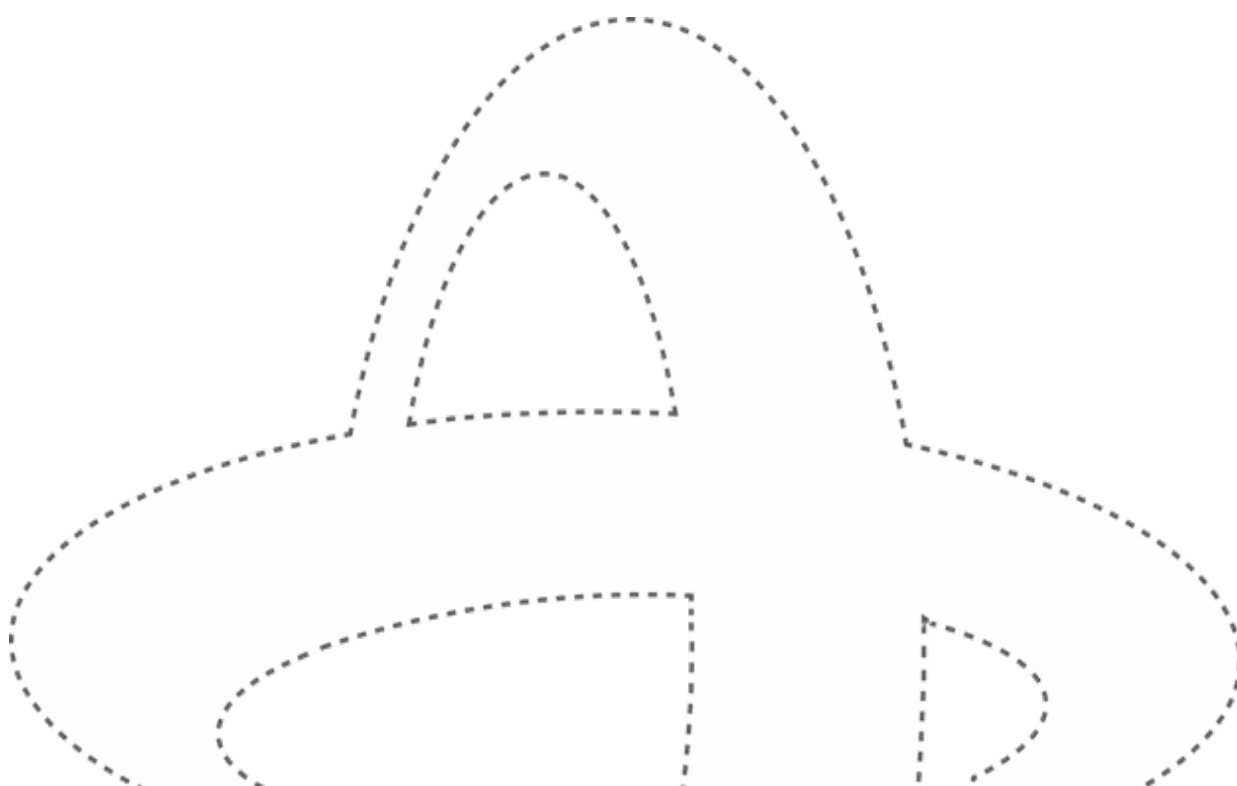


BRUKERHÅNDBOK

nCommand Lite v2.2



Innhold

Kapittel 1	Innledning	4
Seksjon 1.1 -	Formål	4
Seksjon 1.2 -	Ordliste	4
Seksjon 1.3 -	Beskrivelse	5
1.3.1.	Tiltenkt bruk	5
1.3.2.	Indikasjoner for bruk	5
1.3.3.	Tiltenkt pasientpopulasjon	6
1.3.4.	Bruksmiljø	6
1.3.5.	Kontraindikasjoner	6
1.3.6.	Plattformegenskaper	6
1.3.7.	Klinisk nytte	7
1.3.8.	Tiltenkte brukere	7
1.3.9.	Driftsmiljø	7
1.3.10.	Institusjonsmiljø	8
1.3.11.	Minimumskrav	9
1.3.12.	Symboler	11
1.3.13.	Levetid	11
1.3.14.	Oppgradering/oppdatering	12
Kapittel 2	Liste over generelle advarsler og forholdsregler	13
Kapittel 3	Bruk av plattformen på hvert sted	16
Seksjon 3.1 -	Tilgang til og bruk av nCommand Lite	16
Seksjon 3.2 -	Få tilgang til plattformen for første gang	16
3.2.1.	Logg inn via nCommand Lite	17
3.2.2.	Logg inn via ekstern IdP	18
Seksjon 3.3 -	Passordhåndtering	19
Seksjon 3.4 -	Tilgang med Lokal-teknolog-profil	23
Seksjon 3.5 -	Tilgang med Ekstern-teknolog-profil	26
3.5.1.	Tilgangsmodus	26
3.5.2.	Strømmelinje	29
3.5.3.	Flere kameraer	32
3.5.4.	Åpne en annen enhet	34
Seksjon 3.6 -	Chat	36
Seksjon 3.7 -	Avslutte økten på plattformen	38

Seksjon 3.8 -	Operativ trening	41
Seksjon 3.9 -	Retningslinjer for feilsøking	42
Seksjon 3.10 -	Rengjøringsmetoder for maskinvare	46
Kapittel 4	Cybersikkerhet og personvern	47
Seksjon 4.1 -	Sikkerhets- og personvernrisikoer	47
Seksjon 4.2 -	Personvern (GDPR / HIPAA Compliance).....	47
Seksjon 4.3 -	Tilgangsbehandling og autentisering	48
Seksjon 4.4 -	Datasikkerhet og integritet.....	48
Seksjon 4.5 -	Respons til sikkerhetshendelser	48
Kapittel 5	Servicekanaler.....	50
Kapittel 6	Juridisk og regulatorisk informasjon	51
Kapittel 7	Revisjonshistorikk.....	53

**FORSIKTIG**

Føderal lov begrenser denne enheten til salg til en lege som som er lisensiert i delstaten der han/hun praktiserer.
(gjelder for USA)

**FORSIKTIG**

I Brasil er denne programvaren autorisert av Anvisa for bruk utelukkende sammen med en magnetisk resonanstomografi (MR)-enhet. Annen bruk er ikke tillatt.
(for bruk i Brasil)

**FORSIKTIG**

Før bruk må du sørge for at du er klar over de spesifikke kravene i landet eller regionen der du holder til. Manglende overholdelse av forskrifter kan føre til helserisiko.

**FORSIKTIG**

Sørg for at versjonen av denne brukerhåndboken samsvarer med versjonen av plattformen som brukes. Bruk av en versjon som ikke samsvarer, kan føre til feil bruk eller feiltolkning av funksjoner.

Kapittel 1 Innledning

Seksjon 1.1 - Formål

Denne håndboken har som mål å gi lokale og eksterne teknikere en omfattende forståelse av de spesifikke funksjonene til nCommand Lite-systemet. Dette dokumentet fungerer som en brukerhåndbok og gir kortfattet og praktisk informasjon som veileder brukerne gjennom systemets funksjoner og feilsøking. Ved å følge denne håndboken vil brukerne kunne bruke nCommand Lite effektivt, noe som bidrar til å maksimere produktiviteten og redusere avhengigheten av teknisk støtte.

Seksjon 1.2 - Ordliste

**FORSIKTIG**

Dette symbolet gjelder for forhold eller handlinger som utgjør en potensiell fare. Du kan forårsake mindre personskader eller materielle skader hvis du ignorerer disse instruksjonene.

**ADVARSEL**

Dette symbolet identifiserer forhold eller handlinger som fører til en bestemt fare. Du vil forårsake alvorlig personskade eller betydelig materiell skade hvis du ignorerer disse instruksjonene.

Plattformbegrep	Tilsvarende begrep
Bildebehandlingsanlegg	Medisinsk institusjon, enhet, mobile enheter, helseinstitusjon, helseenhet
Ekstern institusjon	Ekstern arbeidsstasjon, eksternt sted, eksternt kontor, kommandosenter
Plattform	nCommand Lite-nettapplikasjonen
System	nCommand Lite med alle delsystemer / alt tilbehør (e-KVM, kamera)
Innretning	Medisinsk skanner, skanner, utstyr, medisinsk utstyr, bildebehandlingsenhet, bildebehandlingsutstyr
Lokal-teknolog	Lokal bruker, Lokal-teknolog, lokalt helsepersonell (LHP), bruker på stedet

Seksjon 1.3 - Beskrivelse

nCommand Lite-systemet er en SaMD (programvare som medisinsk utstyr) som er kunderettet og gir ekstern tilgang via en nettapplikasjon for visning/gransking av bilder, samt mulighet for eksternt å gi veiledning i sanntid til den pasientnære autoriserte teknikeren (den lokale brukeren) som betjener de medisinske avbildningsenhetene i forbindelse med opplæring eller prosedyrevurdering for MR-, CT- og PET/CT-skannere.

Eksterne brukere er autoriserte teknikere som kan få tilgang til en medisinsk avbildningsenhet fra en datamaskin som oppfyller minimumskravene til spesifikasjoner, hvor som helst, ved hjelp av en sikker programvareforbindelse som strømmet video og har tilgang til tastatur og mus. Dette gjør det mulig for eksterne brukere å hjelpe lokale brukere uten at avstand er en begrensning. Denne tilgangen må gis av den lokale brukeren som bruker systemet, og den kan også trekkes tilbake når som helst av den lokale brukeren, slik at han/hun kan opprettholde fullstendig kontroll over økten til enhver tid. Hver eksterne økt kontrolleres også via en sikker påloggingsinformasjon som administreres av den lokale brukeren. Tilkoblinger til medisinsk utstyr er begrenset til én ekstern økt om gangen for å opprettholde streng kontroll over hvem som samhandler eksternt med systemet. Bilder som granskes eksternt, er ikke til diagnostisk bruk.

nCommand Lite-systemet består av en IT-maskinvare- og programvarebasert installasjonsløsning som støtter flere økter, slik at eksterne teknikere kan få tilgang til flere medisinske bildediagnostiske enheter etter behov. Skannere som er kompatible med nCommand Lite-systemet, samsvarer med en felles protokoll, noe som muliggjør administrasjon av skanneparametere og ekstern skanning.

1.3.1. Tiltenkt bruk

nCommand Lite-systemet gir ekstern tilgang for visning/gransking av bilder samt mulighet til å gi ekstern veiledning i sanntid til den autoriserte teknikeren som bruker skanneren. Denne veiledningen inkluderer opplæring, prosedyrevurdering og håndtering av skanneparametere.

1.3.2. Indikasjoner for bruk

nCommand Lite-systemet gir ekstern tilgang for visning/gransking av bilder samt mulighet til å gi ekstern veiledning i sanntid til den autoriserte teknikeren som bruker en kompatibel MR-, CT-

eller PET/CT-skanner. Denne tilgangen må gis av den lokale autoriserte teknikeren som bruker systemet. Ekstern tilgang er bare tilgjengelig for systemer som støtter mulighet for ekstern tilkobling. Bilder som granskes eksternt, er ikke til diagnostisk bruk.

1.3.3. Tiltent pasientpopulasjon

For enhver pasient som er foreskrevet å gjennomgå avbildning via en tilkoblet medisinsk avbildningsenhet.

1.3.4. Bruksmiljø

Bildeinstitusjoner som utfører undersøkelser med magnetresonanstomografi (MR), computertomografi (CT) og positronemisjonstomografi – computertomografi (PET/CT), og eksterne kommandosentre.

1.3.5. Kontraindikasjoner

Plattformen skal ikke brukes av brukere som ikke er autoriserte teknikere, og som ikke har fått opplæring i bruk av nCommand Lite.

1.3.6. Plattformegenskaper

- **Ekstern skanning:** Viser skjermbildet til en medisinsk avbildningsenhet i sanntid, slik at en ekstern autorisert tekniker kan delta på en undersøkelse.
- **Chat:** Gjør kommunikasjon tilgjengelig mellom eksterne og lokale autoriserte teknikere via tekst- og talemeldinger. Lokale og eksterne teknikere kan også foreta og motta tale- og videoanrop.
- **Flere kameraer:** Tilrettelegger for ekstern observasjon av pasienter og helseinstitusjonen under prosedyren. Den eksterne teknikeren kan få tilgang til kameravisningen via fanene som er delt mellom alle kamerafanene og de individuelle. Denne mekanismen replikerer den visuelle oversikten helsepersonell ville ha hvis vedkommende var plassert nær pasienten, og introduserer dermed et forsterket sikkerhetslag.
- **Ekstern skanning med flere økter** gjør det mulig for den eksterne teknikeren å få tilgang til flere medisinske avbildningsenheter etter behov.
- **Tilgangsmodus:** lar den eksterne teknikeren velge mellom visninger eller å styre enheten. I modusen View (Vis) kan eksterne teknikere bare se det som strømmes. I modusen Control (Kontroll) har han/hun kontroll over musen og tastaturet.
- **Administrer tilgang for Ekstern-teknolog:** gjør det mulig for den lokale teknikeren å kontrollere den eksterne teknikerens tilgang og vedkommendes tilgangsmodus (View [Vis] eller Control [Kontroll]). For at den eksterne teknikeren skal kunne koble seg til, må den lokale teknikeren som bruker plattformen, gi tilgang, og den kan også trekkes tilbake når som helst av den lokale teknikeren, slik at han/hun kan opprettholde fullstendig kontroll over økten til enhver tid.
- **Strømmestørrelse:** Den eksterne teknikeren kan se den opprinnelige strømmestørrelsen og den gjeldende strømmestørrelsen i piksler. Han/hun varsles også når den gjeldende strømmestørrelsen er mindre enn originalen.
- **Status for mus og tastatur:** Den eksterne teknikeren får tilbakemelding om musen og tastaturet til den medisinske avbildningsenheten fungerer som de skal.

- **Øktdetaljer:** Den lokale og eksterne teknikeren har tilgang til detaljer om økten.

1.3.7. Klinisk nytte

nCommand Lite forbedrer diagnostisk avbildning ved å muliggjøre ekstern styring av **MR-, CT- og PET-CT-systemer**, noe som sikrer konsistent avbildningskvalitet og overholdelse av protokoller. Det gjør det mulig for erfarne teknikere å overvåke og bistå med skanninger i sanntid, optimalisere arbeidsflytens effektivitet og redusere feil som kan påvirke diagnostisk nøyaktighet. Systemet tilrettelegger for samarbeid mellom teknikere, forbedrer undersøkelseskonsistens og gjør det mulig å ta raskere beslutninger i komplekse tilfeller. Ved å gjøre det mulig for eksterne fagpersoner å støtte flere institusjoner øker **nCommand Lite tilgjengeligheten, variasjonen og kvaliteten** på avbildningsundersøkelser, slik at flere pasienter får tilgang til avansert diagnostikk samtidig som helsetjenesteressurser optimaliseres. I tillegg bidrar det til å redusere personalmangel ved å redusere avhengigheten av spesialister på stedet, samtidig som overholdelse av strenge regulatoriske standarder og datasikkerhetsstandarder opprettholdes.

1.3.8. Tiltente brukere

- **Lokal-teknolog**

Den lokale teknikeren er brukeren på stedet som er ansvarlig for å bistå og veilede pasienter personlig på helseinstitusjonen. Han/hun må ha den nødvendige kunnskapen til å utføre skanneprosedyrer for en gitt avbildningsenhet. I tillegg kontrollerer han/hun den eksterne teknikeren tilgangsmodus (View [Vis] eller Control [Kontroll]), og ekstern tilgang må gis av den lokale teknikeren via plattformen og kan trekkes tilbake når som helst.

- **Ekstern-teknolog**

En fagperson som utfører operasjoner eksternt, med tilgang til og kontroll over enhetens datamaskin. I likhet med den lokale teknikeren må den eksterne teknikeren også ha den nødvendige kunnskapen til å utføre skanneprosedyrer for en gitt avbildningsenhet.

- **Støtte-/IT-bruker**

Fagperson som er ansvarlig for å sette opp plattformen (ikke inkludert i denne brukerhåndboken).

1.3.9. Driftsmiljø

Følgende spesifikasjoner gjelder miljøkravene til e-KVM-datamaskinen.

