Utformingskrav</u> Beskriv hvilke tekniske rapporter/informasjon som kan hentes i løsningen. Dette kan f.eks. være informasjon om:	JA
-----------	--	----

alla
sra



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til applikasjoner og varsler	JA/NEI
	• Programvareversjon /release notes • Rapport over enheter med ulike statuskategorier (f.eks. aktive/inaktive/testenheter/annet) • Rapport på enheter som har, eller får dårligere dekning over tid Beskriv også om systembruker med riktig rolle hos Kunden selv kan hente ut denne informasjonen eller ikke.	
Leverandørens besvarelse: Løsningen gir kundens eget personell mulighet for å hente ut en rekke rapporter i samme webapplikasjon/brukergrensesnitt som for konfigurasjon og drift av tjenesten. Noen eksempler • Enheter: rapporter basert på type, modell, i bruk/ikke, siste livstegn etc. • Tjenestemottakere: rapporter basert på grupper/soner, med/uten enheter etc. • Systembrukere: rapporter basert på roller, grupper/soner Innholdet i rapportene fremvises i webapplikasjonen, eller kan lastes ned som kommaseparerte filer (.csv) for videre bearbeiding i andre verktøy. Alle funksjoner og all informasjon i løsningen er tilgjengelig via et veldokumentert API. Telenor vil bistå kunden med veiledning til implementasjon av uttrekk til rapporter osv. Som beskrevet i svar til krav 4.25 kan det opprettes nye applikasjonsroller for å gi ekstern rapportløsning tilgang kun til akkurat den funksjonalitet som er nødvendig for å hente ut data til rapporter.		
4.30 (E1)	Løsningen bør være et «lærende» system (elementer av AI/kunstig intelligens) og bør over tid kunne registrere og lære av historikk og sanntidsdata, for videre å kunne varsle/forutsi endringer fra en individuell normal/mønster. <u>Utformingskrav</u> Beskriv i hvilken grad løsningen har AI-elementer, eller om Leverandøren har planer knyttet til dette.	JA
Leverandørens besvarelse: Løsningen inneholder elementer av AI/lærende systemer. Vår partner og underleverandør Axis Communications har en omfattende satsning på bruk av AI/maskinlæring i videodeteksjonsalgoritmene. I løpet av 2019 vil vi lansere en løsning som ved hjelp av deteksjonsalgoritmer, nevrale nettverk og maskinlæring gjenkjenner avanserte hendelser i bildet som det deretter varsles om. Eksempelvis kan deteksjonsalgoritmen «gjenkjenne» personer i et videobilde og deretter klassifisere hvilken positur personen har, se figur. Algoritmen trenes da opp til å gjenkjenne elementer i bildet som deretter klassifiseres som personer med gitte positurer. I figuren indikerer rødt «skjelett» fall mens grønt indikerer stående og gult sittende. Slike indikasjoner kan brukes til å varsle/forutsi endringer som fall, reise seg opp fra stol etc. Maskinlæringsalgoritmer kan også utvikles for å oppdage risiko for fall eksempelvis gjennom monitorering av bevegelsesmønster (ustø gange osv) samt monitorering av endring i		

uke
elms



Oslo kommune
Helseetaten

Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til applikasjoner og varsler	JA/NEI
	bevegelsesmønster over tid som kan tyde på økt risiko for fall (endring i hastighet på gange, skrittlengde osv). Tolkningen kan deretter benyttes til å utløse varsler. 	

Tabell 4 – Krav til applikasjoner og varsler



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

• **Eksterne rettslige krav**

Følgende eksterne rettslige krav skal besvares for alle delkonkurranser.

Krav-nr.	Leverandørens løsningsbeskrivelse – Eksterne rettslige krav	JA/NEI
5.1 (M)	Leverandøren skal etterleve de regulatoriske kravene for personvern og informasjonssikkerhet (som listet opp under), samt kravene til Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenester. <u>Sikkerhetsmessige rammebetingelser</u> Kunden skal gjennom SSA-K med bilag og databehandleravtalen sikre at Leverandøren ivaretar relevante krav som stilles til Kunden med hjemmel i lov og forskrift, samt nasjonale standarder i forhold til informasjonssikkerhet og personvern. Leverandørens plikter omfatter oppfyllelse av disse kravene slik de fremkommer til enhver tid. Kravene gjelder både for Leverandøren selv og for alle underleverandører som inngår i leveranse av avtalte IKT-tjenester til Kunden. De særskilte kravene er (listen er ikke uttømmende): <u>Regulatoriske krav:</u> 1. <u>Lov om behandling av personopplysninger (personopplysningsloven)</u> 2. <u>Forskrift om behandling av personopplysninger (personopplysningsforskriften)</u> 3. <u>Lov om behandling av helseopplysninger ved ytelse av helsehjelp (pasientjournalloven)</u> 4. <u>Lov om helseregistre og behandling av helseopplysninger (helseregisterloven)</u> 5. <u>Lov om kommunale helse- og omsorgstjenester m.m. (helse- og omsorgstjenesteloven)</u> 6. <u>Lov om helsepersonell mv. (helsepersonelloven)</u> 7. <u>Lov om pasient – og brukerrettigheter (pasient- og brukerrettighetsloven)</u> <u>Nasjonale standarder</u> a) <u>Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten</u> <u>Utformingskrav:</u> Leverandøren skriver «lest og akseptert».	JA
Leverandørens besvarelse: Lest og akseptert		

Tabell 5 – Eksterne rettslige krav

Arve
Puh



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

• **Krav til informasjonssikkerhet**

Følgende krav til informasjonssikkerhet skal besvares for alle delkonkurranser.

Krav markert med: Dersom dette ikke er på plass pr. d.d., skal Leverandøren dokumentere konkrete planer og tilnærming for at dette er på plass innen teststart. (Med «på plass» menes at løsningen er ferdig utviklet og testet av Leverandør.)*

