

## Phoniro 6000

### Krav til nettverk

Dokumentet beskriver krav –og spesifikasjoner til nettverk for Phoniro 6000.

### Innholdsfortegnelse

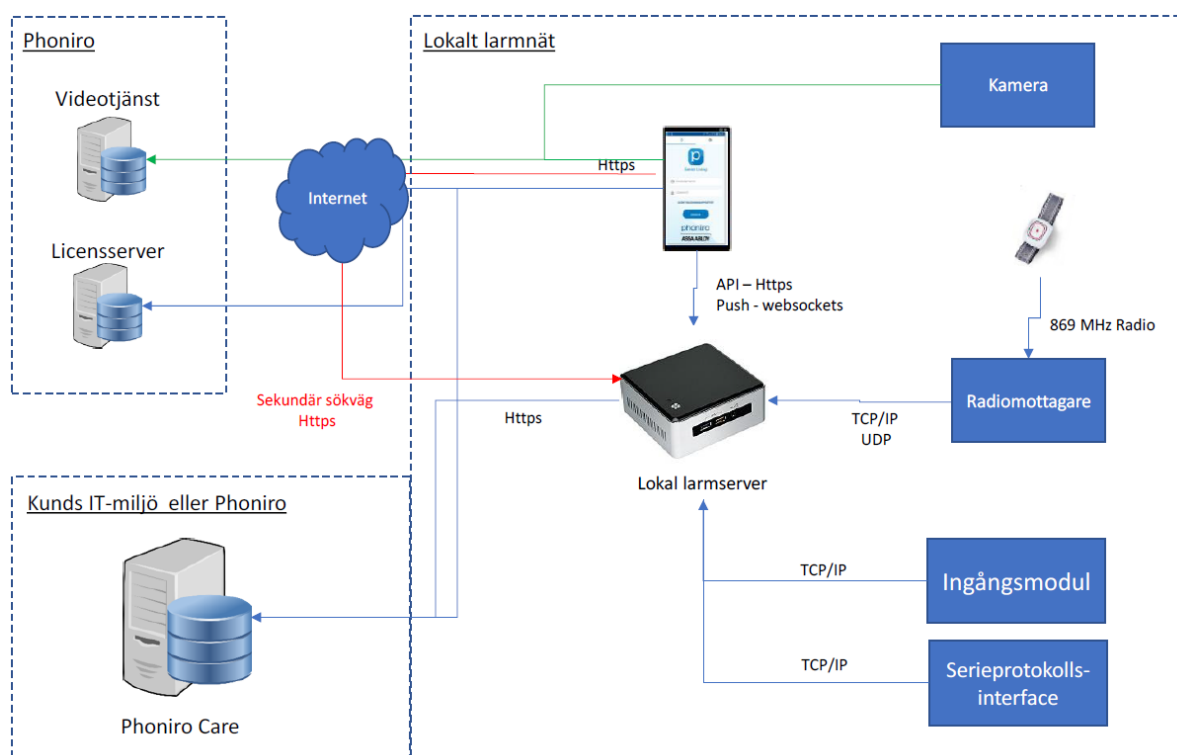
<b>1. PHONIRO 6000 SYSTEMOVERSIKT .....</b>	<b>2</b>
<b>2. NETTVERKS KOMMUNIKASJON .....</b>	<b>3</b>
2.1 KOMMUNIKASJON LOKAL ALARMSERVER PLAS OG PHONIRO CARE WEBGRENSESNIITT.	3
2.2 KOMMUNIKASJON LOKAL ALARMSERVER PLAS OG PHONIRO CARE API.	3
2.3 KOMMUNIKASJON SENIOR LIVING APPEN OG PHONIRO CARE API.	3
2.4 KOMMUNIKASJON SENIOR LIVING APPEN OG LOKAL SERVER PLAS.	4
<b>3. WIFI.....</b>	<b>4</b>
3.1 WiFi.	4
3.2 DEKNING.	5
3.3 SIGNALSTYRKE.	5
3.4 WiFi -KANALER.	5
3.5 NETTVERKSHASTIGHET.	5
3.6 DEDIKERT SSID FOR PASIENTVARSLINGSSYSTEMET.	5
3.7 SYNLIG SSID.	6
3.8 MANAGEMENT/CONTROLLER.	6
<b>4. FALLBACK TIL 4G- SEKUNDÆR SØKE VEI MOT LOKAL ALARMSERVER. ....</b>	<b>6</b>
<b>5. KOMMUNIKASJON MELLOM SENIOR LIVING APPEN OG LISENSSERVER .....</b>	<b>7</b>
<b>6. MDM- FLÅTESTYRING AV ALARMTELEFONER .....</b>	<b>7</b>
<b>7. RADIOMOTTAKERE NEAT D-TECT-IP .....</b>	<b>7</b>
7.1 KOMMUNIKASJON MELLOM RADIOBASE OG LOKAL ALARMSERVER PLAS.	7
7.2 KOMMUNIKASJON MELLOM RADIOBASE D-TECT-IP OG PHONIRO 600 SCAIP RECIVER.	8
7.3 KOMMUNIKASJON MELLOM INNGANGSMODULER OG LOKAL ALARMSERVER PLAS.	8
7.4 KOMMUNIKASJON MELLOM SERIEPROTOKOLLINTERFACE OG LOKAL ALARMSERVER PLAS.	8
<b>8. NTP SERVER &amp; REMOTE.....</b>	<b>8</b>
8.1 NTP.	8
8.2 REMOTE.	8
<b>9. TALE I PHONIRO 6000 .....</b>	<b>9</b>
9.1 KOMMUNIKASJON MELLOM TRYGGHETSALARM NOVO OG PHONIRO 6000.	9
9.2 KOMMUNIKASJON MELLOM TRYGGHETSALARM NOVO OG CMP.	9
<b>10. KAMERA TILSYN VED ALARM.....</b>	<b>10</b>
10.1 KOMMUNIKASJON MELLOM KAMERA OG VIDEOTJENESTEN.	10
10.2 KOMMUNIKASJON MELLOM SENIOR LIVING APPEN OG VIDEOTJENESTEN.	10
<b>11. BATTERI BACKUP / UPS .....</b>	<b>10</b>
<b>12. PORT OVERSIKT .....</b>	<b>10</b>
<b>13. TELEFON INNSTILLINGER .....</b>	<b>11</b>