- **Maksimal høyde over havet (uten trykksetting)**

- o Drift: Fra 0 m (0 fot) til 3048 m (10 000 fot)
- o Lagring: Fra 0 m (0 fot) til 12 192 m (40 000 fot)

- **Temperatur**

- o Drift: Fra 10 °C (50 °F) til 35 °C (95 °F)
- o Lagring: Fra -10 °C (14 °F) til 50 °C (122 °F)

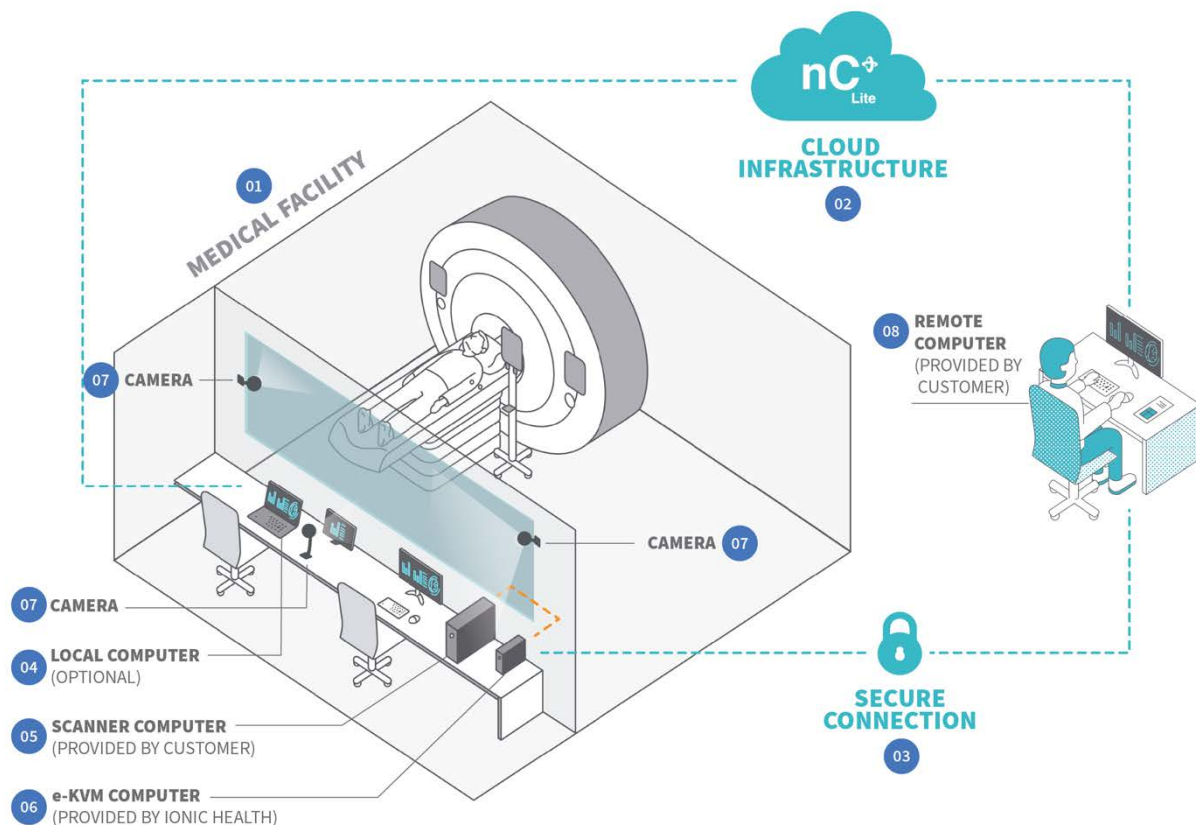
- **Relativ fuktighet**

- o Drift: 20–80 % (ikke-kondenserende)
- o Lagring: 10–90 % (ikke-kondenserende)

1.3.10. Institusjonsmiljø

nCommand Lite-plattformen har to forskjellige typer miljøplassering:

- **Bildebehandlingsenhet:** Institusjoner som utfører undersøkelser med magnetresonanstomografi (MR), computertomografi (CT) eller positronemisjonstomografi – computertomografi (PET/CT).
- **Ekstern institusjon:** Et sted hvor eksterne teknologer kan få tilgang til og eksternt administrere enheter (MR-, CT- eller PET/CT-skannere). Denne arbeidsstasjonen kan brukes i ulike miljøer som kontorer, kommandosentre, eksterne steder eller til og med sekundære steder i helseinstitusjonen. Den eksterne arbeidsstasjonen kan plasseres i ethvert rom som gir brukeren passende forhold for konsentrasjon og minimumstilkobling, og krav til datamaskinkonfigurasjon.



Figur 01: Oversikt over produktet og dets tilkoblinger gjennom en sikker forbindelse (f.eks. VPN).
 01 – Helseinstitusjon; 02 – Skyinfrastruktur; 03 – Sikker forbindelse; 04 – Lokal datamaskin (valgfritt tilbehør); 05 – Skannerdatamaskin (leveres av kunden); 06 – e-KVM (leveres av IONIC Health);
 07 – Kamera; 08 - Fjernstyrt datamaskin (levert av kunden)

**ADVARSEL!****Kompatibilitet med ekstern skanning**

IONIC Health (IH) validerer funksjonaliteten for ekstern skanning på de oppførte kompatible enhetene. IH gjennomfører en fullstendig vurdering av IHs krav til ekstern skanning og tester systemet i målmiljøet under installasjonen. Dette sikrer kompatibilitet og riktig ytelse på det aktuelle tidspunktet for ekstern skanning. Denne verifiseringen innebærer ikke at alle OEM-enhetskrav (Original Equipment Manufacturer) er oppfylt i denne konfigurasjonen. Ethvert avvik fra OEM-kravene er sluttbrukerens ansvar.

Endringer i systemet eller miljøet etter installasjon må rapporteres til IH for å bekrefte fortsatt kompatibilitet. IH kan ikke garantere ytelse eller påta seg ansvar for konfigurasjoner som er forskjellige fra de som ble validert under installasjonen.

1.3.11. Minimumskrav

□ Lokal datamaskin

Denne datamaskinen brukes av **Lokal-teknolog** for å autorisere og støtte ekstern tilgang til enheten gjennom nCommand Lite®. Den tillater også direkte kommunikasjon med **Ekstern-teknolog** via chat-funksjonen på plattformen.

De tekniske minimumskravene er:

- o Prosessor: AMD® A4-9120C eller bedre, eller tilsvarende
- o Minne: 4 GB eller mer
- o Lagring: 128 GB eller større SSD
- o Ekstrautstyr: mikrofon, høyttaler eller hodesett
- o Skjerm: 14" FHD (1920 x 1080) eller større
- o Operativsystem: Chrome OS, Windows OS eller MAC OS
- o Installasjonssted: Denne datamaskinen må være i nærheten av skannerdatamaskinen
- o IT-rutine: Lag en nCommand Lite-snarvei på alle brukernes skrivebord
- o Nettleserkompatibilitet: Google Chrome eller Microsoft Edge.
- o Statisk IP-adresse

□ Ekstern arbeidsstasjon

Denne stasjonen brukes av **Ekstern-teknolog** for å få tilgang til og kontrollere enheten via nCommand Lite®. Den eksterne arbeidsstasjonen må opprette en sikker tilkobling til e-KVM-datamaskinen (levert av IONIC HEALTH®).

Kunden er ansvarlig for å levere den eksterne datamaskinen og vil bestemme seg for ett av to scenarier: det første er døgnåpen drift, det andre er drift kun i arbeidstiden.

For hvert scenario finner du de riktige spesifikasjonene for valg av datamaskinmodeller nedenfor:

Scenario 1 (drift døgnet rundt) – Må oppfylle følgende spesifikasjoner:

- o Intel Xeon W-2223 (4 kjerner, 8 tråder, 8,25 MB hurtigbuffer, 3,90 GHz Turbo) eller bedre.
- o RAM: 16 GB eller mer.
- o Grafikk: NVIDIA RTX A2000 6GB eller bedre, eller tilsvarende.
- o Lagring: 128 GB eller større SSD.
- o Operativsystem: Windows 11 Pro 64B eller nyere.
- o Minimumskrav for skjerm: Størrelse 27", sideforhold 16:9, oppløsning 4k.
- o Hodesett: BLACKWIRE 3200 eller tilsvarende.
- o Nettleserkompatibilitet: Google Chrome eller Microsoft Edge.

Scenario 2 (drift i åpningstiden) – Må oppfylle følgende spesifikasjoner:

- o Intel® Core™ i7-12700k vPro® eller bedre.
- o RAM: 16 GB eller mer.
- o Grafikk: NVIDIA T400 GB eller bedre, eller tilsvarende.
- o Lagring: 128 GB eller større SSD.
- o Operativsystem: Windows 11 Pro 64B eller nyere.
- o Minimumskrav for skjerm: Størrelse 27", sideforhold 16:9, oppløsning 4k.
- o Hodesett: BLACKWIRE 3200 eller tilsvarende.
- o Nettleserkompatibilitet: Google Chrome eller Microsoft Edge.

**ADVARSEL!**

Hvis du ikke oppfyller de riktige kravene for oppsett og minimumskravene, kan dette føre til redusert eller mislykket kommunikasjon mellom brukere.

□ Nettverkskonfigurasjoner (minimumskrav)

For å etablere økten mellom den eksterne brukeren og e-KVM-datamaskinen, må nettverkskommunikasjon mellom de to enhetene sikres. nCommand Lite-systemet bruker peer-to-peer (P2P) for å etablere forbindelse mellom den lokale brukeren, den eksterne brukeren og e-KVM datamaskinen. Det er tre compatible scenarioer:

- o **Scenario 1** – Bedriftsnettverk som bruker en av følgende protokoller: LAN, LAN-til-LAN, MPLS eller VPN;
- o **Scenario 2** – Bedriftsnettverk som bruker pålitelig WAN (eksternt nettverk) og ikke bruker noen av følgende protokoller: LAN, LAN-til-LAN, MPLS eller VPN;
- o **Scenario 3** – Offentlig nettverk på den eksterne datamaskinsiden (ekstern bruker).

Konfigurasjonene for hvert scenario er beskrevet i den tekniske dokumentasjonen.

1.3.12. Symboler

Symbol	Beskrivelse	Referanse
	Produsent	ISO 15223-1, ISO 7000-3082
	Produksjonsdato	ISO 15223-1, ISO 7000-2497
	Symbolet indikerer at dette produktet er en medisinsk enhet	ISO 15223-1
	Unik utstyrsidentifikasjon	ISO 15223-1
	Modellreferanse	ISO 15223-1, ISO 7000-2493
	Importør	ISO 15223-1, ISO 7000-3725
	Se i brukerhåndboken	ISO 15223-1, ISO 7000-1641
	Distributør	ISO 15223-1, ISO 7000-3724
	Forsiktig	ISO 15223-1, ISO 7000-0434A
	Advarsel	ISO 7010-W001
	Serienummer (<i>eller programvareversjon</i>)	ISO 15223-1, ISO 7000-2498
	Autorisert representant i Det europeiske fellesskapet	ISO 15223-1
	Autorisert representant i Sveits (CH-REP)	ISO 15223-1
	CE – Europeisk samsvarsmerking; 2803 – Identifikasjon av teknisk kontrollorgan	EU-forordning 2017/745

1.3.13. Levetid

Produktets forventede levetid er 5 år, med hensyn til levetiden til komponentene som utgjør produktet. Denne omfattende evalueringen sikrer at hver kritiske komponents levetid samsvarer med den totale levetiden, og garanterer konsekvent ytelse og pålitelighet gjennom hele produktets tiltenkte varighet.

1.3.14. Oppgradering/oppdatering

IONIC Health vil oppdatere nCommand Lite-systemet som en del av planlagte vedlikeholds- eller oppgraderingsutgivelser. Disse oppdateringene er utformet for å sikre fortsatt ytelse og pålitelighet uten å forstyrre den nåværende utrullerte versjonen på kundeområder. Avhengig av oppdateringens art, kan produktet oppgraderes eksternt eller kan kreve et besøk på stedet av en feltingeniør.

Merk: Etter at plattformen er oppgradert, bør du tømme nettleserbufferen (se instruksjonene for nettleseren din) før du logger på den nye versjonen.

Kapittel 2 Liste over generelle advarsler og forholdsregler



ADVARSEL!

Les alle advarslene nedenfor før du bruker nCommand Lite-systemet.



FORSIKTIG

nCommand Lite-systemet kan ikke gjennomgå reparasjon eller vedlikehold mens det brukes til å kontrollere et MR-, CT- eller PET-CT-utstyr i nærvær av en pasient.

- ☐ Følg nøye med på alle systemvarsler, da de er avgjørende for trygg bruk.
- ☐ Prioriter sikkerhet og oppmerksomhet under alle operasjoner.
- ☐ Føderal lov begrenser denne enheten til salg til en lege som er lisensiert i delstaten der han/hun praktiserer.
- ☐ nCommand Lite-systemet skal kun brukes av teknikere som har fått opplæring i bruken av plattformen.
- ☐ Bruk dette systemet kun med kompatible nettlesere. Støttede nettlesere er Google Chrome og Microsoft Edge.
- ☐ I tilfelle en nødssituasjon må en opplært, autorisert tekniker bli værende på bildebehandlingsavdelingen for å styre MR-, CT- eller PET/CT-enheten uten nCommand Lite.
- ☐ Å ha tilgang til flere enheter samtidig krever intens konsentrasjon og kommunikasjon med lokale team.
- ☐ Unngå å ha tilgang til enheter med identiske oppsett eller undersøkelser av den samme anatomiske regionen samtidig.
- ☐ Du kan vise flere skjermer, men kontrollen er begrenset til én enhet om gangen.
- ☐ Innled alltid en chat når du er koblet til en enhet, for å sikre tydelig kommunikasjon.
- ☐ Anropsvarsler vises på skjermbildet til den tilknyttede enheten; kun én samtale kan være aktiv om gangen.
- ☐ Test videokommunikasjonen når du åpner applikasjonen (før begynnelsen av en arbeidsøkt) for å sjekke om det er noen feil i videoutgangsforbindelsen til MR-, CT- eller PET/CT-enhetene eller noen enhet relatert til videostrømming.
- ☐ Enheten skal ikke kobles til stikkontakten og/eller den avbruddsfrie og stabiliserte strømforsyningen gjennom skjøteledninger eller forgreininger.
- ☐ Hvis det oppstår videofeil, må du kontrollere videoforbindelsen mellom enhetssystemet og e-KVM-datamaskinen.

- Hvis applikasjonen er treg ved ekstern tilgang, oppdaterer du siden med kommandoen Ctrl+F5 i nettleseren på den eksterne teknikerens datamaskin. Kontakt teknisk støtte hvis problemet vedvarer.
- Når nettlesersiden oppdateres, avbrytes forbindelsen til enheten, noe som krever at godkjenningsprosessen utføres på nytt.
- Ikke logg på med en annen nettleser når du allerede er logget på.
- Kundens billeddiagnostiske avdeling må ha en redundant Internett-forbindelse med en annen leverandør enn hovedforbindelsen for umiddelbart bytte i tilfelle tap av kommunikasjon med systemet/plattformen.
- Ved kommunikasjonstap eller treg musepeker utfører du en «mouse resync» på siden som brukes i nettleseren.
- Sørg for at datamaskinene som brukes til styring av nCommand Lite-systemet, både på billediagnostisk anlegg og i kommandosenteret, oppfyller minimumskravene. Ellers kan applikasjonens ytelse reduseres.
- QoS (tjenestekvalitet) skal brukes på hovedforbindelsen og den redundante forbindelsen for overføring av plattformen, og forbindelsens ytelse skal overvåkes.
- Kontroller lyd- og mikrofonvolumnivåene samt lyd- og mikrofontillatelsen i nettleseren før bruk.
- Før bruk må du kontrollere funksjonen til tastaturet og musen. Hvis de er trege eller ikke synkroniserte, aktiverer du knappen «Mouse resync» (resynkroniser mus). Kontroller om e-KVM-datamaskinen er tilkoblet og slått på.
- Kontroller at tastaturopsettet på den eksterne institusjonen er identisk med tastaturopsettet hos bildebehandlingsenheten.
- Hvis serveren ikke er tilgjengelig, kontrollerer du konfigurasjonen og ytelsen.
- Hvis det er nødvendig å endre stedet der plattformen brukes, må klienten ringe teknisk støtte for å foreta en ny installasjon. Ikke installer på nytt uten å kontakte teknisk støtte.
- Før prosessen for ekstern tilgang til MR-, CT- eller PET/CT-enheten startes, er det viktig at teknikerteamene kontrollerer alle elementene som kreves for at plattformen skal fungere som den skal, slik at undersøkelsen ikke hindres. Disse elementene er oppført i dokumentet «Sjekkliste for tjenestestart».
- Bildeinstitusjonens brannmurkonfigurasjon må kontrolleres månedlig av IT-teamet for å bekrefte at det ikke er noen problemer med brannmurversjonen som kan kompromittere bruken av nCommand Lite.
- Enhver anomali som observeres ved bruk av applikasjonen, må umiddelbart varsles til støtteteamet før tilgangen startes, eller den avbrytes hvis den allerede har startet.
- Kun autoriserte teknikere med opplæring i bruk av nCommand Lite skal betjene applikasjonen.
- Ekstern tilgang via plattformen erstatter eller konkurrerer ikke med noen annen driftsprosedyre for MR-, CT- eller PET/CT-bruk som er etablert av produsenten av det medisinske utstyret, og helseinstitusjonens protokoller og prosedyrer.
- Unngå å bøye eller strekke maskinvarekablene.

- Hvis det oppstår problemer med tale- eller chattekommunikasjon, bruker du telefonanropsfunksjonen til å opprette kommunikasjon mellom den lokale teknikeren ved bildediagnostikkinstitusjonen og den eksterne teknikeren ved kommandosenteret. Følg instruksjonene som er beskrevet i avsnittet «Retningslinjer for feilsøking», og kontakt om nødvendig teknisk støtte for å utføre reparasjonen.
- Hvis det er nødvendig å skifte ut en datamaskin eller annet utstyr som direkte påvirker nCommand Lite-installasjonen, bør du aktivere teknisk støtte for å sikre at systemets drift opprettholdes.
- Bare én person kan få ekstern tilgang til MR-, CT- eller PET/CT-enheten om gangen.
- Ikke berør videotilkoblingene når enhetens datamaskin og nCommand Lite-systemet er slått på.
- Når du får tilgang til en ytterligere enhet, vil en ny fane åpnes. Dra denne fanen til en annen skjerm, siden systemet er designet for bruk med en separat skjerm for hver enhet.
- Enhver alvorlig hendelse relatert til bruken av denne enheten skal rapporteres til både produsenten og helsemyndighetene / den kompetente myndigheten der enheten er installert (se *mer informasjon i kapitlet Servicekanaler*).

Kapittel 3 Bruk av plattformen på hvert sted

Seksjon 3.1 - Tilgang til og bruk av nCommand Lite

**ADVARSEL!**

Hvis det oppstår problemer, kontakt teknisk støtte for hjelp.

**ADVARSEL!**

Kontroller tastaturopsettet og sørg for at det er identisk på begge steder (helseinstitusjon og ekstern institusjon). Ulike tastaturopsett kan hindre brukeropplevelsen.