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til informasjonssikkerhet	JA/NEI
Generelle krav til informasjonssikkerhet		
6.1 (M)	Samtidig med kontraktsignering skal det inngås en databehandleravtale (se bilag 12). Kravene til personvern og informasjonssikkerhet i denne skal ivaretas og Leverandøren plikter å behandle all informasjon i henhold til databehandleravtalen og Behandlingsansvarliges sikkerhetsprinsipper. Resultat fra gjennomført risikovurdering skal fremlegges av databehandler som dokumentasjon av egen og eventuelle underleverandørers sikkerhet. Kundens Akseptansetest vil innebefatte en sikkerhetsgjennomgang av Leverandøren. <u>Utformingskrav</u> Leverandøren skriver «Lest og akseptert».	JA
Leverandørens besvarelse: Lest og akseptert		
6.2 (E1)	Leverandøren bør vedlegge sine sikkerhetsmål, sikkerhetsstrategi og oversikt over hvem som har ansvar for informasjonssikkerheten. <u>Utformingskrav</u> Leverandøren legger ved dokumentasjon på sikkerhetsmål, sikkerhetsstrategi og ansvar for informasjonssikkerheten.	JA
Leverandørens besvarelse: Hovedpunkter innenfor begrensningen av 500 ord er gjengitt nedenfor. Et uttrekk av Sikkerhetshåndbok for Telenor Norge e-helse er lagt ved som vedlegg.		
<u>Sikkerhetsmål</u>		
Overordnede sikkerhetsmål Telenor Norge e-helse har pasientsikkerhet og IKT-sikkerhet som vår høyeste prioritet og vårt sikkerhetsarbeid skal sikre at		
• kundenes pasienter og tjenestemottakere mottar forsvarlig helsehjelp • kundenes plikter som dataansvarlige og Telenors plikter databehandler er ivaretatt på beste måte • Telenor opptretr som ansvarlig samfunnsaktør		
Sikkerhetsmål om forsvarlige helsehjelp Telenor Norge e-helse skal igjennom systematisk forebyggende sikkerhetsarbeid, velorganisert drift,		

AKG
ma



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til informasjonssikkerhet	JA/NEI
	samt læring og forbedring etter uønskede hendelser sikre at • våre tjenester oppfyller relevante lovkrav, samt anerkjente faglige anbefalinger fra offentlige myndigheter eller andre autoriteter. • vi besitter tilstrekkelig bemanning med riktig tverrfaglig sammensatt kompetanse og riktig opplæring til å yte forsvarlig helsehjelp og til å utvikle, drifte og levere e-helseløsninger, støtteverktøy, installasjonstjenester og helsefaglige tjenester som understøtter kundens forutsetninger for å gi forsvarlig helsehjelp. • vi holder en høy etisk standard og yter tjenester med konsekvent kvalitet - behandle hver episode individuelt og uhildet av og levere samme kvalitet på samme tjeneste, uavhengig av kunde. Sikkerhetsmål om forsvarlig IKT Telenor Norge e-helse skal igjennom systematisk forebyggende sikkerhetsarbeid, velorganisert drift, samt læring og forbedring etter uønskede hendelser, sikre tilstrekkelig • konfidensialitet og integritet om person-, tjeneste- og kundeopplysninger. • integritet på person-, tjeneste- og kundeopplysninger, herunder alle konfigurasjoner og variasjoner i tjenesteoppsettet kunde for kunde. • tilgjengelighet på opplysninger og tjenester, nødvendig for å yte forsvarlig helsehjelp og møte inngåtte kundeforpliktelser. Sikkerhetsstrategi Sikkerhetsstrategien beskriver hvordan sikkerhetsmål skal nås og gjelder for alle tjenester som leveres av Telenor Norge e-helse. Strategien omfatter både den organisatoriske enheten «e-helse», forholdet til omkringliggende funksjoner og tjenester i og fra Telenor Norge, og underleverandører og partnere. Vi skal • forvalte et områdespesifikt praktisk orientert styringssystem i form av en sikkerhetshåndbok inn under rammene gitt av Telenor Norges overordnende styringssystem • forvalte en oppdatert risikovurdering per tjeneste som skal være driver for risikobasert forbedring • ha en tydelig organisering med godt definerte roller og tilhørende ansvar, bemanning og kompetanse til å fylle alle roller • ha et kollektivt ansvar for å tilby forsvarlige tjenester • erkjenne at uønskede hendelser vil kunne inntreffe, men benytte alle uønskede hendelser som kilde for ny læring og forbedring • benytte Telenor Norges sikkerhetskompetanse og standardiserte sikkerhetsprodukter og -tjenester der dette er hensiktsmessig • velge underleverandører og partnere med god sikkerhetspraksis, fortrinnsvis virksomheter med styringssystem for informasjonssikkerhet sertifisert iht ISO 27001 av anerkjent sertifiseringsinstans. Organisering av sikkerhetsarbeidet Under vises en overordnet illustrasjon av Telenor Norge e-helse sikkerhetsorganisasjon. Enkelte	

Alle
ant



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til informasjonssikkerhet	JA/NEI
	funksjoner utføres utenfor e-helse enheten. <pre>graph TD TN[Telenor Norge] --> LS[Leder Security / Sikkerhetsdirektør] TN --> HR[HR] TN --> LB[Leder Bedrift] LS --> SR[Security & Risk] LS --> PO[Privacy Office] LS --> PVB[Personvernbud] HR --> PK[Personvernskoordinator] LB --> SJ[Sikkerhetsjef] SJ --> LSD[Leder Smart Digitale] LSD --> LTH[Leder Telenor e-helse] LTH --> SKTH[Sikkerhetskontakt e-helse] SKTH --> PJ[Produktjef] SKTH --> LE[Leveranseleder] SKTH --> PLUP[Prosjektleder Utviklingsprosjekt] PJ --> PVL[Programvare-leverandører] PJ --> PUL[Utstyr-leverandører] PJ --> PTL[Tjeneste-leverandører] LE --> SA[Systemansvarlig] LE --> DS[Drift og Support] LE --> PLL[Prosjektleder Leveransprosjekt] SA --> PVL2[Programvare-leverandører] SA --> DCL[Datacenter-leverandører] SA --> UUL[Utstyr-leverandører] DS --> TLL[Tjeneste-leverandører] PLL --> SA2[Sikkerhetsarkitekt] PLUP --> SA2</pre> Telenor Norge E-helse forholder seg i tillegg som intern kunde til følgende tjenester/funksjoner i Telenor Norge, uten at de er illustrert som del av sikkerhetsorganisasjonen: • Telenor M2M mobilkommunikasjon tale/data • Telenor Internett / Nordic Connect datakommunikasjon • Telenor IP-telefoni talekommunikasjon for Responsplattform • Telenor Security Operations Center overvåkning nett og infrastruktur • Telenor Bedrift Storkunde Feilmottak overvåkning applikasjoner	
6.3 (M)	Leverandøren skal ikke benytte underleverandører i forbindelse med løsningen uten at det er skriftlig avtalt med Behandlingsansvarlig. <u>Utformingskrav</u> Leverandøren skriver «Lest og akseptert».	JA
Leverandørens besvarelse: Lest og akseptert		