## 1. Phoniro 6000 Systemoversikt

Phoniro 6000 har forskjellige system komponenter som er delt inn i

- En lokal alarmserver som fysisk er lokalisert på institusjon- og eller boligen og dermed sikrer lokal driftsstabilitet.
- En sentral alarmtjeneste i Phoniro CARE som enten kan installeres sentralt i kundens driftsmiljø eller levert som en skytjeneste.
- En sentral lisensserver lokalisert i Phoniro systems driftsmiljø og som håndterer den første forbindelsen mellom Senior Living appen og Phoniro CARE samt oppdateringer av appen.

All administrasjon og konfigurasjon av Phoniro 6000 utføres i Phoniro CARE skytjeneste. Den lokale alarmserveren PLAS kommuniserer med skytjenesten Phoniro CARE for å hente konfigurasjon data og alarm statistikk. Ingen informasjon lagres permanent på den lokale serveren PLAS.



Selve alarmstyringen styres autonomt i den lokale alarmserveren. Dermed lokal driftssikkerhet er sikret selv om tilkoblingen til skytjenesten blir brutt.

## 2. Nettverks kommunikasjon

Det foretrekkes at det opprettes eget Subnett / Vlan for pasientvarslingssystemet. Da blir alle funksjoner isolert i eget beskyttede nettverksegment.

Følgende innstillinger må gjøres for å sikre funksjon.