Dette kapittelet gir deg alt du trenger å vite for å få tilgang til og begynne å bruke nCommand Lite-plattformen. Du finner enkle, trinnvise instruksjoner for å logge på, navigere i grensesnittet og forstå hovedfunksjonene. Enten du jobber på stedet eller eksternt, vil denne veiledningen hjelpe deg med å komme raskt og trygt i gang.

Endre språk – Systemet er forhåndsinnstilt til engelsk som standard, men du kan enkelt endre språket etter eget ønske. På påloggingsskjermen klikker du øverst til høyre der Engelsk (English (en-US)) vises. Dette åpner en rullegardinliste med tilgjengelige språk du kan velge mellom.

Etter pålogging kan du også endre språket ved å klikke på det valgte språket på høyre side av topplinjen. Dette åpner en rullegardinliste over tilgjengelige språk du kan velge mellom.

Vær oppmerksom på at hvis du endrer språket mens du er koblet til en enhet, vil den nåværende forbindelsen automatisk bli avsluttet, og du må koble til på nytt.

Når du går inn på plattformen, kan du velge språket du foretrekker på påloggingsskjermen. Noen meldinger som vises under påloggingsprosessen kan imidlertid vises på språket som er angitt i nettleseren din, uavhengig av språket som er valgt på plattformen. For å få en konsekvent opplevelse anbefaler vi at du justerer språkinnstillingene i nettleseren til det foretrukne plattformspråket.

Seksjon 3.2 - Få tilgang til plattformen for første gang

Påloggingsprosessen på plattformen kan gjøres på to måter: via nCommand Lite eller via en ekstern identitetsleverandør (ekstern IdP). Brukeren kan logge på ved hjelp av en av de forhåndskonfigurerte metodene. Hvis den konfigurerte metoden er External Identity Provider (External IdP), vil ikke nCommand Lite-metoden fungere, og omvendt. For å logge på via ekstern IdP, går du direkte til **underpunkt 3.2.2**.

3.2.1. Logg inn via nCommand Lite

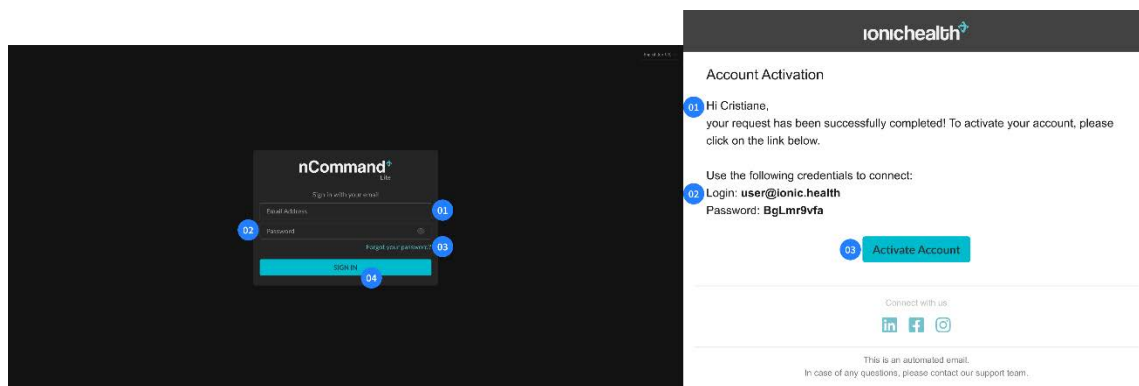
Merk: Denne delen gjelder ikke for brukere som logger på via en ekstern identitetsleverandør (ekstern IdP).

Slå på datamaskinen og dobbeltklikk på snarveiiikonet nCommand Lite, som vanligvis er på skrivebordet. Du kan også få tilgang til URL-adressen direkte i nettleseren.

Din første tilgang er et avgjørende trinn for å begynne å bruke plattformen trygt og effektivt. Her er hva du trenger å vite:

1 – Velkomst-e-post: Du vil motta en e-post med påloggingsdetaljene dine, inkludert din tilknyttede personlige e-postadresse, et midlertidig passord og en direktekobling til klientplattformen. Denne e-posten er avgjørende for å starte din reise på nCommand Lite.

2 – Opprettelse av passord: Når du åpner koblingen, må du angi din tilknyttede e-postadresse og passordet du mottok i velkomst-e-posten. Ved å klikke på «Sign in» (Logg på) blir du sendt til en side for å opprette et nytt passord. Du må angi det gamle passordet, det nye passordet og bekreftelsen av det nye passordet. Det må være sterkt og sikkert, inkludert minst tre av følgende: en liten bokstav, en stor bokstav, et tall og et symbol, og være minst åtte tegn langt. Når du klikker på «Continue» (Fortsett), blir du omdirigert til en side for å bekrefte e-postmeldingen på nytt. Når du klikker på «Continue» (Fortsett), blir du nå omdirigert til startskjermen, som tilpasses i henhold til din spesifikke brukerprofil.



Figur 02: Venstre - Påloggingsside for nCommand Lite: 01 – E-postadresse; 02 – passord; 03 – «Har du glemt passordet?»; 04 – Innloggingsknapp

Høyre - nCommand Lite velkomst-e-post mottatt etter at brukeren er registrert:

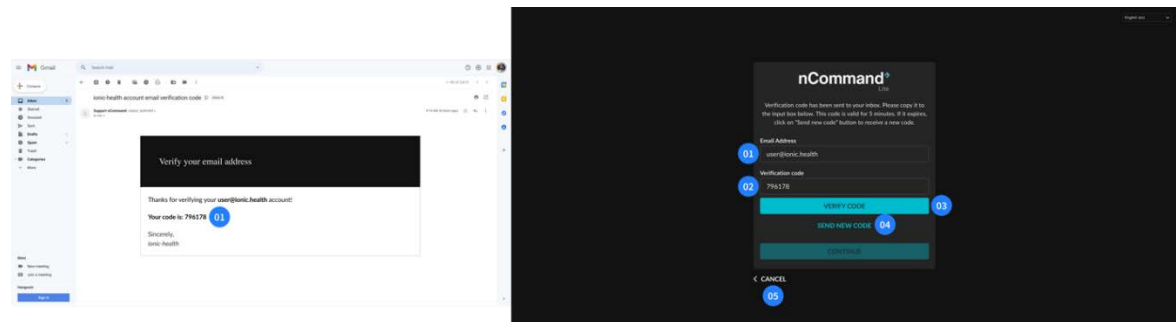
01 – E-posttekst for kontoaktivering; 02 – Påloggingsinformasjon; 03 – Knappen Activate Account (Aktiver konto)

Denne innledende prosedyren er utformet for å sikre maksimal sikkerhet for kontoen din fra starten av. Fra og med din andre tilgang vil prosessen bli effektivisert, men likevel forbli like sikker, med en tofaktorautentiseringskode sendt til din tilknyttede e-postadresse ved hver pålogging for å sikre den løpende sikkerheten til kontoen din. Denne koden vil bli forespurt igjen 12 timer etter pålogging. Hvis tidsgrensen utløper under en aktiv ekstern økt, avsluttes ikke økten, og koden blir forespurt ved neste pålogging.

Når du har logget på nCommand Lite, vil systemet automatisk ta deg til startskjermen, som tilpasses i henhold til din spesifikke brukerprofil. Enten du er en lokal eller en Ekstern-teknolog,

er grensesnittet utformet for å oppfylle behovene og tilgangen som er relevant for rollen din. Denne intuitive utformingen sikrer at du har alle verktøyene og all informasjonen som er nødvendig for en effektiv brukeropplevelse fra øyeblikket du logger på.

Merk: Når påloggingsmetoden er konfigurert som nCommand Lite, må påloggingen alltid gjøres gjennom dette alternativet. Selv om en ekstern IdP-knapp vises på påloggingsskjermen, vil den ikke fungere for disse brukerne.



Figur 03: Venstre - E-post for tofaktorautentisering (2-FA) for nCommand Lite: **01** – 2-FA-kode
Høyre – nCommand Lite-tofaktorautentiseringsside: **01** – Email Address (E-postadresse); **02** – Verification code (Bekreftelseskode); **03** – Knapp for Verify Code (Bekreft kode); **04** – Send New Code (Send ny kode); **05** – Cancel (Avbryt)

3.2.2. Logg inn via ekstern IdP

I noen tilfeller kan brukere logge på plattformen gjennom en ekstern identitetsleverandør (IdP), som lar dem bruke organisasjonens eksisterende autentiseringstjeneste, en mekanisme også kjent som Single Sign On (SSO). Med denne metoden vil den forhåndsregistrerte brukeren ikke motta en velkomst-e-post. Den lokale IT-tjenesten må sjekke kompatibilitet, konfigurere metoden og informere brukeren om hvilken e-post (ekstern IdP) som skal brukes.

Når dette alternativet er tilgjengelig, må brukeren alltid logge på med den eksterne IdP-en (f.eks. Amazon Cognito, Microsoft Entra ID, Microsoft AD B2C). Påloggingsmetoden via nCommand Lite vil ikke være tilgjengelig for eksterne IdP-brukere.

For å logge på med den eksterne IdP-en, klikker du på knappen med IdP-navnet og følger instruksjonene fra den eksterne autentisereren. Hvis institusjonen din har mer enn én ekstern IdP integrert, må du sørge for å bekrefte hvilken leverandør du er registrert hos. Andre leverandører vil ikke fungere. Hvis du har spørsmål eller støter på problemer, ta kontakt med din lokale IT-tjeneste.

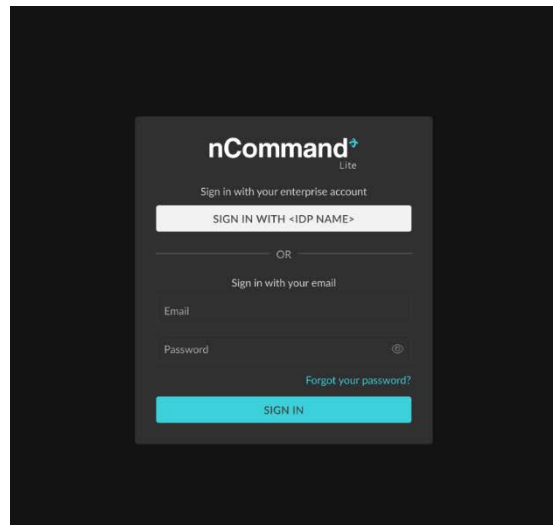
I scenarier der brukere deler samme maskin og bruker Single Sign-On (SSO), anbefales det at hver bruker velger alternativet «ikke forbli pålogget» under ekstern IdP-pålogging (hvis tilgjengelig) eller logger av den eksterne leverandøren etter å ha logget ut av nCommand Lite.

For dette påloggingsalternativet administreres hele påloggings- og utloggingsprosessen – inkludert retningslinjer for opprettelse og utløp av passord, flerfaktorautentisering (MFA) og kontolåsing – utelukkende av kundens IT-team som konfigurerte den eksterne IdP-en.

Når du logger på via ekstern IdP, må funksjonene «Glemt passord» og «Endre passord» utføres i henhold til den eksterne IdP-ens prosess.

Merk: Alternativet «Glemt passord» vil fortsatt vises på påloggingsskjermen, men det vil ikke være funksjonelt for disse brukerne. Den kan lede til de neste trinnene i prosessen, men vil ikke fullføre den. Hvis du trenger å gjenopprette passordet ditt, følger du instruksjonene fra din eksterne IdP.

Viktig: Selv når du bruker en ekstern IdP, må brukeren være forhåndsregistrert i nCommand Lite-plattformen for å få tilgang.



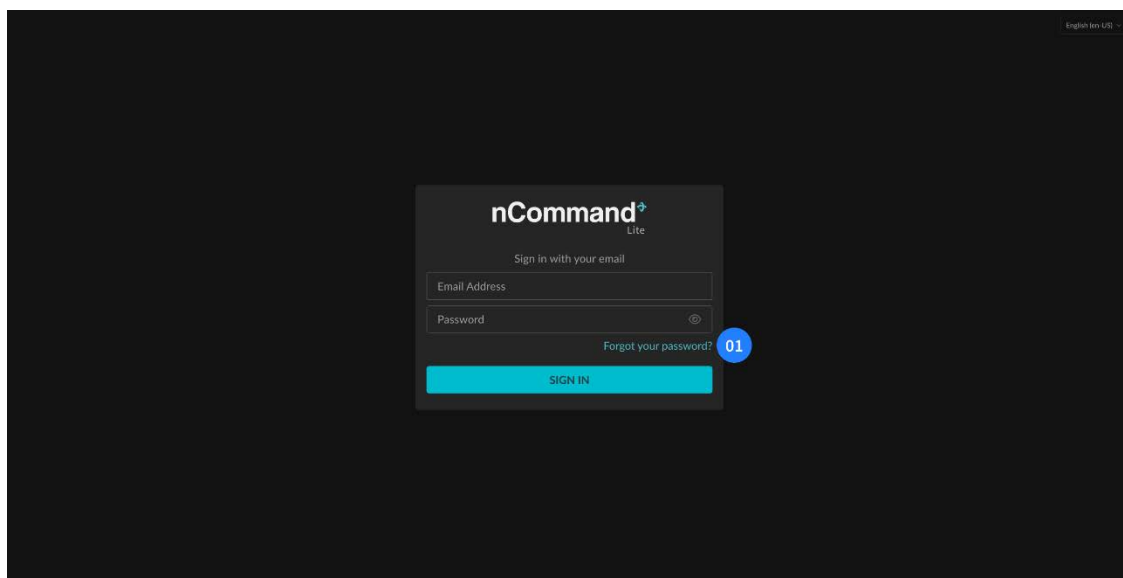
Figur 04: Eksempel på påloggingsskjerm via ekstern IdP

Seksjon 3.3 - Passordhåndtering

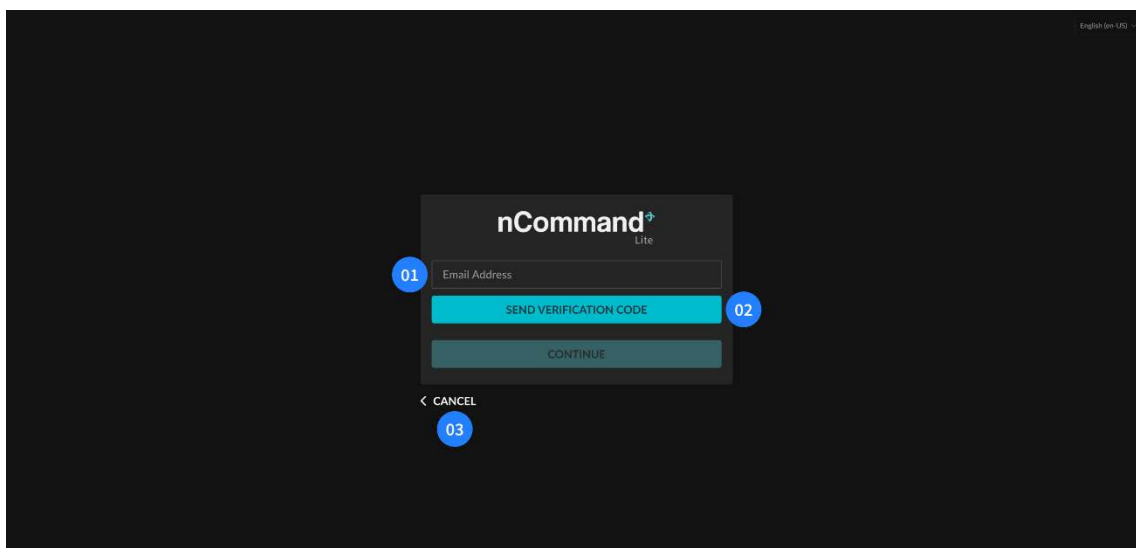
Etter å ha fått tilgang til plattformen for første gang, kan brukerne endre passordet sitt eller, hvis det ble glemt, angi et nytt passord.

Merk: Når du logger på via ekstern IdP, må funksjonene **Glemt passord** og **Endre passord** utføres i henhold til den eksterne IdP-ens prosess.

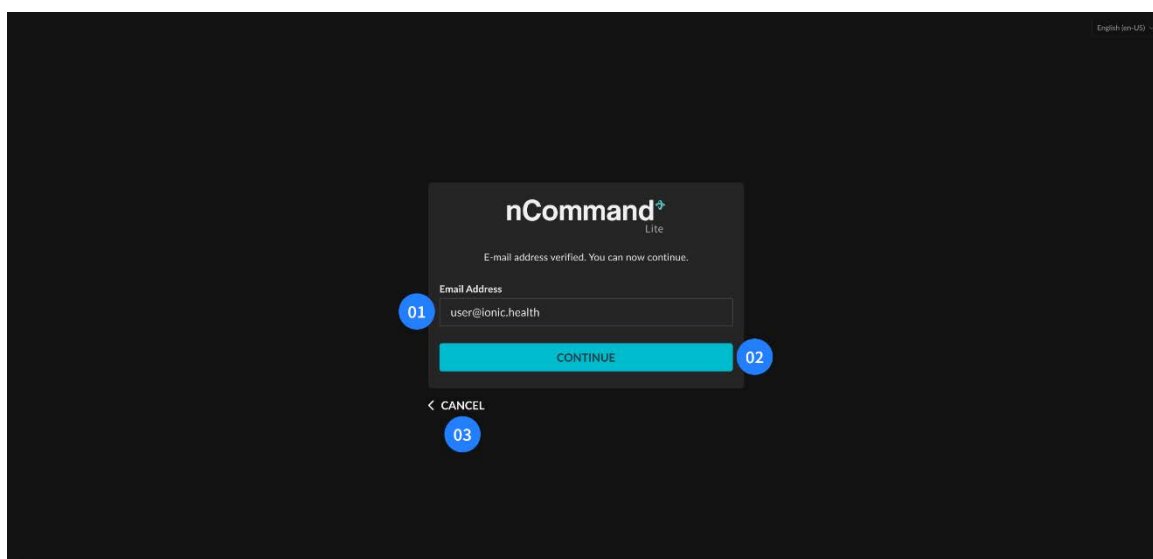
□ **Gjenopprette passord:** Gjør det mulig for brukere å gjenopprette kontotilgang hvis vedkommende glemmer passordet sitt. Klikk på lenken «Forgot your password?» på innloggingssiden, oppgi den tilhørende e-postadressen og send inn informasjonen. Systemet vil deretter sende en e-post med en verifiseringskode. Når brukerne angir koden og klikker på «Verify code» (Bekreft kode), blir de bedt om å bekrefte den tilknyttede e-posten. Ved å klikke på «Continue» (Fortsett) blir brukerne sendt til en side hvor de kan skrive inn et nytt passord og bekreftelse av det nye passordet. Hvis det nye passordet oppfyller systemkravene, kan brukerne registrere det og deretter logge på med den oppdaterte påloggingsinformasjonen.