AKC
CML



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til informasjonssikkerhet	JA/NEI
6.4 (M)	Leverandøren skal sikre at informasjon som behandles på vegne av Behandlingsansvarlig holdes adskilt fra egne og andre virksomheters informasjon og tjenester. <u>Utformingskrav</u> Leverandøren skriver «Lest og akseptert».	JA
Leverandørens besvarelse: Lest og akseptert		
6.5* (M)	Leverandøren plikter å dokumentere sitt system for behandling av helse- og personopplysninger i forbindelse med databehandleravtalen. Med dokumentasjon menes bl.a. beskrivelse av prosedyrer for autorisasjon, autentisering og bruk, samt tekniske og organisatoriske sikkerhetstiltak. Dokumentasjonen skal være tilgjengelig for Behandlingsansvarlig, Datatilsynet og Helsetilsynet. <u>Utformingskrav</u> Leverandøren skriver «Lest og akseptert».	JA
Leverandørens besvarelse: Lest og akseptert		
Autorisering		
6.6 (M)	Tilgangsstyring skal etableres for alt utstyr, jf. Normen kapittel 5.2 Tilgangsstyring. <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet oppfylles.	JA
Leverandørens besvarelse: Det er ulike kategorier utstyr som er relevant for denne leveransen. Besvarelse per hovedkategori iht overordnet arkitekturfigur beskrevet i krav 2.11 følger nedenfor: Brukernært utstyr: Kamera, gateway og sensorer - Ja, tilgangsstyring er etablert i kamera, gateway og sensorer. Det lagres ingen personopplysninger i brukernært utstyr. Viktigste verdier å beskytte mot trusler er konfigurasjoner og kommunikasjon. Axis kamera har interne tilgangsstyringsmekanismer og validerer sikkerhetsbillett (token) ved all eksternt initiert kommunikasjon. Gateway kan ikke aksesserer digitalt fra utsiden via mobilnettet eller fast bredbånd, enheten initierer selv all kommunikasjon mot administrasjonsløsning og/eller alarmløsning. Brukernært infrastruktur: nettverkskomponenter i tjenestemottakers hjem eller på institusjon - Ja, tilgangsstyring er etablert i gateway. Tjenesten forutsetter ingen personopplysninger i nettverkskomponenter. Tilgangsstyring skal primært bidra til å sikre konfigurasjon og tilgjengelighet på Wifi router, POE switch etc. avhengig av installasjon. Brukernær		

Free
Cmb



Oslo kommune
Helseetaten

Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til informasjonssikkerhet	JA/NEI
	infrastruktur på institusjon vil i denne leveransen være kundens ansvar, mens i tjenestemottaker utgjør gateway infrastrukturen, ref. pkt over. Delte videoprosesserings- og utstyrskonfigurasjonsplattformer • Ja, tilgangsstyring er etablert i videoprosessering- og utstyrskonfigurasjonstjenesten. Det lagres ingen personopplysninger i videoprosessering- og utstyrskonfigurasjonstjenesten. Tjenesten er en delt tjeneste under utstyrsleverandørens forvaltningsansvar. AXIS Communications har et ISO27001 sertifisert styringssystem for informasjonssikkerhet som omfatter bl.a. forvaltning av tilgangsstyring til infrastruktur. • Ja, tilgangsstyring er etablert i konfigurasjonstjenesten for gateway. Det lagres få/ingen personopplysninger i konfigurasjonstjenesten for gateway, kun evt angivelse av installasjonssted. Tjenesten er en delt tjeneste under utstyrsleverandørens forvaltningsansvar. Neat Electronics har et ISO27001 sertifisert styringssystem for informasjonssikkerhet som omfatter bl.a. forvaltning av tilgangsstyring til infrastruktur. Shepherd tjeneste- og integrasjonsplattform • Ja, tilgangsstyring er etablert i konfigurasjonstjenesten for Shepherd. Tjenesten er en delt tjeneste under integrasjonsleverandørens forvaltningsansvar. Tellu IOT AS har et ISO27001 sertifisert styringssystem for informasjonssikkerhet som omfatter bl.a. forvaltning av tilgangsstyring til infrastruktur. Infrastrukturen er plassert i datasenter i Norge, hos RedpillLinpro, som utøver daglig tilgangsstyring til utstyr iht veletablerte og fungerende forvaltningsrutiner. Det etableres intet nytt spesifikt utstyr for Oslo kommune som del av denne avtalen.	
6.7 (M)	All tildeling av autorisasjon skal registreres i et autorisasjonsregister, jf. Normen kap. 5.2.1.1 <u>Utformingskrav</u> Leverandøren skriver «Lest og akseptert».	JA
Leverandørens besvarelse: Lest og akseptert		
6.8 (M)	Tildelt autorisasjon skal sikre at den enkelte kan få tilgang til relevante og nødvendige helse- og personopplysninger, jf. Normen kap.5.2.1 <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet oppfylles.	JA

Are
Chb



Oslo kommune
Helseetaten

Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til informasjonssikkerhet	JA/NEI
Leverandørens besvarelse: Tilgang til person- og helseopplysninger gis kun til på forhånd autoriserte brukere. Autorisasjon gis av kommunen selv igjennom tjenestens administrator for aktuell soneenhet/gruppe og omfatter personlig systembrukerkonto, tildelt applikasjonsrolle som gir tilgang til veldefinert funksjonalitet og medlemskap i aktuell(e) gruppe(er) som gir tilgang til spesifikk gruppe tjenestemottakere. Autorisasjonen kan kun benyttes etter tilstrekkelig autentisering av den enkelte ansatte.		
6.9 (M)	Kun teknisk personell med særskilt behov for tilgang, skal kunne autoriseres for større mengder helse- og personopplysninger, jf. Normen kap. 5.2.1 <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet oppfylles.	JA
Leverandørens besvarelse: Separasjon av helse- og personopplysninger i ulike kontoer per soneenhet, samt strukturering av opplysninger i gruppestruktur etter geografi eller andre kriterier er viktigste tiltak for å begrense muligheter for tilgang til større mengder opplysninger. Teknisk personell med tilgang til applikasjonene vil kun få tilgang til data iht tildelt autorisasjon (konto/gruppe og applikasjonsrolle). Følgende avgrensede grupper kategorier teknisk personell kan autoriseres for tilgang til større mengder helse- og personopplysninger • Tjenesteleverandør: Telenor Norge – navngitte enkeltpersoner i Telenor Norges e-helse enhet. Autorisert av kunde igjennom databehandleravtale for utførelse av driftsoppgaver eller for håndtering av 2. linje brukerstøttehenvendelser. Har ikke autorisasjon for annen tilgang enn iht databehandleravtale. • Plattform og integrasjonspartner (underleverandør): Tellu lot - navngitte enkeltpersoner. Autorisert av kunde igjennom databehandleravtale for utførelse av driftsoppgaver eller for håndtering av 3. linje brukerstøttehenvendelser. • Infrastrukturleverandør: Redpill Linpro AS - autorisert av kunde. Har ikke autorisasjon for annen tilgang enn iht databehandleravtale.		
6.10 (M)	Systemet som administrerer autorisasjon skal skille mellom rettigheter til å lese, registrere, redigere, rette, slette og/eller sperre helse- og personopplysninger, jf. Normen kap. 5.2.1 <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet oppfylles.	JA