Den lokale alarmserveren PLAS består av:

1. Et Windows 10 operativsystem som har fast IP adresse som standard er 10.0.10.9  
*Kan endres til alternativ IP-adresse tilpasset i kundens subnett.*
2. En virtuell klient med fast IP-adresse som standard er 10.0.10.10.  
Kan endres til alternativ IP-adresse tilpasset i kundens subnett.  
På denne virtuelle klienten kjøres Phoniro 6000 pasientvarsling system og en DHCP - server som kan benyttes om det ikke er til rette lagt for kundes DHCP i opprettet Subnett. DHCP adresser 10.0.10.16 -10.0.10.250.  
*Kan endres til alternativ IP-adresser tilpasset i kundens subnett.*  
Anbefaler at kommunens DHCP-server benyttes.
3. En virtuell klient med fast IP-adresse som standard er 10.0.10.11.  
*Kan endres til alternativ IP-adresse tilpasset i kundens subnett.*  
CMS kjører på denne serveren med funksjon for å håndtere innganger og serielle grensnettmoduler.

Den laveste nettverkshastigheten for kommunikasjon mellom kablede enheter i alarmsystemet er 10 Mbit / s

### 2.1 Kommunikasjon lokal alarmserver PLAS og Phoniro CARE webgrensesnitt.

Kommunikasjon fra lokal alarmserver PLAS til Phoniro Care webgrensesnitt er ikke nødvendig for alarmfunksjonalitet, men bør være tilgjengelig for å opprettholde all service- og supportinnsats f.eks statistikk, logger og konfigurasjons endringer.

Trafikken kjøres på HTTPS port 443 (TCP) eller HTTP port 80 (TCP) fra den lokale alarmserveren PLAS til Phoniro Care webgrensesnitt

### 2.2 Kommunikasjon lokal alarmserver PLAS og Phoniro CARE API.

Kommunikasjon fra lokal alarmserver PLAS til Phoniro Care startes fra den lokale alarmserveren og kjøre på HTTPS og krever at port 443 (TCP) er åpen i brannmuren for utgående trafikk til Phoniro Care API. Ingen brannmuråpninger trenger å lages fra Phoniro Care til den lokale alarmserveren PLAS.

### 2.3 Kommunikasjon Senior Living appen og Phoniro CARE API.

Innloggingen i Senior Living appen skjer direkte mot Phoniro Care, så det kreves en portåpning for port 443 (TCP) fra WiFi-nettverket der alarmtelefonene er plassert mot den sentrale alarmtjenesten Phoniro Care API. Derfor er det nødvendig med en forbindelse mellom WiFi-nettverket og den sentrale alarmtjenesten.

---

## 2.4 Kommunikasjon Senior Living appen og lokal server PLAS.

Den lokale alarmserveren sender normalt ut alarmer til alarmtelefoner på institusjon –og eller boligen via WiFi. Det er også en tilleggsfunksjon som lar alarmtelefoner og den lokale alarmserveren kommunisere med en sekundær kommunikasjonsbane over mobilt Internett 4G hvis alarmtelefonen mister kontakten med den lokale alarmserveren via sin primære kommunikasjonsbane.

Som standard er kommunikasjonen mellom Senior Living appen og den lokale alarmserveren PLAS via HTTPS eller HTTPS på port 8080 (TCP), portene må være åpne fra subnett der alarmtelefonene er plassert til nettverket der den lokale alarmserveren er lokalisert.

Senior Living appen krever også at push-meldinger er tillatt. Disse går over HTTPS eller HTTP port 8080 (TCP)

## 3. WiFi

### 3.1 WiFi.

Kommunikasjon mellom Senior Living appen i alarmtelefonen og den lokale alarmserveren stiller ingen spesifikke krav til for eksempel 802.11-standarder, men alarmsystemet er utelukkende avhengig av en forbindelse mellom disse.