Figur 05: Kobling til side for tilbakestilling av passord for nCommand Lite
01 – Forgot your password? (Har du glemt passordet?)

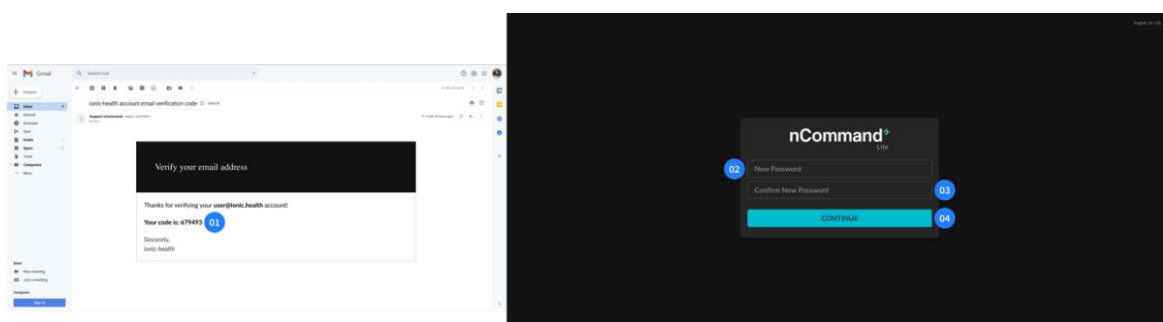


Figur 06: Side for tilbakestilling av passord for nCommand Lite
01 – Email Address (E-postadresse); **02** – Send Verification Code (Send Bekreftelseskode); **03** – Cancel (Avbryt)



Figur 07: E-postbekreftelse i nCommand Lite

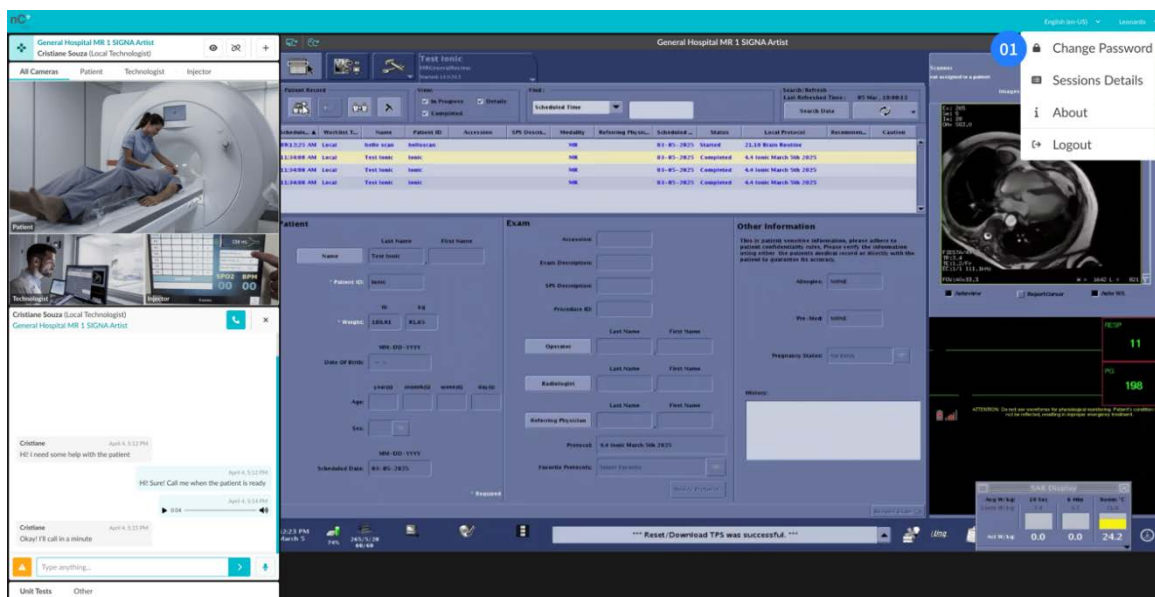
01 – Email Address (E-postadresse); **02** – Knappen Continue (Fortsett); **03** – Cancel (Avbryt)



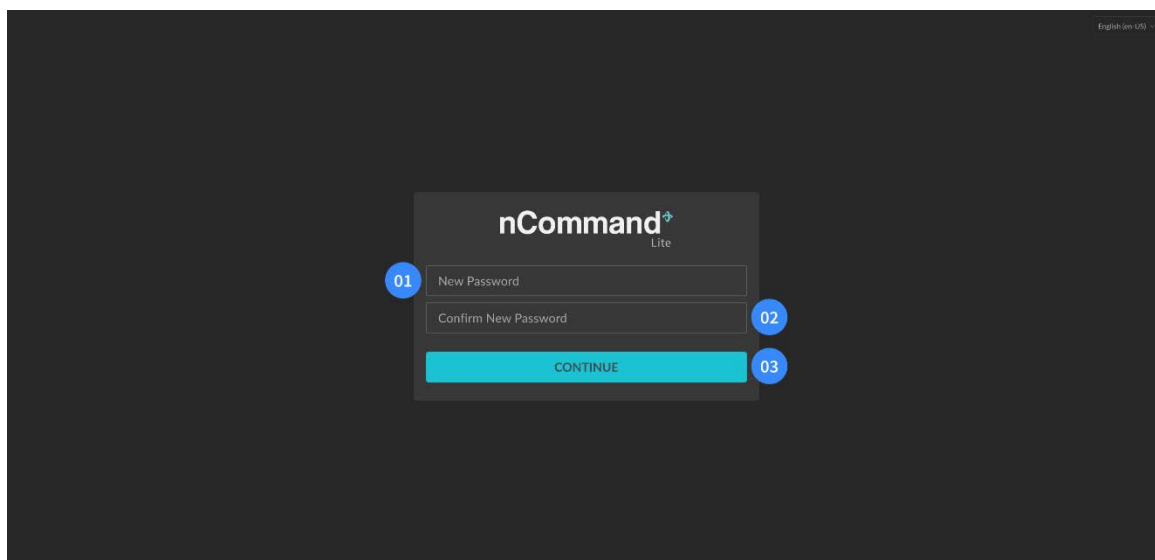
Figur 08: E-post med kode for å registrere nytt passord for nCommand Lite (venstre) og siden for endring av passord for nCommand Lite (høyre)

01 – 2-FA-kode; **02** – New Password (Nytt passord); **03** – Confirm New Password (Bekreft nytt passord); **04** – Knappen Continue (Fortsett)

□ **Change Password (Endre passord):** Lar brukerne oppdatere passordet sitt ved å følge spesifikke kriterier, inkludert minst tre av følgende: en liten bokstav, en stor bokstav, et tall og et symbol, og være minst åtte tegn langt. Systemet kontrollerer om det nye passordet oppfyller disse kriteriene, og gir brukeren en melding hvis det ikke gjør det. Brukerne må også bekrefte det nye passordet for å unngå inntastingsfeil. For å endre passordet må brukeren etter påloggingsprosessen klikke på ikonet øverst til høyre og velge menyen «Change Password» (Endre passord). Han/hun vil bli koblet fra plattformen og sendt til en side for å bekrefte den tilknyttede e-postadressen. Systemet vil deretter sende en e-post med en verifiseringskode. Når brukerne angir koden og klikker på «Verify code» (Bekreft kode), omdirigeres de til et skjermbilde der de kan angi et nytt passord.



Figur 09: Kommandoen Change Password (Endre passord) på rullegardinmenyen i nCommand Lite
01 – Change Password (Endre passord)



Figur 10: Side for endring av passord i nCommand Lite
01 – New Password (Nytt passord); 02 – Confirm New Password (Bekreft nytt passord);
03 – Knappen Continue (Fortsett)

Seksjon 3.4 - Tilgang med Lokal-teknolog-profil

**ADVARSEL!**

Før du bruker plattformen, må du kontakte den eksterne teknikeren på telefon.

**ADVARSEL!**

For å unngå overoppheting må du ikke plassere noen gjenstander foran luftkjøleren på e-KVM-datamaskinen, og for å unngå skade må du ikke plassere noen gjenstander oppå den.

**ADVARSEL!**

Under eksterne økter er den lokale teknikeren ansvarlig for å håndtere og håndheve lokale sikkerhetsregler for hver type undersøkelse og undersøkelsens spesifikke krav. Vær alltid til stede i kontrollrommet og/eller undersøkelsesrommet for å sikre sikkerheten til både pasienten og de involverte fagpersonene.

**ADVARSEL!**

Bordbevegelser under økten må bare utføres av den lokale teknikeren når systemet ber om det. Før den lokale teknikeren forlater operasjonsrommet, må vedkommende alltid trekke tilbake tilgangen til den eksterne teknikeren.

**ADVARSEL!**

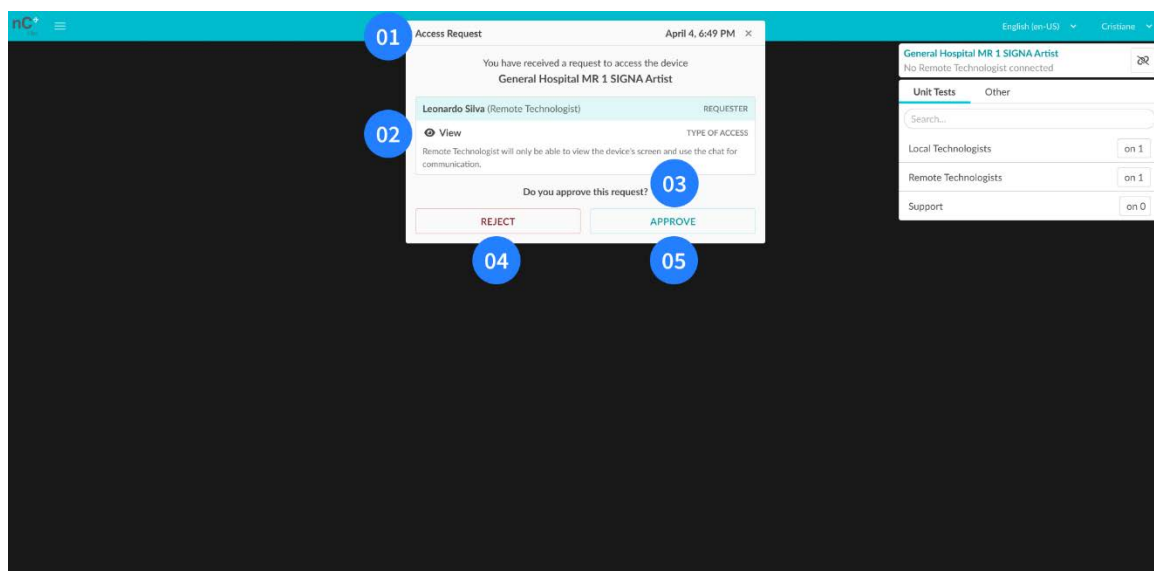
Bare den lokale teknikeren kan flytte bordet for å plassere pasienten inne i enheten og frigjøre pasienten trygt. Før den lokale teknikeren forlater operasjonsrommet, må vedkommende alltid trekke tilbake tilgangen til den eksterne brukeren.

Etter at du har logget på plattformen, fortsetter du med å velge ønsket enhet i boksen Device Selection (Enhetsvalg). Du vil være ansvarlig for denne enheten, slik at du kan gjennomgå forespørselen fra den eksterne teknikeren om tilgang til enheten. Når en Ekstern-teknolog ønsker å få tilgang til enheten, vises et popup-vindu som lar deg gjennomgå all informasjonen som presenteres før du gir eller nekter tilgang. Vær på utkikk etter en innkommende forespørsel fra en Ekstern-teknolog. Det er ytterst viktig å kontrollere hver detalj nøye. I tilfeller der den oppgitte informasjonen ikke gjenkjennes, må du ikke gi tilgang.

Den eksterne teknikeren kan få tilgang til enheten ved å bruke én av to tilgangsmoduser: **Control** eller **View**:

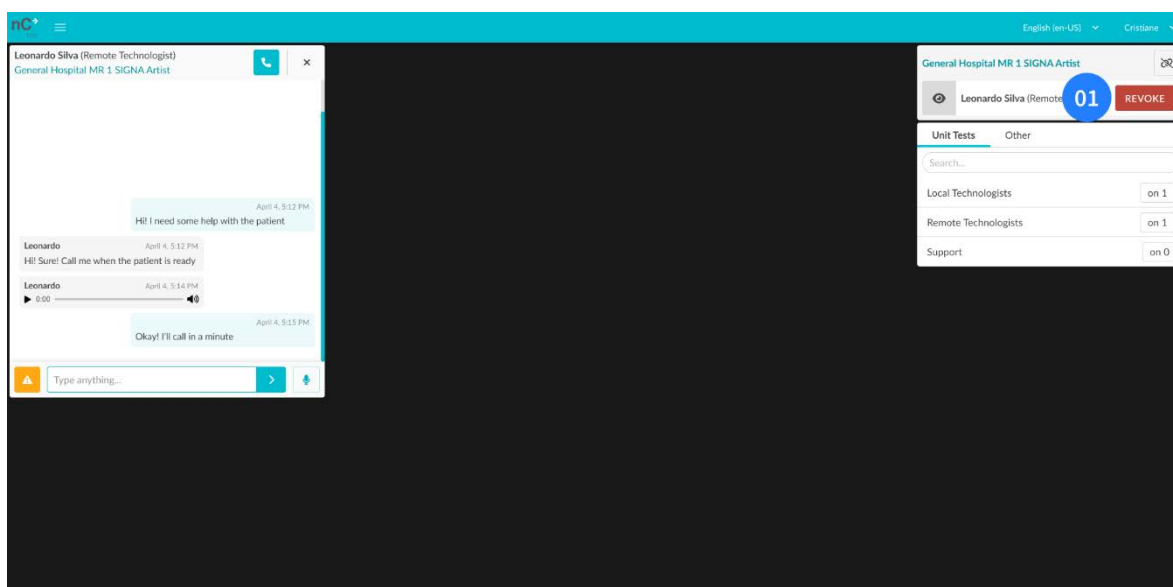
- **Control (Kontroll)** - lar den eksterne teknikeren kontrollere musen og tastaturet, samt vise enhetens strømming. Den lokale teknikeren mister imidlertid ikke kontroll over den lokale musen og det lokale tastaturet, og kan ta kontroll når som helst.
- **View (Vis)** - tillater at den eksterne teknikeren kun kan vise enhetens skjerm og bruke chatten til kommunikasjon

Etter at enheten er valgt, har brukeren tilgang til chattefunksjonen som muliggjør kommunikasjon via tekst, lydmeldinger, tale- og videosamtaler med de andre brukerne.



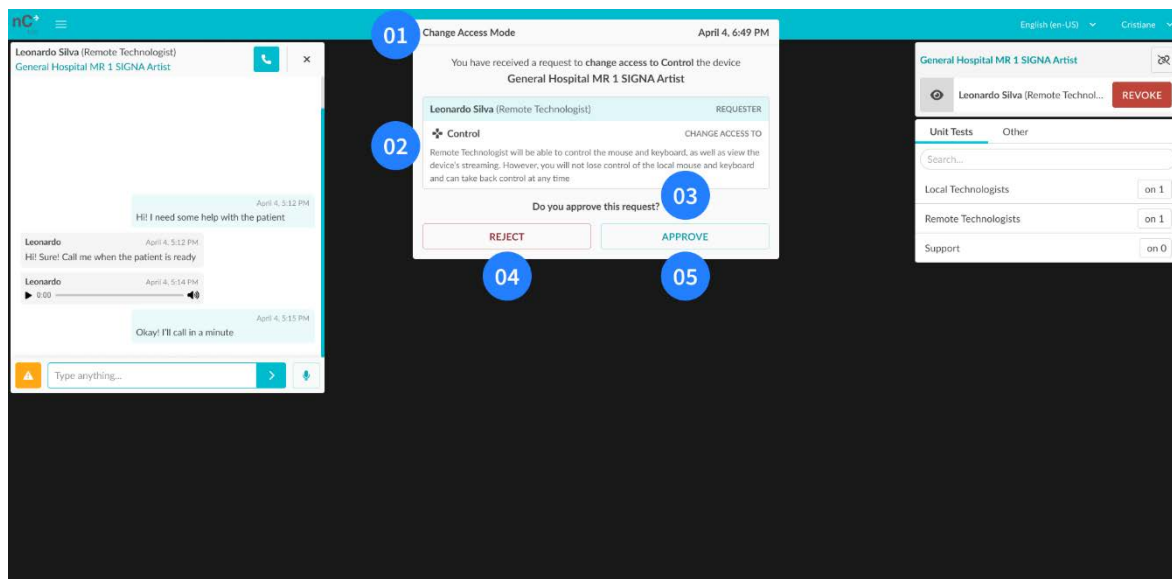
Figur 11: Lokal hovedskjerm i nCommand Lite med varsling om tilgangsforespørsel
01 – Tittel (Access Request [Tilgangsforespørsel]); **02** – Beskrivelse av forespørres navn, rolle og tilgangstype;
03 – Spørsmål: «Do you approve this request?» (Godkjenner du denne forespørselen?); **04** – Knappen Reject (Avvis); **05** – Knappen Approve (Godkjenn)

Etter godkjenning kan den lokale teknikeren når som helst trekke tilbake den eksterne teknikerens tilgang ved å klikke på knappen REVOKE (OPPHEV).