uke
ans



Oslo kommune
Helseetaten

Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til informasjonssikkerhet	JA/NEI
Leverandørens besvarelse: Tjeneste- og integrasjonsplattformens underliggende autorisasjonstjenester tilbyr en fingranulert tilgangsmodell med muligheter for å definere spesifikke roller per tjeneste. For hver applikasjonsrolle som opprettes angis det for hvert informasjonselement i løsningen (tjenestemottaker, utstyrsenhet, egenskaper, systembruker, grupper, regler, varsler etc.) om rollen har opprett-, endre-, lese- og/eller sletterrettigheter. For tjenesten Digitalt tilsyn er det forhåndsdefinert et antall applikasjonsroller med ulik tilgang til informasjon og funksjonalitet. Ytterligere applikasjonsroller kan defineres igjennom konfigurasjon av overnevnte tilgangsrettigheter opprett, endre etc. for hver av de aktuelle informasjonselementene. Se også svar på krav knyttet til roller i løsningen, krav 4.24-4.28.		
6.11* (M)	Systembrukeres tilganger skal kunne tidsbegrenses. Med «tidsbegrensning» menes at systembrukeres tilgang kun er aktiv i en gitt periode, f.eks. mellom en start- og sluttdato. Funksjonen vil blant annet være spesielt nyttig når vikarer benyttes, disse kan gjerne legges inn som systembrukere før vedkommende starter, men tilgangen skal kun være aktiv i f.eks. juni og juli. <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet oppfylles.	JA
Leverandørens besvarelse: I en ny versjon av Telenor Digitalt tilsyn, som skal være klar før 1. oktober 2019, vil det være mulig å tidsbegrense systembrukeres tilgang til tjenesten. Det vil være mulig å definere tidsbegrenset tilgang for hver konto hvor brukeren har tilgang. Tidsbegrensningen vil være definert med en fra- og til-dato, og utenfor det angitte tidsrommet vil systembrukerens tilgang være deaktivert. Tidsbegrensning vil kunne aktiveres i administrasjonssystem for Shepherd.		
Autentisering		
6.12 (M)	Autentisering skal sikre identifisering i korrekt rolle i hvert enkelt tilfelle, jf. Normen kap. 5.2.2. <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet oppfylles.	JA

Wke
Cvth



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til informasjonssikkerhet	JA/NEI
Leverandørens besvarelse: Identifisering og autentisering iht Normen kap. 5.2.2 er etablert. Løsningens sikkerhetstjenester krever tilstrekkelig autentisering av systembruker før tilgang til applikasjon og informasjon. Etter gjennomført pålogging/autentisering angis tjenestekonto og rolle for brukersesjonen. Brukersesjonen representeres deretter igjennom en sikkerhetsbillett som medfølger i hver eneste kommunikasjon/oppslag/tjenestekall mellom systembrukerens utstyr og klientprogramvare (f.eks. pc og nettleser eller mobiltelefon og mobilapplikasjon). For hver eneste kommunikasjon/oppslag/tjenestekall valideres systembrukerens autentisering og autorisasjon, representert ved denne sikkerhetsbilletten, mtp. gyldighet (sikkerhetsbillettens levetid), tilgang til forespurt funksjonalitet og forespurt tilgang til data. Dersom valideringen avslås vil systembruker ikke få tilgang.		
6.13* (M)	Tilgang til applikasjonen skal kunne beskyttes av tofaktorautentisering (f.eks. SMS med engangskode) i henhold til «Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor*». To-faktorautentisering kan aktiveres pr. rolle. <u>Utformingskrav</u> Leverandøren skriver «Lest og akseptert». * https://www.regjeringen.no/no/dokumenter/rammeverk-for-autentisering-og-uavviseli/id505958/	JA
Leverandørens besvarelse: Lest og akseptert		
6.14* (M)	Påloggings-ID (brukernavn) for systembrukere skal ikke være autogenerated. For ansatte i Oslo kommune skal standard ansattnummer benyttes (dvs. kun siffer i påloggings-id). Andre systembrukere (f.eks. ansatte på alarmsentral, pårørende eller andre) skal kunne benytte en påloggings-ID som består av enten kun tall, kun bokstaver, eller en kombinasjon av disse, samt epostadresser. Påloggings-ID skal være unik. <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet oppfylles.	JA
Leverandørens besvarelse: Løsningen stiller ikke krav om noe spesielt format for brukernavn. Både kun-siffer, e-postadresser eller andre kombinasjoner kan benyttes. Påloggings-ID/brukernavn er unik innenfor en konto. Enkelte kommuner velger å benytte flere kontoer for å organisere sin Digitalt tilsyn tjeneste. Samme Påloggings-ID/brukernavn kan derfor benyttes i flere kontoer/tjenester.		

Arce
Cbo



Oslo kommune
Helseetaten

Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til informasjonssikkerhet	JA/NEI
6.15 (M)	Flere personer skal ikke benytte samme autentiseringskriterier, jf. Normen kap. 5.2.2. <u>Utformingskrav</u> Leverandøren skriver «Lest og akseptert».	JA
Leverandørens besvarelse: Lest og akseptert		
6.16 (M)	Ulike roller skal kunne tildeles ulike autentiseringskriterier ved behov, jf. Normen kap. 5.2.2. <u>Utformingskrav</u> Leverandøren skriver «Lest og akseptert».	JA
Leverandørens besvarelse: Lest og akseptert		
6.17* (M)	Passord skal tilfredsstillende følgende krav: • Passordkompleksitet: ○ Passord skal bestå av minimum 8 tegn ○ Passord skal bestå av siffer og store og små bokstaver ○ Passord kan inneholde spesialtegn som +?=&%# ○ Passord kan ikke inneholde bokstavene æøå • Varighet og historikk: ○ Passordets varighet skal være konfigurerbart, eksempelvis «90 dager» eller «utløper ikke» ○ Det skal ikke være tillatt å gjenbruke de 5 siste passordene ○ Passord skal ikke kunne byttes mer enn 1 gang i døgnet • Bytte av passord: ○ Tvunget bytte av passord skal være mulig. Skal være valgfritt for Kunden ○ Ved tvunget bytte av passord varsles brukeren minst fem dager før utløp, ved innlogging og/eller pr epost. <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet oppfylles.	JA
Leverandørens besvarelse: Oslo kommunes passordkrav er ikke implementert ved tilbudsinnstilling, men vil leveres innenfor angitt frist. Basert på Telenors og våre kunders sikkerhetsanbefalinger og vår erfaring fra tjenesten i praktisk drift har løsningen pt. implementert følgende krav til passordstyrke: Evalueringskriterium: Minimumskrav til kompleksitet: 18 poeng		