Valg av type telefon kan imidlertid bety at det må stilles noen krav til hvordan WiFi-nettverket er satt opp. Retningslinjer som er satt opp for å forbedre stabiliteten.

Generelle anbefalinger:

- Kommunikasjonen mellom den lokale alarmserveren PLAS og alarmtelefonene skal være minst 6 Mbps, men kan midlertidig gå ned til 1 Mbps hvis det ikke påvirker tilkoblingen mellom alarmtelefonen og alarmserveren. Ved kommunikasjon skal det ikke være mer enn 1% avbrudd i løpet av 24 timer og ingen kommunikasjonsavbrudd lenger enn 30 sekunder.
- WiFi-nettverket og Vlan må være i samme subnett som radiobaser og den lokale alarmserveren PLAS.
- WiFi-standarder endres kravene ut i fra forskjellige alarmtelefoner, og WiFi-standarden må derfor tilpasses de ulike telefonmodeller som er ment å brukes. Eksempel på en sertifisert alarmtelefonene som brukes av Phoniro Systems, kompatibilitetstestede Samsung Galaxy Xcover 4S og den tåler 802.11 a / b / g / n / ac 2,4 + 5GHz4

Basert på erfaring fra tidligere installasjoner, anbefales det imidlertid å unngå 802.11a og 802.11b og bruke 802.11n og / eller 802.11ac så mye som mulig i stedet

### 3.2 Dekning.

- For å sikre at det alltid kan leveres alarmer, anbefales det at alarmtelefonene kan "streife" sømløst og raskt hand over mellom tilgangspunktene (AP) i WiFi-nettverket. For å oppnå dette, anbefales det at WiFi-nettverket er konfigurert og dimensjonert slik at alarmtelefonene kan bevege seg fritt i hele området der det skal være mulig å motta alarmer uten å slippe noen datapakker når du bytter tilgangspunkt(AP).  
Derfor anbefales det at tilgangspunktene (AP) støtter 802.11k, 802.11v og 802.11r
- Det er viktig at det tas hensyn til dekningsområdet slik at alle rom i institusjon/bolig der pleiepersonell som bruker alarmsystemet som for eksempel beboer rom, felles rom/korridorer, trapperom, administrasjon ect har 100% dekning.

### 3.3 Signalstyrke.

- Når du måler signalstyrke til WiFi, er det viktig at den type alarmtelefon som Senior Living appen brukes på, er den som benyttes under måling av WiFi signal styrke.
- Tellu anbefaler at alarmtelefonen alltid er innenfor dekningsområdet til to tilgangspunkt der de har signalstyrke i henhold til:
  - Primært tilgangspunkt(AP): Minimum signalstyrke på -65 dB
  - Sekundært tilgangspunkt: Minimum signalstyrke på -75 dB
  - Dimensjonering og planlegging av signalstyrken i WiFi-nettverket gjøres for å motvirke såkalte "Sticky clients".

### 3.4 WiFi -kanaler.

- Når du planlegger WiFi-nettverket, bør følgende tas i betraktning:
  - Kanalbredden på kanalene anbefales til 20 MHz(**Formulere bedre**)
  - Unngå om mulig DFS-kanaler (Dynamic Frequency Selection)
  - Kanaler som brukes skal ikke ha mer enn 50% kanalbruk kontinuerlig.

### 3.5 Nettverkshastighet.

- Senior Living applikasjonen krever ikke høy hastighet, men tilkoblingen er veldig viktig. Derfor bør WiFi-nettverket være optimalisert for tilkobling fremfor ytelse. Dette kan bety at lavere nettverkshastigheter foretrekkes som obligatoriske. Et eksempel på dette er 6 og 9 Mbps på 5GHz-båndet og muligens ned til 1 Mbps på 2,4 GHz hvis det ikke har for negativ effekt på kanalutnyttelsen.