Figur 12: Hovedskjermbildet til Lokal-teknolog i nCommand Lite
01 – Knappen Revoke (Opphev)

Under den eksterne økten kan den eksterne teknikeren be om en endring av tilgangsmodus. Et popup-vindu med forespørselen vises på skjermen. Du kan godkjenne eller avvise den. Vær oppmerksom på privilegiene hver tilgangsmodus gir den eksterne teknikeren.



Figur 13: Lokal hovedskjerm i nCommand Lite med forespørsel om å endre tilgangsmodus

- 01** – Tittel (Change Access Mode [Endre tilgangsmodus]); **02** – Beskrivelse av bestillerens navn, rolle og tilgangstype;
03 – Spørsmål: «Do you approve this request?» (Godkjenner du denne forespørselen?); **04** – Knappen Reject (Avvis); **05** – Knappen Approve (Godkjenn)



ADVARSEL!

Hvis forbindelsen forsvinner på den lokale datamaskinen, har den eksterne teknikeren fortsatt tilgang til **enheten**. **Kontakt** umiddelbart den eksterne teknikeren og be ham/henne om å **koble fra** ELLER logg på en annen datamaskin og **trekk tilbake tilgangen** til den eksterne teknikeren ELLER **trykk på strømknappen** for å slå av e-KVM-datamaskinen.



ADVARSEL!

Ved vedlikehold av skanneren:

Før feltteknikeren starter noen prosedyrer (enten på enheten eller i kontrollrommet), må du informere den eksterne teknikeren og trekke tilbake tilgangen ved å klikke på knappen «REVOKE ACCESS» (TILBAKEKALL TILGANG). Logg deretter av fra nCommand Lite-plattformen.

Hvis ingen Ekstern-teknolog er tilkoblet, logger du av fra nCommand Lite-plattformen før du starter vedlikehold.

Seksjon 3.5 - Tilgang med Ekstern-teknolog-profil

Den eksterne teknikerens arbeidsplass omfatter utstyr som datamaskin, skjermer (vanligvis tre), mus, et tastatur og et headsett.

I den kliniske arbeidsflyten har lokale teknikere direkte kontakt med pasienten. De er ansvarlige for pasientsamhandling, posisjonering og sikring av sikkerhet og protokolloverholdelse under MR-, CT- eller PET/CT-prosedyrer, i henhold til institusjonelle og regulatoriske standarder.

3.5.1. Tilgangsmodus

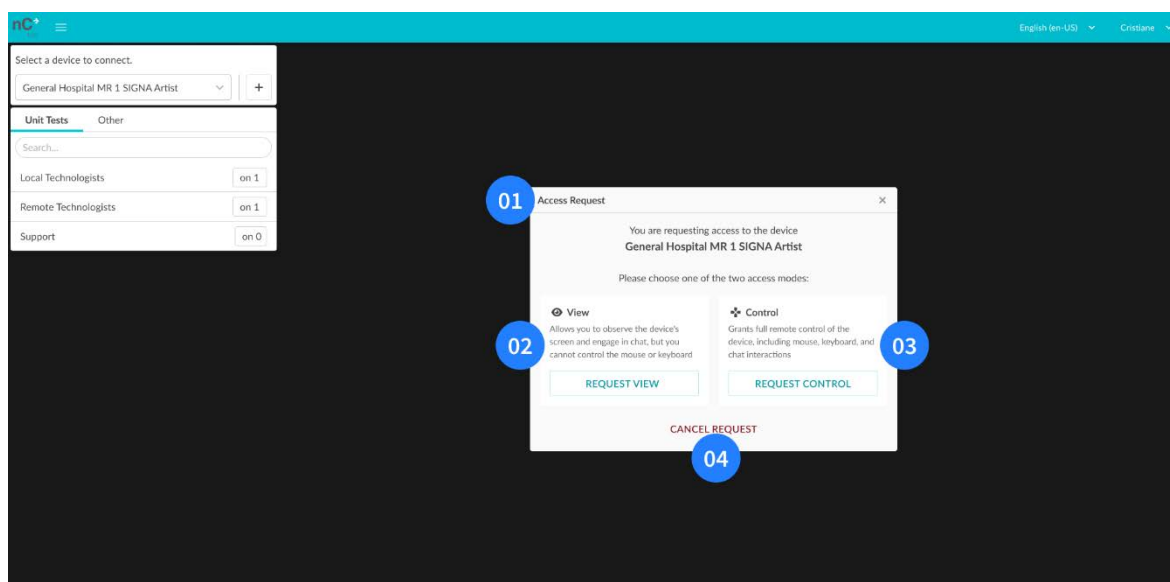
Når du har logget på plattformen, velger du enheten du vil koble til i boksen Device Selection (Enhetsvalg). Et popup-vindu åpnes for å velge tilgangsmodus mellom **Control (Kontroll)** og **View (Vis)**:

□ **Control (Kontroll)** – I denne modusen er mus- og tastaturkontroll aktivert i tillegg til skjermvisning. Lokale fagfolk beholder full tilgang til den lokale musen og det lokale tastaturet, og kan ta tilbake kontroll når som helst.

□ **View (Vis)** – Det er kun mulig å vise enhetens skjerm og bruke chatten til kommunikasjon.

Når du velger tilgangsmodus, vil en boks med «Waiting for approval» (Venter på godkjenning) vises, noe som indikerer at godkjenning fra den lokale teknikeren som er tilkoblet, er nødvendig for å fortsette. Denne lokale teknikeren har full myndighet til å godkjenne eller avslå tilgang og trekke tilbake tilgang når som helst hvis det anses som nødvendig. Dette tiltaket er avgjørende for å sikre streng kontroll og opprettholde sikkerheten ved bruk av enheten.

Etter at enheten er valgt, har brukeren tilgang til chattefunksjonen som muliggjør kommunikasjon via tekst, lydmeldinger, tale- og videosamtaler med de andre brukerne. Brukeren trenger ikke å bli godkjent for å få tilgang til chatten.



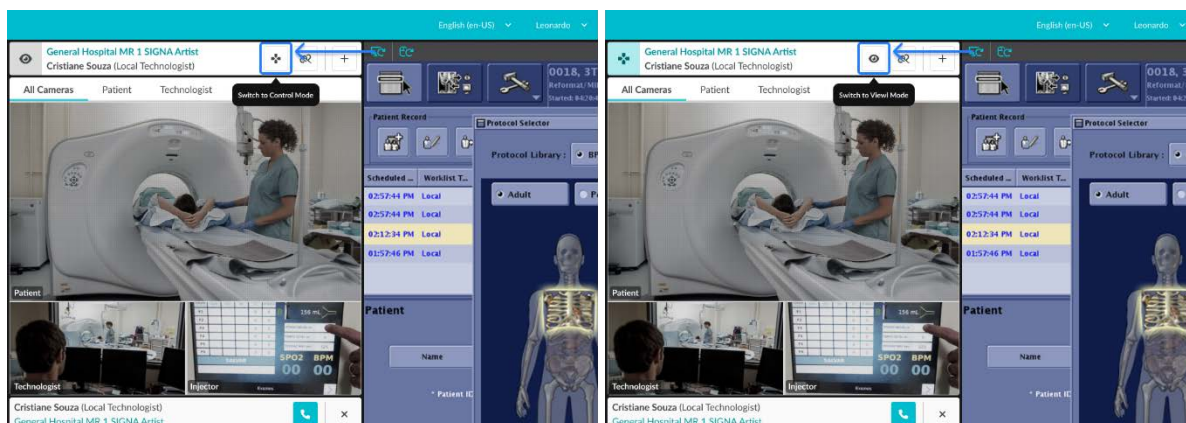
Figur 14: Dialogboks i nCommand Lite for forespørsel om tilgang for Ekstern-teknolog etter valg av enhet
01 – Tittel (Access Request [Tilgangsforespørsel]); **02** – Beskrivelse av modusen View (Vis) og knappen Request View (Be om Vis); **03** – Beskrivelse av modusen Control (Kontroll) og knappen Request Control (Be om Kontroll); **04** – Cancel Request (Kanseller forespørsel)

Når enhetstilgangen er autorisert av den lokale teknikeren, oppdateres den eksterne teknikerens grensesnitt for å vise sanntidsstrømming av enheten og dens tilhørende kameraer. Hvis den valgte tilgangsmodusen er Control (Kontroll), aktiveres muligheten for ekstern styring av enheten.

Denne prosessen sikrer effektiv og sikker samhandling, slik at enheten trygt kan brukes eksternt uten at det går på bekostning av enhetens integritet eller pasientsikkerheten.

Hvis du vil be om en endring i tilgangsmodus under en ekstern økt, klikker du på det tilsvarende ikonet. Den lokale teknikeren kan godta eller avvise forespørselen:

- **Accept (Godta)** – Strømmingen lastes inn på nytt, men chatteinnhold vil ikke gå tapt. Hvis du er i en tale- og videosamtale, avsluttes den og må startes på nytt av en av brukerne.
- **Decline (Avslå)**- et popup-vindu dukker opp som varsler deg om den lokale teknikerens avvisning, og den nåværende tilgangen vil forbli aktiv



**Figur 15: Venstre – Bytt til Kontroll-modusikon og verktøytips
Høyre - Bytt til Vis-modusikon og verktøytips**



ADVARSEL!

Bruker- og rotpassord for enhetens datamaskin: Begge må innehas av verten på stedet som skal motta installasjonsteamet.



ADVARSEL!

Bordbevegelser under økten må bare utføres av den lokale teknikeren når systemet ber om det. Før den lokale teknikeren forlater operasjonsrommet, må vedkommende alltid trekke tilbake tilgangen til den eksterne teknikeren.



ADVARSEL!

Bare den lokale teknikeren kan flytte bordet for å plassere pasienten inne i enheten og frigjøre pasienten trygt. Før den lokale teknikeren forlater operasjonsrommet, må vedkommende alltid trekke tilbake tilgangen til den eksterne brukeren.



ADVARSEL!

Vær alltid oppmerksom på rommet gjennom videokameraet og sørg for kommunikasjon med den lokale teknikeren før du utfører noen aktiviteter.



ADVARSEL!

Hvis forbindelsen mistes på den lokale datamaskinen, må du kontakte den lokale teknikeren umiddelbart og koble fra.



ADVARSEL!

Ved vedlikehold av skanneren:

Etter å ha blitt varslet om starten på vedlikeholdet av enheten, må du kontrollere at tilgangen er trukket tilbake av den lokale teknikeren og logge av fra nCommand Lite-plattformen.

Hvis tilgangen ikke er trukket tilbake, logger du av fra nCommand Lite-plattformen og kontakter umiddelbart den lokale teknikeren for å varsle ham/henne.

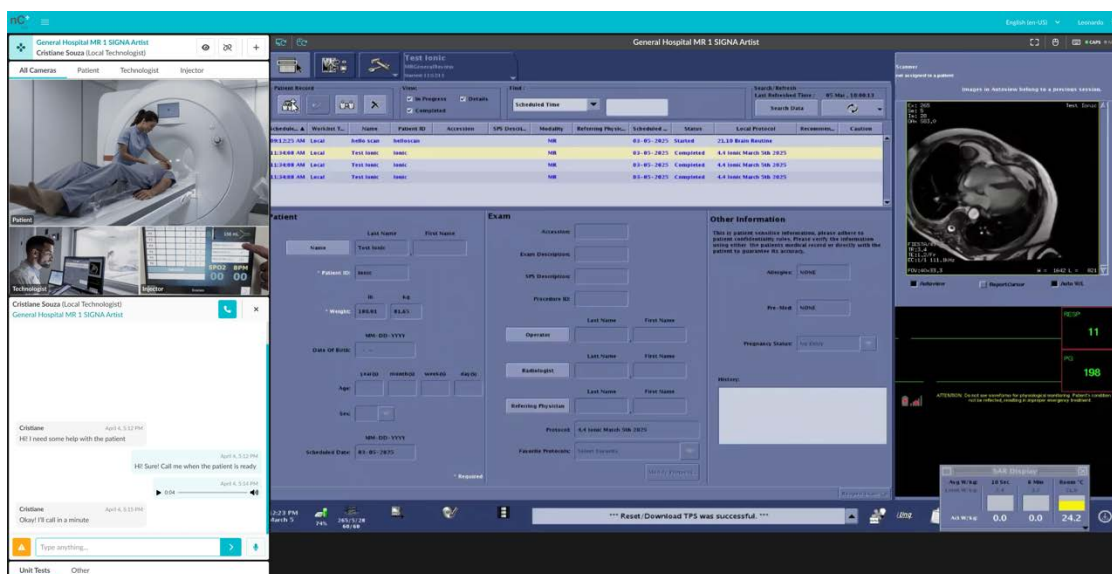


ADVARSEL!

Hvis du vil kontrollere musen og tastaturet eksternt, må den valgte tilgangsmodusen være Control (Kontroll); i modusen View (Vis) har den eksterne teknikeren bare tillatelse til å vise strømming og lokale kameraer.

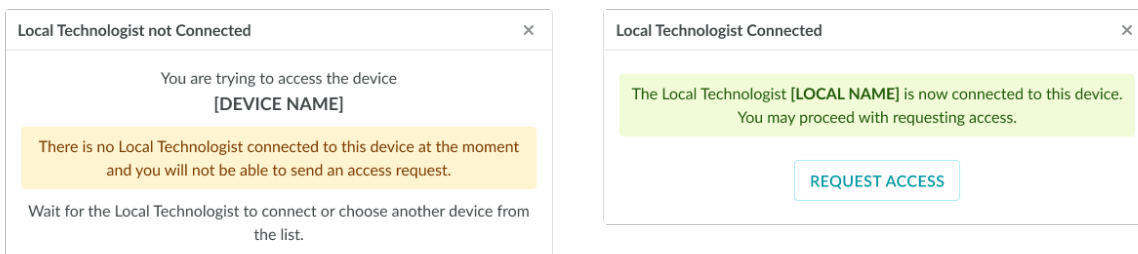
**ADVARSEL!**

Hvis svaret på forespørselen tar lengre tid enn forventet, kontakter du den lokale teknikeren via chat eller telefon.



Figur 16: Visning av hovedskjermbildet for Ekstern-teknolog i nCommand Lite

Når den eksterne teknikeren ber om tilgang og ingen Lokal-teknolog er koblet til enheten, viser plattformen en popup-advarsel. Så snart den lokale teknikeren kobler til, informerer plattformen den eksterne teknikeren om at de kan be om tilgang igjen.



Figur 17: nCommand Lite-advarsler – tilkoblingsstatus for Lokal-teknolog

Venstre panel: Varsel som indikerer at det ble gjort et forsøk på å få tilgang til enheten ([ENHETSNAVN]), men ingen Lokal-teknolog er tilkoblet for øyeblikket.

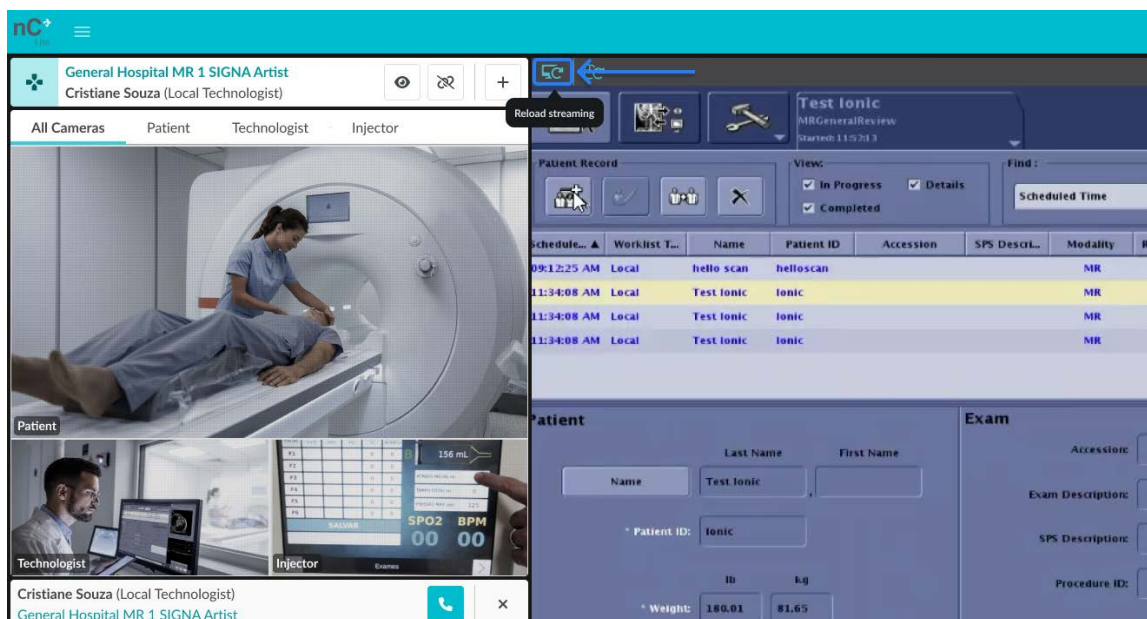
Høyre panel: Melding som bekrefter at den lokale teknikeren ([LOCAL NAME]) har koblet seg til enheten ([DEVICE NAME]) etter tidligere ikke å ha vært tilkoblet.