Handwritten signature



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til informasjonssikkerhet	JA/NEI
Poenggivning: • Minimumslengde 6 tegn: 6 • Tilleggs poeng for hvert tegn over minimumslengde: 2 • Tilleggs poeng for kombinasjon store og små bokstaver: 4 • Tilleggs poeng for å ha tegn ut over a-z 0-9: 6 Eksempler: • Korteste passord med bare små bokstaver: 16-tegn abcdefghijklmno • Korteste passord med store og små bokstaver, tall og tegn: 8 tegn a2cD%Fgh Passordkrav «varighet og historikk» er ikke implementert, men kan implementeres innenfor angitt frist. Passordkrav «tvungen bytte» er implementert og kan settes per systembruker konto. Varsling er ikke implementert, men kan utvikles innenfor angitt frist.		
6.18* (M)	Applikasjonen skal ha en funksjon der systembruker selv kan be om automatisk å få tilsendt nytt passord. <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet oppfylles.	JA
Leverandørens besvarelse: Oslo kommunes funksjonskrav er ikke implementert i tjenesten for Digitalt tilsyn ved tilbudsinn sending, men vil leveres innenfor angitt frist. Tjenesteplattformen Shepherd har funksjonalitet for dette allerede i dag, men funksjonaliteten er ikke lagt inn i Digitalt tilsyn applikasjonen. Funksjonaliteten kan benyttes i dag ved å gå til en annen og generisk tjeneste på plattformen, men vil bli lagt inn som integrert del av digitalt tilsyn applikasjonen innen frist for videreutvikling.		
6.19 (M)	Tekniske tiltak skal iverksettes slik at personer i eller utenfor virksomheten ikke skal kunne endre opplysninger uten at det registreres i løsningen, jf. Normen kap.5.2.1 <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet oppfylles.	JA

Arbeid
WB



Oslo kommune
Helseetaten

Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til informasjonssikkerhet	JA/NEI
Leverandørens besvarelse: Kravet oppfylles av to aspekter ved løsningen 1. Verifikasjon av brukerens autorisasjon ved hvert eneste tjenestekall. Løsningens sikkerhetstjenester krever tilstrekkelig autentisering av systembruker før tilgang til applikasjon og informasjon. Etter gjennomført pålogging/autentisering angis tjenestekonto og rolle for brukersesjonen. Brukersesjonen representeres deretter igjennom en sikkerhetsbillett som medfølger i hver eneste kommunikasjon/oppslag/tjenestekall mellom systembrukerens utstyr og klientprogramvare (f.eks. pc og nettleser eller mobiltelefon og mobilapplikasjon). For hver eneste kommunikasjon/oppslag/tjenestekall valideres systembrukerens autentisering og autorisasjon, representert ved denne sikkerhetsbilletten, mtp. gyldighet (sikkerhetsbillettens levetid), tilgang til forespurt funksjonalitet og forespurt tilgang til data. Dersom valideringen avslås vil systembruker ikke få tilgang. 2. Logging av endringer til autorisasjonsregister. Løsningens sikkerhetstjenester logger endringer av brukertilganger og autorisasjoner til autorisasjonsregister. Sikkerheten ved pkt 1) gjør at en har en sikker identifikasjon på personen som har utført endringen.		
6.20 (M)	Alle systemer skal ha mekanismer som hindrer uautoriserte endringer av helse- og personopplysninger. <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet oppfylles.	JA
Leverandørens besvarelse: Løsningens sikkerhetstjenester krever tilstrekkelig autentisering av systembruker før tilgang til applikasjon og informasjon. Etter gjennomført pålogging/autentisering angis tjenestekonto og rolle for brukersesjonen. Brukersesjonen representeres deretter igjennom en sikkerhetsbillett som medfølger i hver eneste kommunikasjon/oppslag/tjenestekall mellom systembrukerens utstyr og klientprogramvare (f.eks. pc og nettleser eller mobiltelefon og mobilapplikasjon). For hver eneste kommunikasjon/oppslag/tjenestekall valideres systembrukerens autentisering og autorisasjon, representert ved denne sikkerhetsbilletten, mtp. gyldighet (sikkerhetsbillettens levetid), tilgang til forespurt funksjonalitet og forespurt tilgang til data. Dersom valideringen avslås vil systembruker ikke få tilgang. Telenor har gjennomført tredjeparts uavhengig penetrasjonstest, som gav den konklusjon at det ikke var mulig for uautorisert aktør å endre opplysninger i tjeneste- og integrasjonsplattformen Shepherd.		

Åke
Chub



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til informasjonssikkerhet	JA/NEI
6.21* (M)	Tilgang til applikasjonen skal sikres med IP-filtrering. Den skal kunne gjelde for utvalgte roller, slik at eksempelvis pårørende kan unntas. <u>Utformingskrav</u> Leverandøren skriver «Lest og akseptert».	JA
Leverandørens besvarelse: Lest og akseptert		
Logging		
6.22 (M)	Logger med sikkerhetsmessig betydning, herunder registrering av autorisert bruk og forsøk på uautorisert bruk skal tas vare på til det av helsehjelpens karakter ikke lenger antas å være bruk for, jf. Normen kap. 2.3 og 5.4.4. <u>Utformingskrav</u> Leverandøren skriver «Lest og akseptert».	JA
Leverandørens besvarelse: Lest og akseptert		
6.23 (M)	Det skal registreres i logger i løsningen hvem som har hatt tilgang, jf. Normen kap. 3 (konfidensialitet). <u>Utformingskrav</u> Leverandøren skriver «Lest og akseptert». Leverandørene viser også hvordan kravet er oppfylt gjennom demonstrasjon iht. oppgitte demosituasjoner i Vedlegg 1 Beskrivelse av demonstrasjoner.	JA
Leverandørens besvarelse: Lest og akseptert		
6.24 (M)	Det skal registreres hvem som har foretatt registrering, endring, retting og sletting, jf. Normen kap. 3 (integritet). <u>Utformingskrav</u> Leverandøren skriver «Lest og akseptert». Leverandørene viser også hvordan kravet er oppfylt gjennom demonstrasjon iht. oppgitte demosituasjoner i Vedlegg 1 Beskrivelse av demonstrasjoner.	JA
Leverandørens besvarelse: Lest og akseptert		

Alice
Puls



Oslo kommune
Helseetaten

Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til informasjonssikkerhet	JA/NEI
6.25 (M)	For å oppdage brudd eller forsøk på å bryte regelverket skal det som minimum føres logger over, jf. Normen kap. 5.4.4: • Autorisert bruk • Alle forsøk på uautorisert bruk <u>Utformingskrav</u> Leverandøren skriver «Lest og akseptert». Leverandørene viser også hvordan kravet er oppfylt gjennom demonstrasjon iht. oppgitte demosituasjoner i Vedlegg 1 Beskrivelse av demonstrasjoner.	JA
Leverandørens besvarelse: Lest og akseptert		
6.26 (M)	Følgende skal minimum registreres i logger, jf. Normen kap.5.4.4.: • Entydig identifikator for den autoriserte brukeren • Hvilke type opplysninger det er gitt tilgang til • Hvilke endringer som er blitt utført («endret fra – endret til») • Hvem som har fått utlevert helseopplysninger som er knyttet til tjenestemottakers eller brukerens navn eller fødselsnummer • Grunnlaget for tilgangen • Tidspunkt og varighet for tilgangen <u>Utformingskrav</u> Leverandøren skriver «Lest og akseptert». Leverandørene viser også hvordan kravet er oppfylt gjennom demonstrasjon iht. oppgitte demosituasjoner i Vedlegg 1 Beskrivelse av demonstrasjoner.	JA
Leverandørens besvarelse: Lest og akseptert		
6.27* (E3)	Løsningen bør ivareta at Kunden kan ta ut en rapport over systembrukere, som viser systembrukers sonetilhørighet, tildelt(e) rolle(r) og tidsperiode for aktiv tilgang. Rapporten kan overføres til excel. <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet oppfylles.	JA