### 3.6 Dedikert SSID for pasientvarslingssystemet.

- Anbefalingen fra Tellu er at det er satt opp en egen SSID for pasientvarslingssystemet for å sjekke at ingen andre enheter er i samme subnett og forstyrrer alarmfunksjonaliteten. Det anbefales imidlertid ikke å bruke mer enn 4 unike SSID-er per subnett, da dette kan forårsake problemer med kanalopphopning og andre ytelser i WiFi-nettverket.

---

Dedikert SSID er å foretrekke hvis Phoniro 6000 kombineres med Phoniro Systems digital nøkkelhåndtering for spesielle institusjoner/boliger, ettersom flere av Phoniro-systemets produkter vil bruke WiFi-nettverket

### 3.7 Synlig SSID.

- Phoniro 6000 har ingen krav om at SSID for WiFi-nettverket skal være synlig eller skjult. Men anbefalingen er å bruke en synlig SSID for å gjøre det lettere for alarmtelefonene å veksle mellom tilgangspunktene(AP) i WiFi-nettverket

### 3.8 Management/Controller.

- For å sikre at alarmsystemet har høyest mulig oppe tid og dermed forhindrer at alarmfunksjonaliteten forsvinner, anbefales det at det lokale WiFi-nettverket opprettholder funksjon i tilfelle med eventuell brudd møte WiFi Controller i kommunens driftsmiljø.

## 4. Fallback til 4G- sekundær søke vei mot lokal alarmserver.

Den primære kommunikasjonsmetoden mellom Senior Living appen og lokal alarmserver PLAS er som beskrevet før WiFi-tilkobling. Men som en tilleggsfunksjon er det funksjonalitet for å tilordne Senior Living appen til en offentlig og en lokal adresse til lokal alarmserveren PLAS, og dermed kan selve alarmtelefonen velge om den vil nå lokal alarmserveren PLAS via WiFi-tilkobling eller 4G mobilforbindelse.

Dette betyr at den primære adressen som brukes for å nå alarmsystemet, må være en offentlig adresse, og deretter bestemmer alarmtelefonen selv hvilken tilkoblingsmetode som er best for å opprettholde kontakten med alarmserveren.

For at dette skal være mulig, må alarmtelefonene være i stand til å koble seg til 4G mobilt internett og kunne nå den lokale alarmserveren PLAS via begge kommunikasjonsveiene på port 443 (TCP).

Ved å bruke denne funksjonen anbefaler Tellu på det sterkeste at trafikk fra alarmtelefonen til den lokale alarmserveren PLAS blir beskyttet av enten brannmurregler for filtrering av hvilke alarmtelefoner (IP-adresser) som kan nå den lokale alarmserveren eller at mobildatatrafikken er beskyttet av et såkalt "Access Point Name" (APN)

I tilfelle at alarmtelefonen registrerer at den mistet kontakten med den lokale alarmserveren PLAS via den offentlige adressen, er det også muligheten for å beholde en lokal bane til alarmserveren. Tanken bak er at alarmmappen prøver å nå alarmsystemet via WiFi-tilkoblingen på den adressen hvis den offentlige adressen av en eller annen grunn ikke kan nås.

## 5. Kommunikasjon mellom Senior Living appen og lisensserver

For at Senior Living appen skal oppdateres, må alarmtelefonen kunne kommunisere via HTTPS port 443 (TCP) mot lisensserver som er tilgjengelig i Phoniro Systems på [secure.phoniro.se](https://secure.phoniro.se)

Andre distribusjonskanaler

- Play Store
- MDM

## 6. MDM- flåtestyring av alarmtelefoner

Personalet håndterer alarmene i en app på en mobiltelefon.

Tellu har en liste for Certified Devices som kontinuerlig oppdateres over hvilke mobiltelefoner som er testet for å fungere med Phoniro 6000 og også hvilke versjoner av mobiltelefonoperativsystemet som er verifisert for å fungere i systemet. Det er viktig å administrere mobiltelefonene via en såkalt. Mobile Device Management (MDM) verktøy for å forhindre utilsiktet oppgradering av det mobile operativsystemet til versjoner som ikke er testet for å fungere med systemet.