3.5.2. Strømmelinje

Strømmelinjen viser nøkkelinformasjon og kontroller relatert til strømmingsøkten for enheten. Den inkluderer knappene «Reload Streaming» og «Mouse Resync», enhetsnavnet, skjermopløsningen og gjeldende status for den eksterne datamaskinens mus og tastatur.

1 – Reload streaming (Last strømning på nytt)

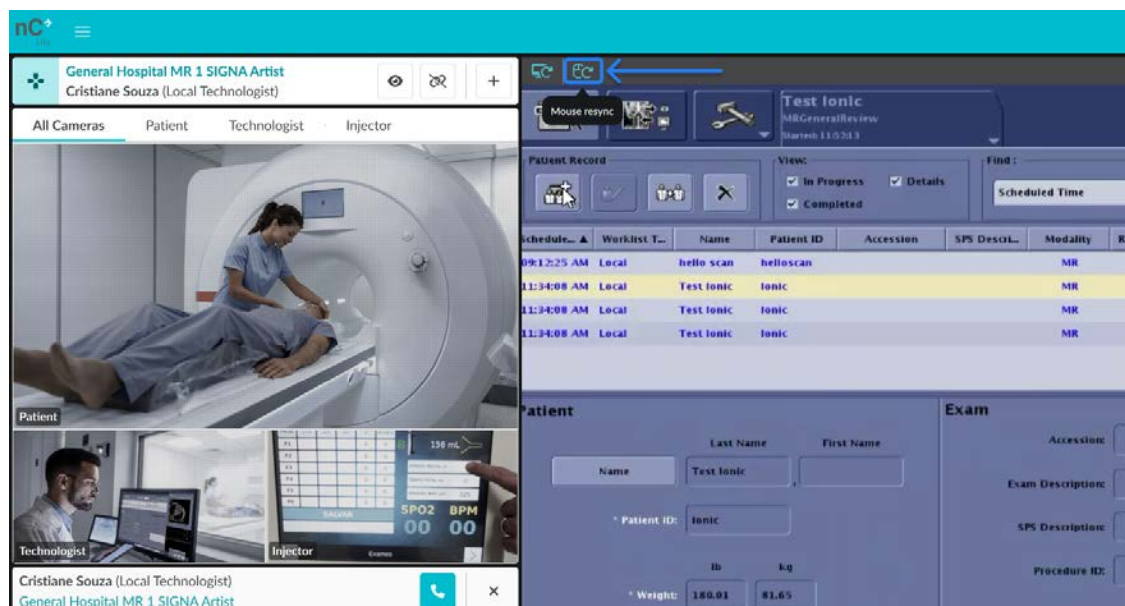
Denne funksjonen gjør det mulig for eksterne teknikere å gjenopprette tilgang til enheter ved tilkoblingsfeil eller ytelsesnedgang. Hvis du opplever noen form for frakobling eller skjermforsinkelse på enhetens datamaskin, kan du klikke på «Reload Streaming»-ikonet i strømmelinjen. Dette vil be plattformen om å koble til enhetens datamaskin på nytt og laste inn systemkameraene på nytt også.



Figur 18:Knappen for å laste inn strømning på nytt i nCommand Lite

2 – Mouse resync (Mus-resynkronisering)

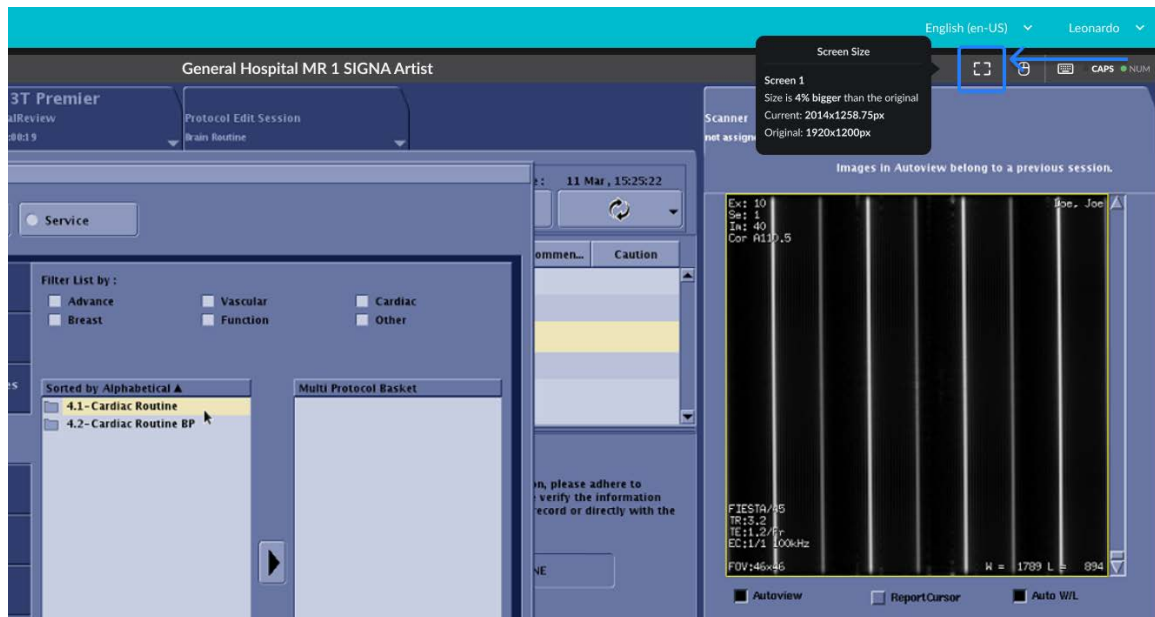
Hvis musen er treg eller ikke fungerer som den skal, klikker du på «Mouse Resync»-knappen som ligger på linjen over strømmevinduet for å synkronisere enhetens mus med e-KVM-datamaskinen på nytt.



Figur 19:Knappen Mouse resync (Mus-resynkronisering) i nCommand Lite

3 – Strømningsvisning

Denne funksjonen gir den eksterne teknikeren informasjon om den opprinnelige strømmeoppløsningen (fra enheten) og gjeldende oppløsning i piksler som vises på den eksterne arbeidsstasjonen.



Figur 20: Verktøytips med informasjon om strømmestørrelse i nCommand Lite

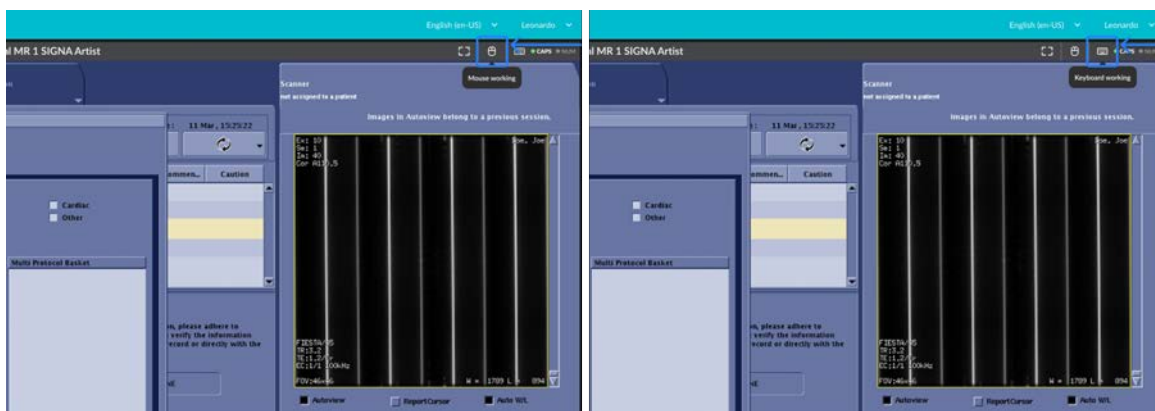
4 – Mus- og tastaturstatus

Denne funksjonen informerer den eksterne teknikeren om hvorvidt musen og tastaturet fungerer som de skal. Sammen med tastaturstatusen kan brukeren se om tastene **Caps lock** og **Num lock** på enhetens datamaskin er på eller av. Denne funksjonaliteten avhenger imidlertid av at enhetens datamaskin oppgir denne informasjonen. I situasjoner der denne informasjonen ikke gjøres tilgjengelig av enhetssystemet, vises ikke statusen til tastene **Caps Lock** og **Num Lock**. Både mus- og tastaturstatusene vises bare når brukeren har tilgangstypen Control (Kontroll).

Når du kobler til en enhet, kan en uoverensstemmelse mellom indikatorene for **Caps Lock** og **Num Lock** på den eksterne datamaskinen og enheten føre til inkonsekvent skriveatferd. Hvis indikatorene vises aktivert på enheten, men faktisk ikke er aktive på den eksterne datamaskinen, kan brukeren skrive inn store bokstaver på enheten mens teksten vises i små bokstaver i chatten, eller omvendt. Tilsvarende, hvis **Caps Lock** er aktivert på den eksterne datamaskinen, men deaktivert på enheten, vil det samme problemet oppstå på omvendt måte.

For å unngå dette problemet må du sørge for at både **Caps Lock** og **Num Lock** enten er aktivert, eller deaktivert før du logger på enheten. Hvis det oppstår uoverensstemmelse, skal brukeren koble fra enheten, justere tastaturstatusen på den eksterne datamaskinen og deretter koble til på nytt.

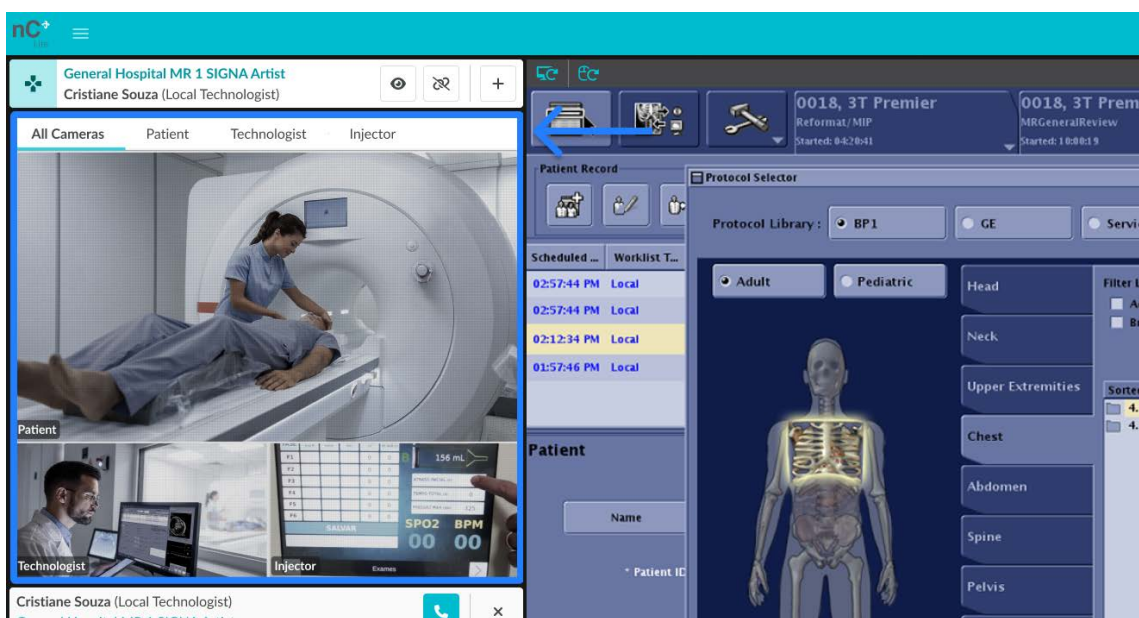
I tillegg vises **statusindikatorene for mus og tastatur** bare når brukeren har **Control (Kontroll)-tilgang** til enheten.



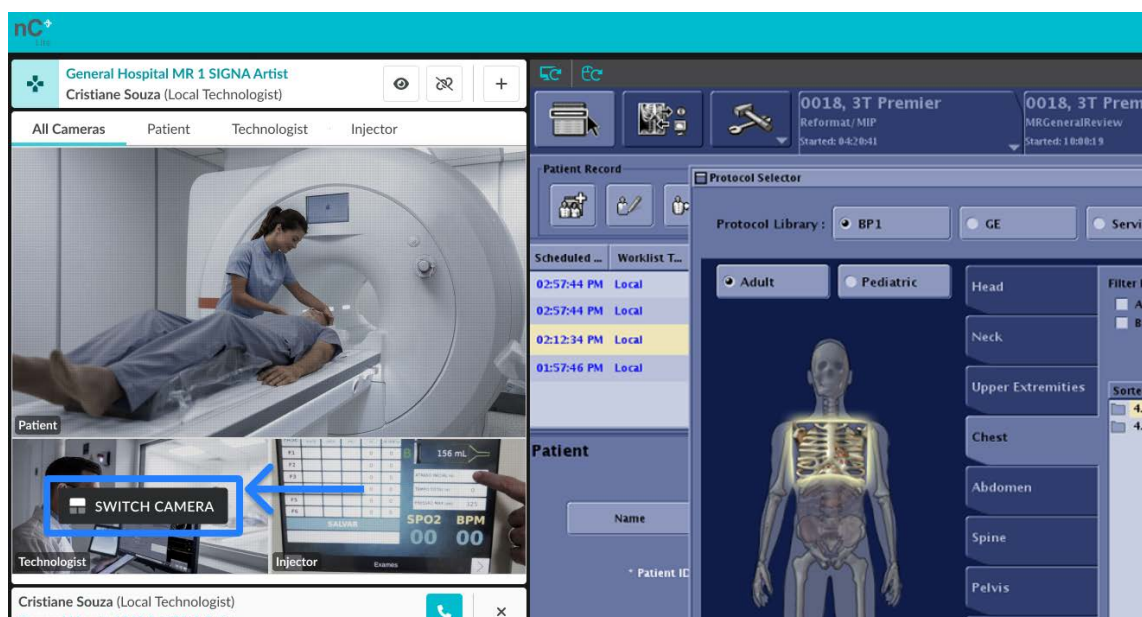
Figur 21: Venstre - Informasjon om verktøytips for musestatus for nCommand Lite
Høyre - Informasjon om verktøytips for tastaturstatus for nCommand Lite

3.5.3. Flere kameraer

Med denne funksjonen kan den eksterne teknikeren vise flere kameraer samtidig. Hvis mer enn ett kamera er tilgjengelig, er det mulig å vise bare ett og bytte mellom dem ved å klikke på menyen med det angitte navnet for hvert kamera. Når du velger «ALL CAMERAS» (ALLE KAMERAER), vises alle tilgjengelige kameraer i rammen, med ett av dem uthevet. Hvis du vil bytte det uthevede kameraet, holder du ganske enkelt musen over et av kameraene i den mindre rammen og klikker på «SWITCH CAMERA» (BYTT KAMERA).



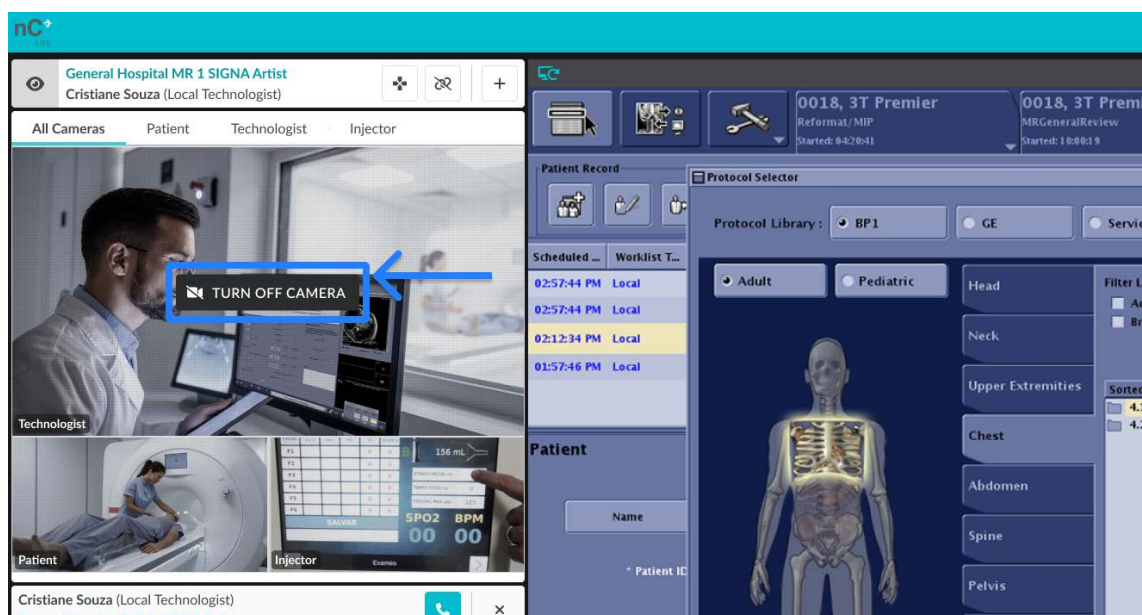
Figur 22: nCommand Lite-rammevisning med flere kameraer



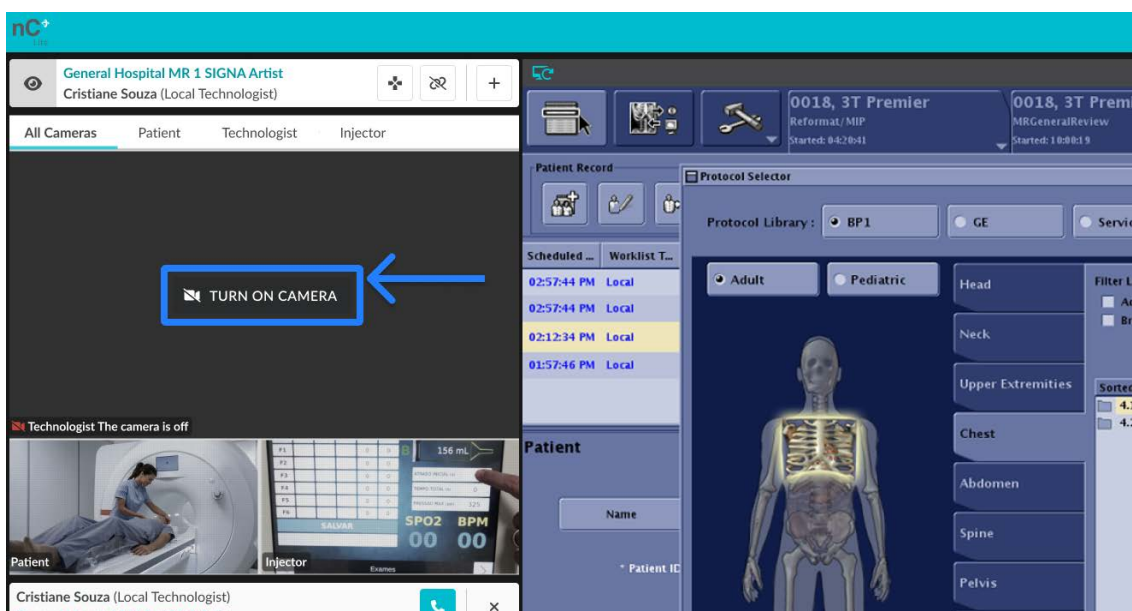
Figur 23: «SWITCH CAMERA» (BYTT KAMERA)-knappen for flere kameraer i nCommand Lite

Hvis den eksterne teknikerer har tilgang som **View (Vis)** under en aktiv ekstern økt, er det et alternativ for å slå av ett eller flere kameraer ved å holde musen over det valgte kameraet og klikke på «TURN OFF CAMERA» (SLÅ AV KAMERA). For å vise kameraet igjen gjentar du ganske enkelt prosessen og klikker på «TURN ON CAMERA» (SLÅ PÅ KAMERA).