Arce
CML



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

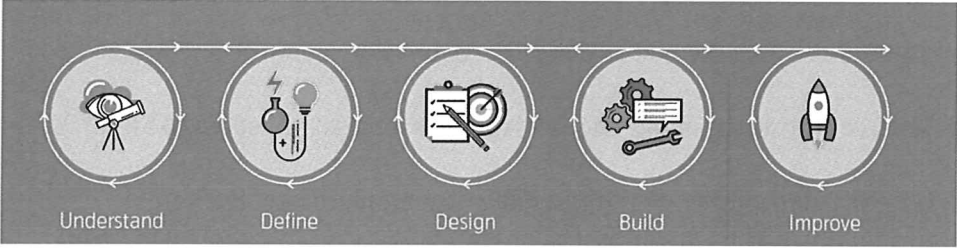
Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til informasjonssikkerhet	JA/NEI
Leverandørens besvarelse: Oslo kommunes funksjonskrav er ikke fullstendig implementert i tjenesten for Digitalt tilsyn ved tilbudsinnssending, men vil leveres innenfor angitt frist. Tjenestens administrasjonsløsning har i dag mulighet for å ta ut lister/rapporter på en rekke områder per konto/soneenhet, med relevante opplysninger per rapport, bl.a. rapporter over: • Systembrukere • Tilgangsgrupper • Tjenestemottakere • Roller Rapportene kan eksporteres til Excel. Siste aktive tilgang er pt. tilgjengelig i brukergrensesnitt, ikke inkludert i rapport, men kan kopieres ut fra aktivitetslogg og enkelt filtreres frem i Excel. Ytterligere rapporter og kombinasjonsmuligheter kan utvikles på nærmere spesifisering.		
Integritet		
6.28 (M)	Helse- og personopplysninger skal være korrekte og knyttes til rett identifisert person, jf. Normen kap. 3 (integritet). <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet oppfylles.	JA
Leverandørens besvarelse: Telenors Digitalt tilsyn tjeneste kan benyttes som en pseudonymisert eller personidentifiserende tjeneste. Enhetene kan også være koblet til lokasjon (adresse/rom) ikke person. Dersom kunden velger å benytte Digitalt tilsyn som en personidentifiserende tjeneste vil alle opplysninger være knyttet til det underliggende tekniske pasient-ressurs i tjenesten. Sikkerhetsløsningen har som beskrevet i krav 6.12, 6.19 og 6.20 mekanismer som verifiserer autorisasjon til å lagre data til aktuell person/ressurs. Løsningen har blitt omfattende testet, både ved intern testing og igjennom uavhengig tredjeparts penetrasjonstest, mtp skrijving av data til feil person, noe som i testene ikke har vært mulig verken igjennom brukergrensesnitt eller forsøk på uautorisert bruk av integrasjonstjenester.		
Innebygget personvern		
6.29 (M)	Løsningens standardinnstillinger skal på forhånd være satt til å være mest mulig personvernvennlig i henhold til Datatilsynets veileder for innebygget personvern eller tilsvarende: https://www.datatilsynet.no/regelverk-og-verktoy/veiledere/programvareutvikling-med-innebygd-personvern/ <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet oppfylles.	JA
Leverandørens besvarelse: Telenors digitalt tilsyn er utformet og utviklet iht prinsippene for innebygget personvern beskrevet i		

AKO
CMB



Oslo kommune Helseetaten

Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til informasjonssikkerhet	JA/NEI
	Datatilsynets veileder, denne sammenfaller svært godt med Telenors tjenstedesignprosess. Telenors Digitalt tilsyn er etablert etter denne metodikken som for alle andre tjenester som etableres i Telenor. Tjenstedesignprosessen er basert på iterasjoner, med gjentagende prototyping, utprøving, evaluering og forbedring. Vi legger vekt på tilstrekkelig involvering av relevante brukere og personell, inkludert personvernbeskyrminger og innstillinger, samt involverer Telenors egne personvernspesialister for vurderinger igjennom alle faser av arbeidet. Tjenstedesignprosessen er illustrert under:  Datatilsynets veileder for innebygget personvern og Telenors tjenstedesignprosess sammenfaller som følger (Datatilsynets begreper først, Telenors begreper i parentes). Opplæring (Understand) - alle medarbeidere har gjennomført Telenors obligatoriske opplæringsprogram for personvern. Alle i vårt e-helse tjenesteutviklingsteam har i tillegg spesiell opplæring i personvernakspekter ved tjenesteutvikling. Vi har tilgang på spisskompetanse fra Telenors øvrige personvernfunksjoner og –ombud. En kritisk del av opplæringen er Understand/Innsiktsfasen, hvor vi innhenter mer kunnskap om behov rundt den spesifikke tjenesten, både aktører, arbeidsprosesser, deres kompetanse osv. Krav (Define) - produkter og tjenester etableres med kravstyring, som sikrer at funksjonskrav til løsningen, herunder personvernkrav følges opp igjennom alle faser av prosessen. Både den registrertes rettigheter, virksomhetens plikter og øvrige personvernrelaterte krav spesifisert i helselovgivningen og Normen ivaretas her. Kravstyring er en kontinuerlig prosess som følges opp igjennom alle faser av en produktlivssyklus. Design (Design) - Designfasen gjennomføres basert på gjentatte runder med prototyping, testing og intervjuer med relevante aktører, herunder representative tjenestemottakere, helsepersonell og administratorer. Koding og Test (Build) - Tjenesten er bygget på anerkjente open-source applikasjonsrammeverk med aktive miljøer/communities som bidrar inn i feilretting og forbedring. Koden forvaltes i versjonshåndteringssystemer med automatiserte rutiner for kvalitetssikring. Hver nye kodesnutt gjennomgås av sidemann for uavhengig kvalitetssikring iht utviklingspartners ISO27001 sertifiserte styringssystem og prosedyrer. Tjenesten utvikles i iterasjoner etter smidige prinsipper og test-dreven utviklingsmetodikk. Funksjonalitet, herunder innebygget personvern, testes i små deler underveis, og vi gjennomfører regresjonstest av tidligere etablert funksjonalitet for alle nye hovedversjoner. Produksjonssetting (ikke omhandlet i Telenors tjenstedesignprosess) - Tjenesten digitalt tilsyn gjennomgår Telenors gatekeeperprosess for godkjenning før salg/produksjonssetting. Dette er en	