## 7. Radiomottakere Neat D-TECT-IP

Radiomottakere D-Tect IP fra Neat drives som standard via nettverket ved hjelp av Power over Ethernet [PoE]. Skulle det ikke være tilgjengelig, kan det suppleres med 230V adapter som da krever 230V ved plassering av radiomottaker.

### 7.1 Kommunikasjon mellom radiobase og lokal alarmserver PLAS.

Alarmer sendes fra alarmentheter (for eksempel alarmknapper) via radio (869 MHz) til radiomottakere på boligen som overfører alarmen på det lokale subnett til den lokale alarmserveren.

Når radiobasene startes, tildeles de en DHCP-adresse og lager deretter en UDP multi-cast på port 12150 i nettverket med sikte på å etablere kontakt med den lokale alarmserveren automatisk. Det er derfor viktig at radiobaser installeres i et eget subnett sammen med den lokale alarmserveren. Dette for å sikre at radiobasene bare kan kontakte sin lokale alarmserver.

For å kunne sende kommandoer, konfigurasjon og starte radiomottakeren om nødvendig, må alarmserveren være i stand til å kommunisere med radiobasene på port 12160 (TCP).

## **7.2 Kommunikasjon mellom radiobase D-TECT-IP og Phoniro 600 SCAIP reciver.**

Som standard drives D-TECT-IP-radiomottakere via alarmentnettverket ved hjelp av Power over Ethernet [PoE] Alarmmeldinger sendes mellom Phoniro 6000 SCAIP-mottakeren og radiomottakeren i port 7650

## **7.3 Kommunikasjon mellom inngangsmoduler og lokal alarmserver PLAS.**

Det er mulig å koble inngangsmoduler til Phoniro 6000. Inngangsmodulen tildeles en DHCP-adresse ved oppstart og konfigureres deretter for å sende alarmhendelser til den lokale alarmserveren.

Inngangsmodulene kommuniserer bare med den lokale alarmserveren i det lokale subnett port 502 (TCP / UDP).

## **7.4 Kommunikasjon mellom serieprotokollinterface og lokal alarmserver PLAS.**

Det er mulig å koble det serielle protokollgrensesnittet til Phoniro 6000. Dette gjøres for eksempel via RS232 seriell protokoll ESPA-444 når brannalarmvisning er ønsket i alarmtelefonene. Det serielle protokollgrensesnittet er tildelt en DHCP-adresse ved oppstart og deretter konfigurert til å sende alarmindikasjoner til den lokale alarmserveren.

Det serielle protokollgrensesnittet kommuniserer bare med den lokale alarmserveren i det lokale subnett port 4001 (TCP / UDP).

# **8. NTP server & Remote**

## **8.1 NTP.**

For å sikre at alarmtelefoner, den lokale alarmserveren og Phoniro Care har samme tidsinnstillinger, er NTP på port 123 (UDP) nødvendig. Enten fra en NTP-server i IT-miljøet der alarmsystemet er installert eller en offentlig på internett.

## **8.2 Remote.**

For at Tellu og Phoniro Systems skal kunne utføre service og support, er det nødvendig at support- og serviceteknikere har mulighet for ekstern tilkobling til den lokale alarmserveren.



Som standard er en Team Viewer-vert installert på den lokale alarmserveren og installert i forbindelse med introduksjonen av Phoniro 6000. For å aktivere ekstern tilkobling via Team Viewer må følgende port åpninger nødvendige for utgående trafikk til Internett

- Port 5938 (TCP / UDP) - Brukes som den primære kommunikasjonsporten
- Port 443 (TCP) - Brukes som en sekundær kommunikasjonsport

Hvis en annen type ekstern tilkoblingsløsning skal brukes, er det nødvendig med koordinering mellom Tellu og nettverksleverandøren. Men det kreves da at Tellu og Phoniro Systems kan koble seg til RDP på port 3389 (TCP) til den lokale alarmserveren.