MERK: Alternativet for å slå av kameraer er bare tilgjengelig i modusen View (Vis). I modusen Control (Kontroll) er det ikke mulig å slå av kameraene.



Figur 24: «TURN OFF CAMERA» (SLÅ AV KAMERA)-knappen for flere kameraer i modusen View (Vis) i nCommand Lite



Figur 25: «TURN ON CAMERA» (SLÅ PÅ KAMERA)-knappen for flere kameraer i modusen View (Vis) i nCommand Lite

3.5.4. Åpne en annen enhet

Lar den eksterne teknikeren åpne en ny nettlesefane i nCommand Lite, slik at brukeren kan velge en ny enhet for å utføre mer enn én ekstern skanning samtidig. For å åpne en ny enhet for tilgang, klikker du bare på knappen «Open Another Device» (Åpne en annen enhet), så gis det en advarsel slik at du trygt kan utføre denne samtidige operasjonen. Du bør lese advarselen før du åpner dette nye vinduet.

MERK: For bedre visning under samtidig tilgang anbefales det at du etter å ha klikket på «OPEN ANOTHER DEVICE» (ÅPNE EN ANNEN ENHET) og klikket på «OK» på advarslene, drar den nye fanen til en annen tilgjengelig skjerm.

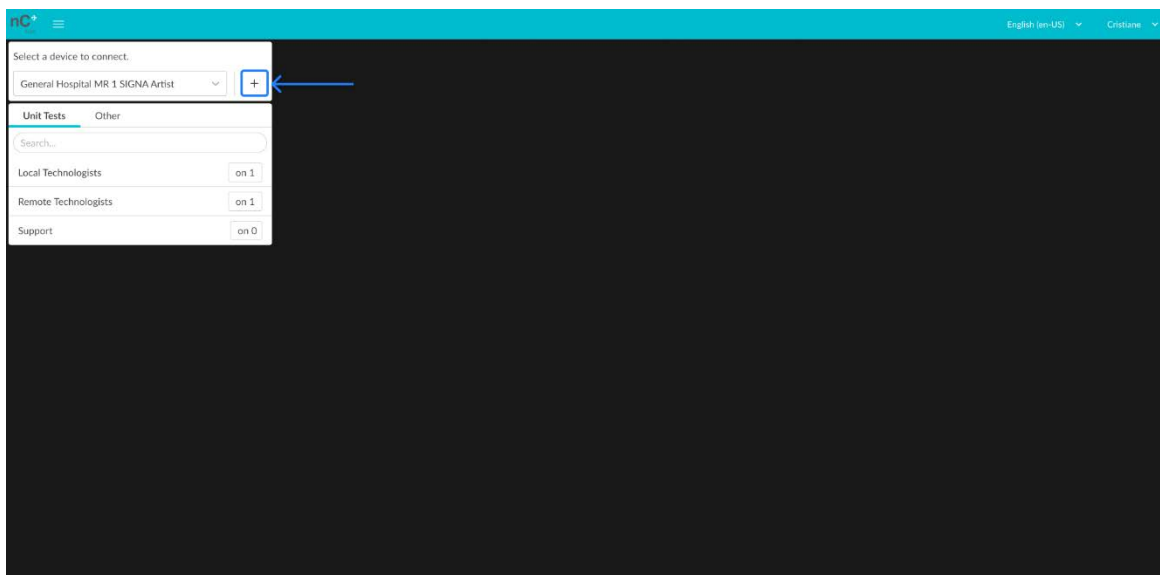


ADVARSEL!

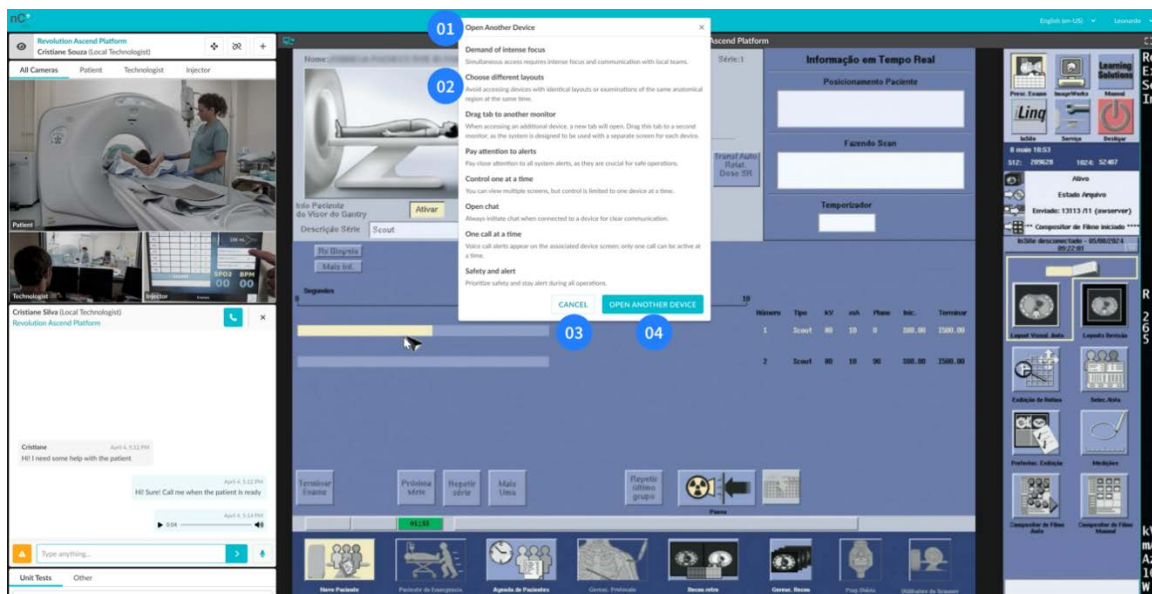
Sikkerhetsadvarsel for tilgang til flere skannere

- **• Demand of intense focus (Krav om intens konsentrasjon):** Samtidig tilgang krever intens konsentrasjon og kommunikasjon med lokale team.
- **Velg forskjellige oppsett:** Unngå å ha tilgang til enheter med identiske oppsett eller undersøkelser av den samme anatomiske regionen samtidig.
- **Dra fanen til en annen skjerm:** Når du får tilgang til en ytterligere enhet, vil en ny fane åpnes. Dra denne fanen til en annen skjerm, siden systemet er designet for bruk med en separat skjerm for hver enhet.
- **• Pay attention to alerts (Vær oppmerksom på varsler):** Følg nøye med på alle systemvarsler, da de er avgjørende for trygt bruk.
- **• Control one at a time (Kontroller én om gangen):** Du kan vise flere skjermer, men kontrollen er begrenset til én enhet om gangen.

- ● **Open chat (Åpne chat):** Innled alltid chat når du er koblet til en enhet, for klar kommunikasjon.
- **Ett anrop om gangen:** Taleanropsvarsler vises på skjermbildet til den tilknyttede enheten; kun én samtale kan være aktiv om gangen.
- ● **Sikkerhet og årvåkenhet:** Prioriter sikkerhet og vær årvåken under alle operasjoner.



Figur 26: Visning av hovedskjermbildet i nCommand Lite med knappen «Open Another Device» (Åpne en annen enhet) (+)



Figur 27: Dialogboksen for tilgang til flere enheter i nCommand Lite
01 – Tittel (Åpne en annen enhet); 02 – Driftssikkerhetsadvarsler; 03 – Knappen Avbryt;
04 – Åpne en annen enhet-knapp

Seksjon 3.6 - Chat

Plattformen tilbyr en sanntids-chat og samtale med tale- og videofunksjoner som brukes til effektiv kommunikasjon mellom autoriserte teknikere. Gjennom disse funksjonene kan de lisensierte teknikerne samhandle angående alle saker knyttet til arbeidsflyten til økten, ved å bruke direkte tale- og tekstkommunikasjon.

**ADVARSEL!**

Hvis denne funksjonen svikter, ringer du den lokale teknikeren.

Når du kobler til en enhet, vil du ha umiddelbar tilgang til chat-brukerlisten, organisert i to faner. For kunder med flere områder kan hver filial konfigureres som en separat kontrakt. Når den er aktivert, grupperes brukere etter kontrakt, med brukere fra andre kontrakter som vises under «Others»-fanen.

For å starte en samtale dobbeltklikker du på en brukers navn for å åpne chat-grensesnittet, som støtter både tekstmeldinger og taleanrop. Sørg for at den valgte økten samsvarer med riktig enhet. Plattformen varsler brukere hvis nettverkstilkoblingen blir treg eller ustabil.

**ADVARSEL!**

Før du starter kontakten, må du bekrefte enhetsnavnet som vises under brukerens navn, siden noen eksterne teknikere kan være koblet til flere enheter.

Her er verktøyene som er tilgjengelige for kommunikasjon på plattformen:

1. **Tale- og videosamtaler:** Klikk på ikonet for å starte en tale- og videosamtale på opptil 60 minutter mellom en ekstern og en Lokal-teknolog. Tilkoblinger mellom brukere med samme profil (Lokal–Lokal eller Ekstern–Ekstern) støttes ikke.

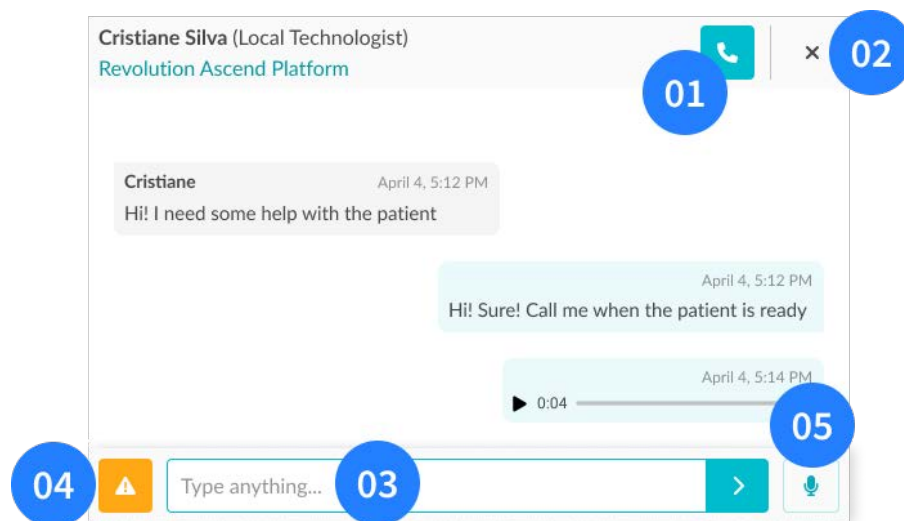
Når en Lokal-teknolog starter en samtale, kan den eksterne teknikeren velge å godta eller avslå. I motsatt fall, når en Ekstern-teknolog starter samtalen, kobles den automatisk til, og den lokale teknikeren blir varslet – disse funksjonene er en sikkerhetsmekanisme for å sikre at den eksterne teknikeren alltid kan kommunisere med den som er fysisk til stede, som om han/hun var der personlig.

Som standard er mikrofonen aktiv ved starten av samtalen, mens kameraet forblir av. Hver teknolog kan manuelt slå mikrofonen og kameraet av eller på når som helst.

For å lykkes med å opprette en samtale, må begge brukerne ha en fungerende mikrofon og lydutgang, med nettlesertillatelser riktig aktivert. Hvis noen av disse komponentene mangler, vil systemet varsle begge brukerne, og samtalen vil ikke bli fullført. Et kamera er valgfritt – hvis det ikke er tilgjengelig eller ikke oppdages, vil systemet oppdatere ikonet for å gjenspeile at video ikke støttes.

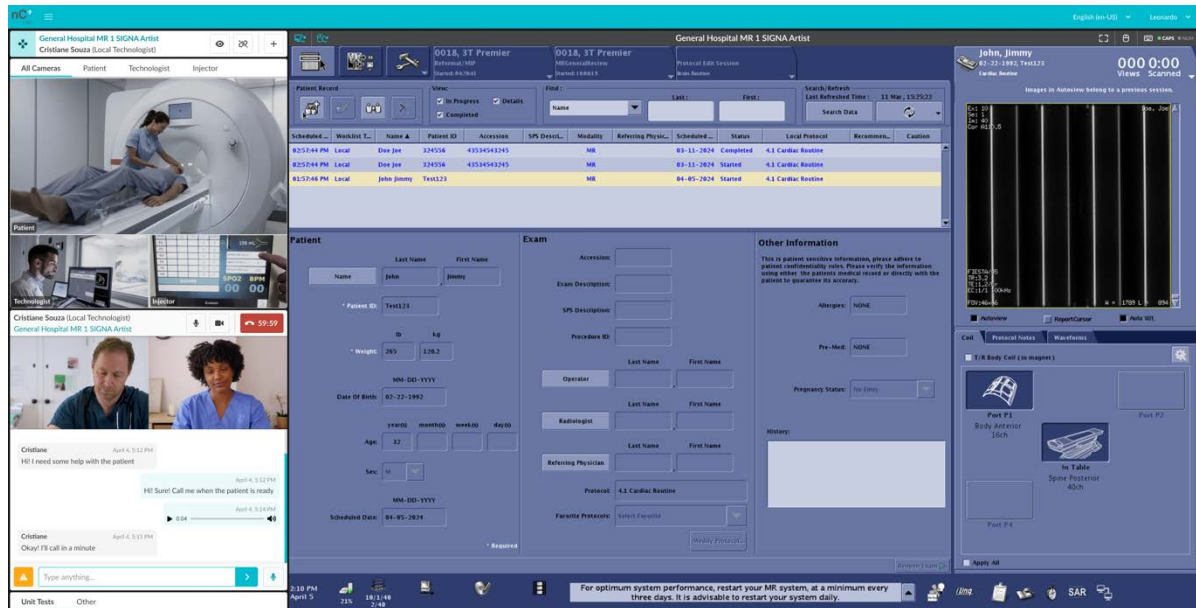
Bare én aktiv samtale er tillatt per bruker. Hvis en teknolog prøver å starte en ny samtale mens han allerede er i en, vil systemet blokkere forsøket og vise et varsel. På samme måte, hvis en bruker allerede er i en samtale og mottar et annet innkommende anrop, vil den som ringer bli informert om at mottakeren for øyeblikket ikke er tilgjengelig, og brukeren i den pågående samtalen vil motta et varsel som indikerer at noen har forsøkt å kontakte ham/henne.

2. **Lukke chatter:** Når én av brukerne lukker chatten ved å klikke på lukk-knappen, sendes en automatisk melding til den andre brukeren, og chatfanen lukkes. Dette sikrer at begge parter blir informert om at samtalen er avsluttet. Når chatvinduet lukkes, forsvinner alle meldingene. Hvis du åpner det på nytt under økten, startes samtalen på nytt uten tidligere meldinger.
3. **Tekstmeldinger:** Send tekstmeldinger i det angitte feltet. Når en melding sendes, vises et ikon med en grå hake, og når meldingen mottas av mottakeren, vises et annet ikon med to blå hakemerker. Dette muliggjør sikker, tydelig og konsis skriftlig kommunikasjon mellom de to partene.
4. **Be om oppmerksomhet:** Tiltrekk den andre brukerens oppmerksomhet ved å klikke på knappen med et utropstegn. Denne handlingen aktiverer en visuell vibrasjonseffekt på den andre brukerens vindu i noen sekunder, og det sendes automatisk en melding som signaliserer at det haster eller er viktig.
5. **Lydmeldinger:** Send lydmeldinger ved å klikke på mikrofonknappen. Dette brukes når du ønsker å formidle en melding mer personlig eller når det ikke er praktisk å skrive.