Ake
Chen



Oslo kommune
Helseetaten

Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til informasjonssikkerhet	JA/NEI
	kvalitetssikring av alle ledd, fra produktkvalitet til utstyrslogistikk, hendelsesoppfølging, feilretting, support og administrative prosedyrer. Forvaltning (Improve, samt driftsrutiner) - Digitalt tilsyn følger for Telenor e-helse samme prosedyrer som for alle andre velferdsteknologitjenester vi har i drift mtp. Hendeshåndtering, varsling til dataansvarlige mv. For videreutvikling av tjenesten følges tjenstedesignprosessen på nytt dersom større endringer skal gjøres, mens for mindre forbedringer gjennomføres samme prosess i et nedskalert format. Etablert funksjonalitet: Det er flere tekniske mekanismer i tjenesten som bidrar til innebygget personvern: • Kunden kan anvende et fritt valgt antall "kontoer" for høyeste grad av separasjon av informasjon. • Tjenesten kan benyttes uten direkte identifiserende personopplysninger dersom hensiktsmessig, f.eks. ved bruk på institusjon kan romnummer eller pseudonym benyttes istedenfor navn. • Som standard er tilsynsvindu lukket. Administrator må gjøre kamera tilgjengelig for tilsyn for utvalgte tidspunkt før det kan tas i bruk, og tilsynsvinduer kan når som helst begrenses. • Nye operatører har ved registrering ikke tilgang til tjenestemottakers kamera, de må eksplisitt legges til aktuell tilgangsgruppe.	
6.30 (M)	Løsningen skal kun innhente nødvendige personopplysninger iht. det besluttede formålet. Metoder for å begrense mengden personopplysninger kan være: • Særlige kategorier av personopplysninger er utelatt • Fødselsnummer er utelatt • Informasjon som registreres kan kun indirekte identifisere en person (en person vil være indirekte identifiserbar dersom det er mulig å identifisere vedkommende gjennom bakgrunnsopplysninger som f.eks. bostedskommune eller institusjonstilknytning med opplysninger om alder, kjønn, yrke, diagnose eller liknende) • Navn er erstattet med pseudonym <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet oppfylles.	JA

AKK
CMA



Oslo kommune
Helseetaten

Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til informasjonssikkerhet	JA/NEI
Leverandørens besvarelse: Det er kun et svært begrenset antall personopplysninger som er nødvendig for å benytte tjenesten. Tjenesten kan benyttes uten direkte identifiserende personopplysninger dersom hensiktsmessig, f.eks. ved bruk på institusjon kan romnummer benyttes istedenfor navn. Det kan fritt benyttes pseudonym istedenfor navn. Fødselsnummer er ikke påkrevet med mindre kunden ønsker å benytte dette f.eks. ifbm integrasjon mot Velferdsteknologisk knutepunkt hvor fødselsnummer er påkrevet.		
6.31* (M)	Sletterutiner skal være etablert, og informasjon kan slettes automatisk etter bestemte tidsintervaller, eller når formålet ved behandlingen er opphevet. Dette forutsetter at opplysningene ikke er journalpliktige iht. pasientjournalloven. <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet blir ivaretatt og hvordan dette er dokumentert.	JA
Leverandørens besvarelse: Det er etablert automatiserte sletterutiner for all informasjon som ikke eksplisitt slettes av tjenesteutøver ifbm administrasjon av tjenesten. Registrerte personopplysninger som navn osv. slettes umiddelbart når tjenestemottaker avregistreres fra tjenesten. Telenors vurdering er at tjenesten ikke skal være hovedkilde for journalpliktige opplysninger, dette skal ligge i kommunens EPJ. Shepherd har automatiske sletterutiner for hendelsesloggen i en konto. Ved konfigurasjon av en konto definerer man en TTL (Time To Live) for innslagene i loggen, og de slettes deretter automatisk når de utløper. Det lagres ingen personopplysninger i administrasjonsløsning for personlig gateway. Sletterutiner er følgelig ikke nødvendig. Utstyrskonfigurasjoner (som ikke inneholder personopplysninger) slettes når utstyr slette/avregistreres. Det lagres ingen personopplysninger i administrasjonsløsning for kamera. Sletterutiner er følgelig ikke nødvendig. Utstyrskonfigurasjoner (som ikke inneholder personopplysninger) slettes når utstyr slette/avregistreres.		
6.32 (E3)	Løsningen bør ha muligheter for konfigurering av egendefinerte tidsintervaller for automatisk sletting av spesifikk informasjon. <u>Utformingskrav</u> Leverandøren beskriver hvilke typer data som kan tilknyttes egendefinerte tidsintervaller for sletting. Dette kan f.eks. være data knyttet til: • Tekniske varsler Aktivitetsrelaterte data (bilder, video, lyd, hendelser, varsler, målinger m.m.).	JA

ACE
04/6



Oslo kommune
Helseetaten

Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til informasjonssikkerhet	JA/NEI
Leverandørens besvarelse: Det lagres ingen video, lyd eller andre aktivitetsrelaterte data i løsningen. Det er følgelig ikke heller relevant med sletteintervaller for disse. Hendelser og varsler slettes iht en konfigurert TTL (Time To Live) både for hendelser og varsler fra utstyr, og for hendelser og varsler relatert til tjenestemottaker, som beskrevet i svar til kap. 6.31. De mest vanlig brukte sletteintervallene er 30 og 90 dager.		
6.33* (M)	Brukergrensesnittet skal begrense muligheten til å oppgi unødvendig personlig informasjon. <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet oppfylles.	JA
Leverandørens besvarelse: Viktigste tiltak for å forhindre registrering av unødvendig personlig informasjon er at det er svært få felter for registrering av opplysninger i løsningen. Brukergrensesnittet for Telenors digitalt tilsyn er spesielt etablert for formålet med tjenesten og har ingen felter for registrering av unødvendige personopplysninger. Det finnes kun ett generelt fritekstfelt for å angi noe som identifiserer for hvem eller hvor hendelsen har inntruffet, ut over dette er det ingen muligheter for å registrere personopplysninger. I det ene fritekstfeltet som finnes kan en registrere enten fullt navn, eller en adresse, eller et romnummer, eller en annen identifiserende opplysning som et kallenavn, eller et pseudonym etter kommunens ønske.		
6.34 (M)	Lagret informasjon skal være kryptert for å begrense tilgangen til hva for eksempel systemadministrator kan se av personopplysninger. <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet oppfylles.	JA
Leverandørens besvarelse: All kommunikasjon med systemet, og mellom systemet og eksterne integrasjoner går over krypterte kommunikasjonskanaler. Data som lagres i systemet, både personopplysninger om tjenestemottakere og systembrukere, samt konfigurasjon av tjenesten, lagres kryptert.		
6.35 (M)	Enkelte systembrukere skal kunne sperres for innsyn til enkelte tjenestemottakere, slik at vi kan ivareta innbyggernes rettigheter til å sperre egne helseopplysninger for enkelte ansatte. <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet oppfylles.	JA