## 9. Tale I Phoniro 6000

### 9.1 Kommunikasjon mellom trygghetsalarm Novo og Phoniro 6000.

Det er mulig å bruke trygghetsalarmen Neat Novo som støtter SCAIP-protokollen i Phoniro 6000. Alarmmeldinger sendes mellom Phoniro 6000 SCAIP-mottakeren og sikkerhetstelefonen i port 7650 Når tale forbindelse skal startes til trygghetsalarmen, kan dette gjøres enten via GSM-anrop eller som en samtale via SIP. I tilfelle der SIP skal brukes, kreves det at trygghetsalarmen må være registrert som SIP-bruker i en IP-PBX, og det er mulig å ringe fra alarmtelefonen via IP-PBX til trygghetsalarmen.

### 9.2 Kommunikasjon mellom trygghetsalarm Novo og CMP.

Det er mulig å koble trygghetsalarmen NOVO til en sentral portal for trygghetsalarmer kalt CMP [Carhone Management Portal]. Hvis dette er gjort, kan trygghetsalarmen konfigureres, oppdateres og overvåkes eksternt.

For å få denne funksjonen, er det nødvendig med utgående trafikkåpninger i henhold til:

Pprt	Adress	Funktion
Port 8080 (TCP)	iot-cmp.neat-cloud.com	Konfiguration och ev. heartbeat
Port 123 (UDP)	ntp1.sptime.se och ntp3.sptime.se	Synkronisering av tid
Port 30777 (TCP)	ftp-novo.neat-group.com	Uppdatering av mjukvaran

## 10. Kamera tilsyn ved alarm

### 10.1 Kommunikasjon mellom kamera og videotjenesten.

Kameraene har en ruter som støtter tilkobling via fast nettverksport.

Når du bruker fastnettport, brukes port 1194 (TCP) for å nå Phoniros sentrale tjeneste "serv005.phoniro.se" og VPN-tilkoblingen er av typen OVPN.

### 10.2 Kommunikasjon mellom Senior Living appen og videotjenesten.

For at alarmmappen skal kunne vise videostrømmen fra et kamera, må den kunne koble seg til den sentrale videotjenesten "serv004.phoniro.se" på port 19081 (TCP)

## 11. Batteri backup / UPS

Tellu anbefaler å sikre at pasientvarslingssystemet fungerer i tilfelle strømbrudd, det anbefales at alle komponentene i pasientvarslingssystemet som er tilknyttet nettverket drives av en UPS / Battery backup.

## 12. Port oversikt

From	To	Protocol	Port	Usage
PLAS	Phoniro CARE	TCP	443	Webgrensesnitt
PLAS	Phoniro CARE	TCP	80	Webgrensesnitt
PLAS	Phoniro CARE	TCP	443	Phoniro CARE API
Senior Living	Phoniro CARE	TCP	443	WiFi mot Phoniro CARE API
Senior Living	PLAS	TCP	8080	I tillegg må Push meldinger aktiveres
4G	PLAS	TCP	443	APN
Senior Living	Phoniro CARE	TCP	443	Lisensserver
D-Tect-IP	PLAS	TCP/UDP	12150	DHCP Multicast(UDP) TCP kommunikasjon PLAS –D-Tect-IP
D-Tect-IP	SCAIP	TCP	7650	Kommunikasjon D-Tect-IP SCAIP reciver(PLAS)
CMS	PLAS	TCP/UDP	502	CMS kommunikasjon mot PLAS
MOXA	PLAS	TCP/UDP	4001	ESPA- serielt grensesnitt
PLAS	NTP	TCP	123	Klokkesync, Senior Living, PLAS-Phoniro CARE
Team Viewer	PLAS	TCP/UDP	5398	Brukes som den primære kommunikasjonsporten
Team Viewer	PLAS	TCP	443	Brukes som en sekundær kommunikasjonsport

Anne type remote	PLAS	RDP	3389	Ekstern tilkoblingsløsning
Fastnett-router*	Videotjenesten - serv005.phoniro.se	TCP	1194	VPN-tilkoblingen er av typen OVPN
Senior Living*	Videotjenesten - serv004.phoniro.se	TCP	19081	Vise video strømmen fra et kamera Utgående trafikk på

\*Mer detaljert informasjon –kameratilsyn.