Alle
Chh



Oslo kommune
Helseetaten

Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til informasjonssikkerhet	JA/NEI
Leverandørens besvarelse: I administrasjonssystem til Shepherd kan administrator for tjenesten konfigurere at en systembruker skal nektes innsyn til en eller flere tjenestemottakere. All tilgang til data for disse tjenestemottakerene vil da bli sperret, uavhengig hvilken rolle brukeren har, og tilgangene som er gitt til rollen.		
6.36 (M)	Det skal være etablert kryptert kommunikasjon over Internett, i databaser og på mobile enheter. Kryptering gjelder alle ledd av verdikjeden som tjenesten består av. <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet oppfylles.	JA
Leverandørens besvarelse: Overordnet arkitekturf figur beskrevet i krav 2.11 viser kommunikasjon mellom ulike komponenter i løsningen. All kommunikasjon i verdikjeden, mellom komponentene nummerert 1-16, har tilstrekkelig kompleks transportkryptering. Noen eksempler: • Axis kamera – Axis Guardian Communication system • Axis Guardian Communication system – Telenor Shepherd • Neat Care Manager – Telenor Shepherd • Telenor Shepherd – ID-porten • Telenor Shepherd – systembrukers klient (pc/nettbrett/mobil) • Neat Care Manager – systembrukers klient (pc/nettbrett/mobil) • Telenor Shepherd – VKP • mv. Med tilstrekkelig kompleks transportkryptering mener Telenor Transport Layer Security (TLS) på standardiserte kommunikasjonsprotokoller som http og websockets. TLS er en Internet Engineering Task Force (IETF) standard som muliggjør ende-til-ende autentisering og privat kommunikasjon ved hjelp av kryptografi. Hvilken krypteringsprotokoll som anvendes i hvert enkelt grensesnitt varierer med hva endepunktene kan støtte, som igjen avhenger av hvilke programversjoner som er installert. Telenor har prosedyrer for å sikre oppdatert programvare på alle ledd i verdikjeden som er vårt ansvar, mens kommunen er ansvarlig for å sikre oppdatert programvare på alle ledd i verdikjeden som er kommunens ansvar, for eksempel nettleser på den ansattes pc'er. Dersom ikke programvare er tilstrekkelig oppdatert vil den komponenten med de strengeste sikkerhetskrav avvise kommunikasjon med komponenten med ikke tilstrekkelig sikkerhet, og kommunikasjon kan ikke etableres. Et eksempel på dette er dersom nettleser på kommunens pc kun støtter TLS v1.1 (vurdert per september 2019 som ikke sikker), mens Telenors tjeneste krever TLS v1.2 (nyeste med utbredte standard), eller dersom ikke mest oppdaterte krypteringsalgoritmer benyttes, f.eks ved at en kommunikasjonspart kun støtter RC4 krypteringsalgoritme som er vurdert som usikker for bruk innenfor TLS. Gjeldende sikkerhetsanbefalinger er at grensesnitt er sikret med gyldige sertifikater med minst 2048bits nøkler. Alle grensesnitt i løsningen er sikret med sertifikater med minst 2048bits nøkler		



Oslo kommune
Helseetaten

Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til informasjonssikkerhet	JA/NEI
utstedt av anerkjent sertifikatmyndighet og gyldighet innenfor aktuell tidsperiode. Telenor har prosedyrer for periodisk fornyelse av sertifikater. Telenor tester komponenter under vårt ansvar bl.a. med SSL-labs. Webserver for Telenors Digitalt tilsyn validerer til karakter A+ (høyeste nivå) per september 2019 (https://www.ssllabs.com/ssltest/analyze.html?d=www.smartracker.no).		
Håndtering av teknisk sårbarhet		
6.37 (M)	Det skal finnes prosedyrer for å innhente informasjon om tekniske sårbarheter i løsningen. Informasjon innhentes jevnlig, eksponering overfor disse sårbarhetene evalueres og egnede tiltak iverksettes for å håndtere risikoen forbundet med dem. Eksempler på kilder til dette er <u>Microsoft Security TechCenter</u>, <u>Security Bulletins</u>, <u>Cisco Security Advisories and Alerts</u> og <u>Symantec Security Center</u>. <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet oppfylles.	JA
Leverandørens besvarelse: Telenor, partnere og underleverandører har hver sine prosedyrer for kontinuerlig innhenting og evaluering av oppdatert informasjon og trusler og sårbarheter. Kort sammendrag nedenfor: Telenor Norge Security – fortløpende vurdering av generelt trusselbilde og generelle IKT og IoT tekniske sårbarheter basert på en rekke kilder. Anbefaler basert på dette generelle tiltak. Forvalter også Telenor interne IKT- og IoT sikkerhetspolicyer og anbefalte tiltak. Ukentlig intern distribusjon fra Telenor Norge Security og evaluering i Telenor Norge e-helse. Telenor Norge E-helse – Sikkerhetsansvarlig utøver strategi- og internkontrollfunksjon for risikostyring for produktene, bl.a. etterlevelse av Telenor IKT og IoT sikkerhetspolicyer. Sikrer oppfølging av eksternt identifiserte trusler og sårbarheter videre i Telenor Norge e-helse produkter og verdikjede. Produktsjefer holder fortløpende dialog med utstys- og andre underleverandører for oppfølging av endringer i trusler og sårbarheter og evt. endringer av risikovurderinger og tilhørende korrigerende tiltak. Gjelder både brukernært utstyr, programvare og infrastruktur. Utstys- og tjeneste underleverandører utfører fortløpende vurderinger på sine områder. Telenors partnere og underleverandører: Tellu IoT (ISO 27001 sertifisert), Axis Communications (ISO 27001 sertifisert), Neat Electronics (ISO 27001 sertifisert) og AWS (ISO 27001 sertifisert) har alle styringssystemer for informasjonssikkerhet med etablerte prosedyrer for monitorering og oppfølging av risikobildet med trusler og sårbarheter henhold til internasjonal kvalitetsstandard i forhold til aktuelle komponenter, og følger opp relevante sikkerhetsbulletiner og lignende som inkluderer kilder eksemplifisert i kravspesifikasjon og andre som for eksempel blogger, nyhetsbrev, rapporter osv fra Norsis (https://norsis.no/), Nasjonal Sikkerhetsmyndighet (NSM) (https://www.nsm.stat.no/) og Mnemonic (https://www.mnemonic.no/). Utvalg av offentlig publiserte produktspesifikke kilder nedenfor:		

Are
CMB