40.114.218.250 DNS serv004.phoniro.se **168.63.15.183**

52.174.35.151 DNS serv005.phoniro.se

Port 19081 må åpnes for utgående trafikk mot adressen <https://serv004.phoniro.se> Den underliggende IP-adressen kan endres så det er viktig å ikke låse brannmur mot selve IP-adresse.

Portåpning av 1194(TCP) åpnes mot adressen serv005.phoniro.se. Fastnett ruterer bruker VPN-forbindelsen av type OVPN. Den underliggende IP-adressen kan endres så det er viktig å ikke låse brannmur mot selve IP-adressen. Åpnes for utgående trafikk.

### 13. Telefon innstillinger

For at Android-telefoner skal fungere tilfredsstillende, må hver telefon konfigureres slik at batteribesparelser og oppdateringer deaktiveres. Fire innstillinger er nødvendige for å utføre. De kan finnes forskjellige steder i brukergrensesnittet, avhengig av valg av telefonmodell.

Det er også et eget dokument som beskriver disse innstillingene mer i dybden for forskjellige versjoner av Android.

Eksempler: Kan avvike ut i fra hvilken modell, eksempel er tatt ut i fra Samsung Xcover 4

1. Behold WiFi i hvilemodus
  - a) Gå til Innstillinger – Tilkoblinger-WiFi
  - b) Velg WiFi
  - c) Velg Avansert
  - d) Slå av « Slå på Wi-Fi automatisk»
2. Slå av "Smart Network Switching" / "Adaptive Wi-Fi" –funksjon
  - a) Gå til Innstillinger – Tilkoblinger-WiFi
  - b) Klikk på avansert
  - c) Slå av «Bytt til mobildata» og «Slå på Wi-Fi automatisk
3. Deaktiver strømsparingsmodus
  - a) Gå til Innstillinger –Enhetsvedlikehold-Batteri-innstillinger

- b) Innstillinger for strømoptimalisering- slå av
- c) Gå til Innstillinger –Enhetsvedlikehold-Batteri
- d) Strømodus- Skal være optimalisert

#### 4. Deaktiver optimalisering av batteribruk for Senior Living-appen

- a) Gå til Innstillinger – Apper-Velg alle
- b) Søk etter Senior Living appen
- c) Gå til batteri
- d) Gå til optimaliser batteribruk
- e) Velg alle
- f) Søk etter Senior Living appen
- g) Slå av batteri optimalisering
- h) Logg på Senior Living appen- skal da ikke komme advarsel om batteri optimalisering.

#### 5. Deaktiver automatiske oppdateringer

- a) Gå til Innstillinger –Programvareoppdateringer
- b) Slå av Last ned automatisk over Wi-Fi

## Mobildata

Som standard skal mobildata være slått av.

Hvis tilleggsfunksjonen "Sekundær bane via mobilt internett til den lokale alarmserveren" brukes, må mobildata være slått på.

## Automatiske oppdateringer

Automatiske oppdateringer bør slås av.

Gå gjennom telefonene slik at de ikke er innstilt på å laste ned nye oppdateringer automatisk. For å gjøre dette, klikker du på telefonen til: Innstillinger -> Programvareoppdatering og sørg for at "Last ned oppdateringer automatisk" er slått av. (Det kan avvike hvor du angir dette avhengig av telefonmodell).