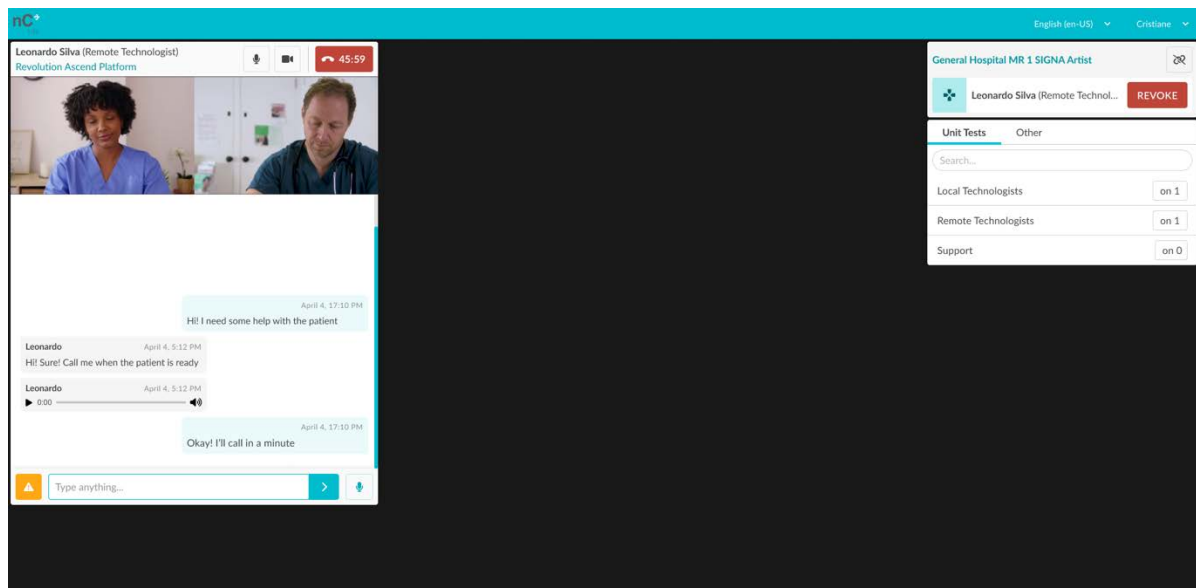


Figur 28: Visning av chatvinduet i nCommand Lite

- 01 – Tale- og videosamtaleknapp; 02 - Lukk chat-knapp; 03 – Meldingstekstboks;
04 – Kall på oppmerksomhet-knapp; 05 – Ta opp lydmelding-knapp



Figur 29: Hovedskjermbildet til Ekstern-teknolog i nCommand Lite med aktiv chat og aktivt videoanrop vist (nederst til venstre)



Figur 30: Hovedskjermbildet til Lokal-teknolog i nCommand Lite med aktiv chat og aktivt videoanrop vist (øverst til venstre)

Seksjon 3.7 - Avslutte økten på plattformen

Når oppgaven er avsluttet, må den autoriserte teknikeren koble fra enheten og logge ut av plattformen.

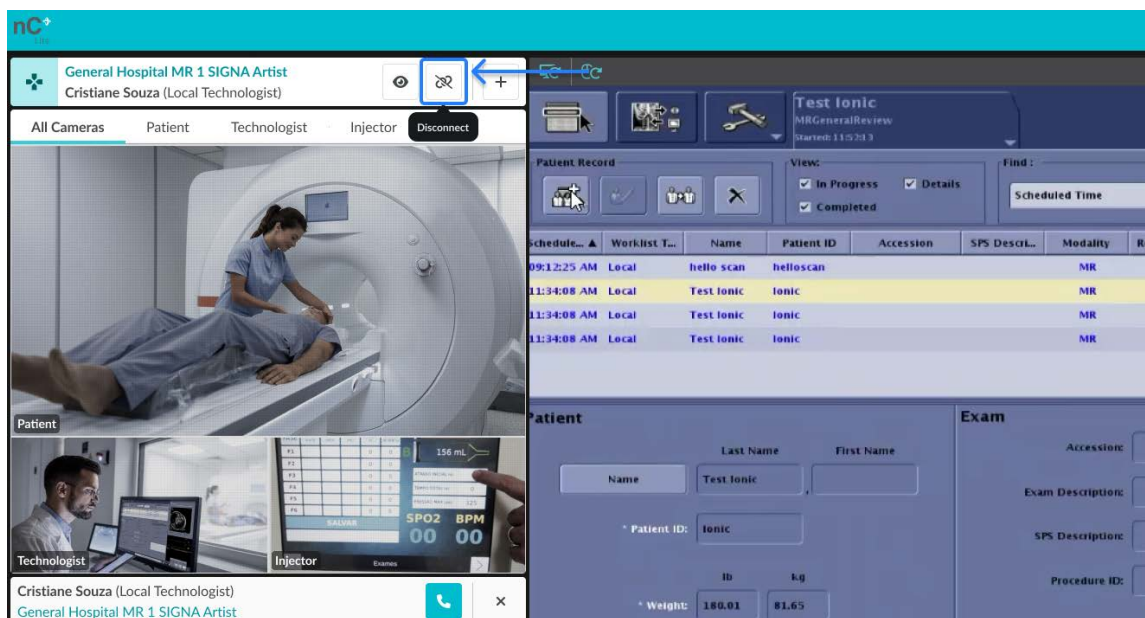


ADVARSEL!

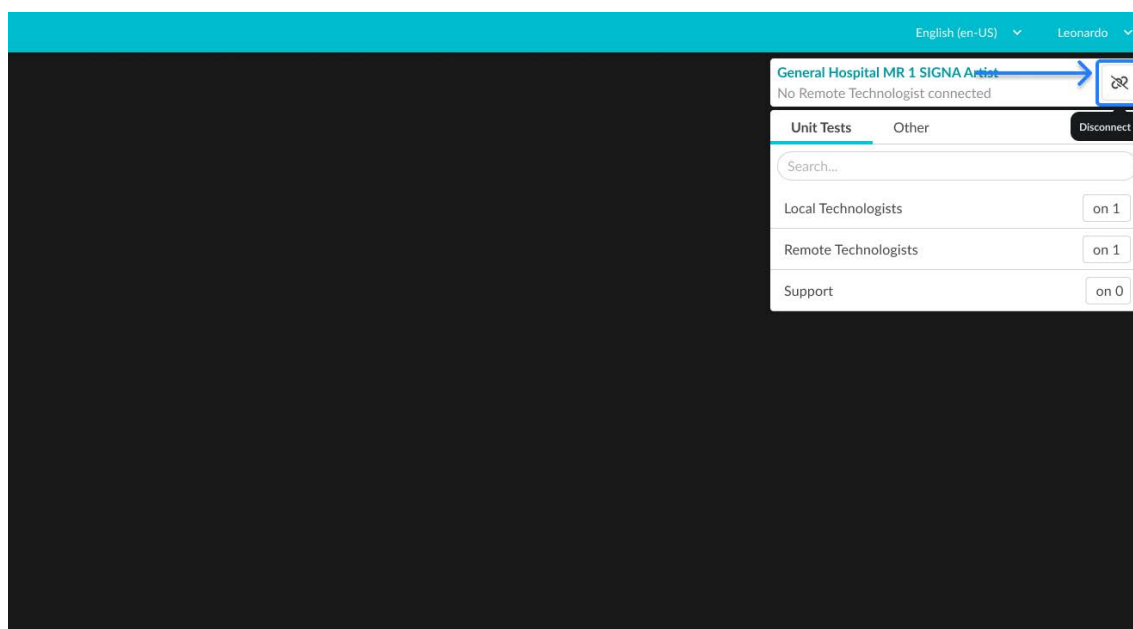
De autoriserte teknikerne må ikke glemme å logge ut av plattformen før oppgaven er over.

For å koble fra enheten må du klikke på frakoblingsikonet som finnes i enhetsboksen. Merk: Hvis du arbeider som Lokal-teknolog, må du sørge for at du har trukket tilbake eventuell tilgang for Ekstern-teknolog før du kobler deg fra enheten.

For å sikre sikkerheten vil du motta et varsel for å bekrefte at du ønsker å koble deg fra enheten. Når du har bekreftet, vil du bli omdirigert til startskjermen uten noen enhet valgt.



Figur 31: Hovedskjermbildet til Ekstern-teknolog i nCommand Lite med knappen «Disconnect»



Figur 32: Hovedskjermbildet til Lokal-teknolog i nCommand Lite med knappen «Disconnect»

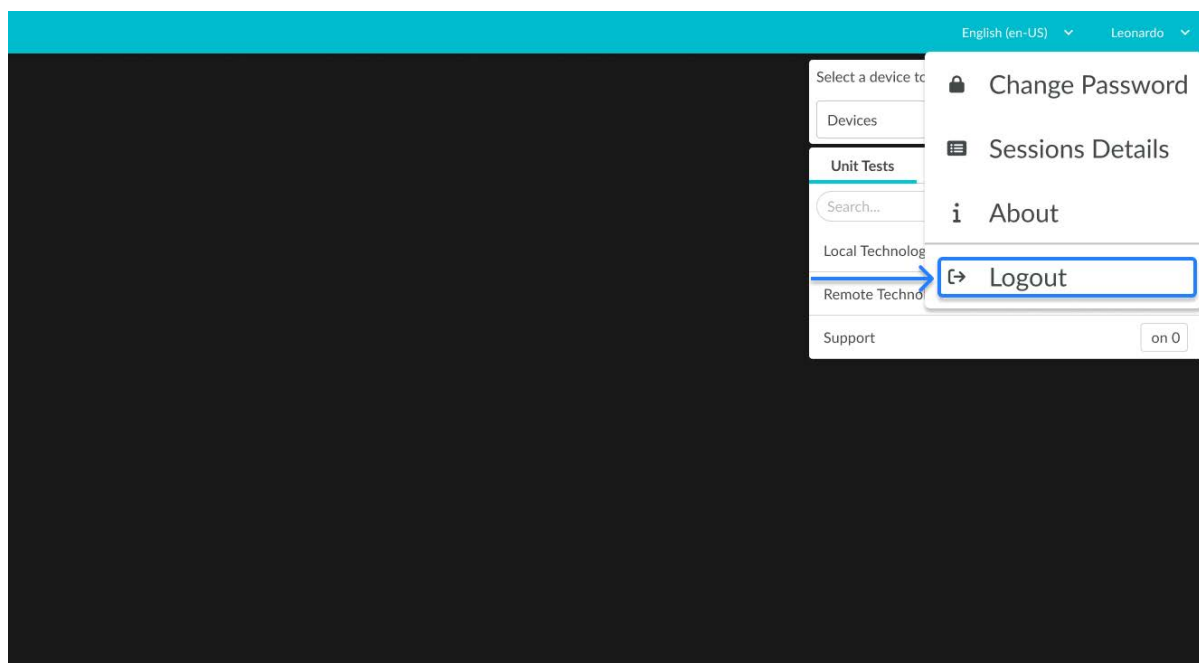
Problemer med internett-forbindelsen – Når en av teknikerne opplever problemer med nettverksforbindelsen, vil systemet vise en melding og forsøke å koble til på nytt. Hvis forbindelsen gjenopprettes, viser systemet en **ONLINE**-melding, og den eksterne økten fortsetter som vanlig. Hvis forbindelsen imidlertid ikke gjenopprettes etter flere forsøk på å koble til igjen, vil systemet avslutte den aktive økten og varsle teknikeren om at vedkommende har blitt frakoblet på grunn av Internett-problemer. Samtidig vil det også varsle den andre teknikeren om at motparten har blitt frakoblet på grunn av internett-problemer.

**ADVARSEL!**

Før du logger av, må du kontrollere at alle ytterligere faner som ble åpnet, er lukket.

For å avslutte økten på plattformen, klikker du på brukernavnet ditt øverst til høyre på skjermen og velger alternativet «Logout» (Logg ut). Du vil motta et varsel for å bekrefte at du ønsker å forlate helsesenteret der du arbeidet. Når du har bekreftet, vil du bli omdirigert til applikasjonens påloggingsside, og dermed er arbeidsforløpet trygt avsluttet.

nCommand Lite kontrollerer ikke brukerens økt på den eksterne IdP-en og kan derfor ikke utføre en utlogging på IdP-nivå. I scenarier der brukere deler samme maskin og bruker Single Sign-On (SSO), anbefales det at hver bruker velger alternativet «ikke forbli pålogget» under ekstern IdP-innlogging (hvis tilgjengelig) eller logger ut av IdP etter å ha logget ut av nCommand Lite. Dette sikrer at ingen etterfølgende brukere på samme enhet utilsiktet kan gjenbruke en aktiv økt.



Figur 33: Rullegardinmenyalternativet Logout (Logg ut) i nCommand Lite

**ADVARSEL!**

Når du bruker en ekstern identitetsleverandør på en delt eller offentlig datamaskin, etter at du har logget ut av plattformen, logger du også ut fra identitetsleverandøren. Hvis du vil ha mer informasjon om hvordan du går frem, kan du kontakte organisasjonens IT-støtteteam.

Seksjon 3.8 - Operativ trening

Deltakelse i opplæringsprogrammet er obligatorisk for alle brukere av nCommand Lite-systemet. Brukerregistrering på plattformen administreres av IONIC Health-teamet og igangsettes først etter bekreftelse på at brukeren har fullført nødvendig LMS-opplæring og er tilstrekkelig kvalifisert til å bruke plattformen. Denne prosessen sikrer at alle brukere har en grundig forståelse av systemets funksjonalitet og er forberedt på å bruke plattformen effektivt og trygt. For å starte påmeldingsprosessen for opplæring, kan du kontakte salgsrepresentanten din.

Seksjon 3.9 - Retningslinjer for feilsøking

BRUKER OG PASSORD	
Passordendring	Bekreft at passordkravene er oppfylt – passordet må være sterkt og sikkert, inkludert minst én liten bokstav, én stor bokstav, ett spesialtegn og være minst 8 tegn langt.
Glemt passordet mitt	Sjekk e-postinnboksen din: Kontroller at du bruker riktig e-postadresse, og at e-posten for gjenoppretting av passord ikke er filtrert inn i søppelpostmappen. Prøv på nytt: Vent noen minutter og be om en ny e-post for gjenoppretting av passord ved å klikke på «Did you Forget your password?» (Har du glemt passordet?). Kontroller internettforbindelsen: Kontroller at du er koblet til internett.
Velkomst-e-post ikke mottatt	Kontroller om e-posten er i søppelpostmappen. Hvis den ikke er der, kontakter du en administratorbruker for å kontrollere at e-postadressen i registreringen er riktig. Hvis den ikke er riktig, skal administratoren oppdatere den og sende velkomst-e-posten på nytt.
Tofaktoraautentiseringskode ikke mottatt	Klikk på «Resend Code» (Send kode på nytt) og sjekk søppelpostmappen. Hvis du ikke mottar den, vennligst kontakt en administratorbruker for å bekrefte om e-postadressen som er registrert i tilgangskontrollen, er riktig.
Overskredet påloggingsforsøk	Hvis du overskrider det tillatte antallet påloggingsforsøk, må du vente i en periode før du prøver på nytt.
LEVERANDØR AV EKSTERN IDENTITET	
Problemer med å logge på produktet	Hvis du støter på påloggingsproblemer mens du bruker en ekstern identitetsleverandør (IdP), bør du være oppmerksom på at autentiseringsprosessen administreres utelukkende av IdP-en og ikke av produktleverandøren, dvs.: Ionic Health. Produktet, som det er, kan ikke hjelpe med kontolegitimasjon, tilgangspolicyer, autentiseringsfeil eller kontrolåsing. I disse tilfellene bør du kontakte organisasjonens IT-støtteteam, som kan se gjennom IdP-

	konfigurasjonen og hjelpe deg med å løse problemet.
Problemer med legitimasjon	Eventuelle legitimasjonsrelaterte problemer (f.eks. glemt passord, endring av passord) må løses direkte med IT-støtteteamet til organisasjonen din. De kan gjennomgå IdP-konfigurasjonen og gi nødvendig hjelp.
Problemer med autentisering med flere faktorer (MFA)	Eventuelle problemer relatert til autentisering med flere faktorer (MFA) (f.eks. problemer med utløp av MFA, MFA fungerer ikke, pålogging uten å be om MFA) må løses direkte med organisasjonens IT-støtteteam. De kan gjennomgå IdP-konfigurasjonen og gi nødvendig hjelp.
Legitimasjon fungerer ikke på plattformen	Når du bruker eksterne identitetsleverandører (IdP), logger du på produktet kun ved hjelp av IdP. Bruk av IdP-legitimasjonen direkte på påloggingssiden til produktet vil resultere i mislykket pålogging.
SKJERMEN TIL SKANNERENS DATAMASKIN	
Slår seg ikke på	Kontroller skjermens tilkobling til datamaskinen og stikkontakten. Frakoblinger kan forekomme. Trykk på skjermens strømknapp igjen.
PLATTFORM	
Kan ikke nås	Kontroller nettverksforbindelsen. Kontroller om plattformen har startet, og om påloggingen har funnet sted.
Plattformlatens	Oppdater siden ved å trykke på Ctrl+F5. Kontroller om enhetens (helseinstitusjonens) chat er åpen i mer enn én fane. I så fall lukker du fanen som ikke brukes. Hvis problemet vedvarer, kan du prøve å logge ut av plattformen, tømme hurtigbufferen, lukke nettleseren og deretter logge på igjen.
Funksjoner som ikke fungerer	Før du prøver andre feilsøkningsprosedyrer, tømmer du nettleserbufferen (se etter instruksjoner i den nåværende nettleseren) etter pålogging, lukker og åpne nettleseren på nytt, logger på plattformen igjen, og prøver handlingen på nytt.
Oppgradere	Etter at plattformen er oppgradert, tømmer du nettleserbufferen (se instruksjonene for nettleseren din) før du logger på den nye versjonen.
LYD	

Ingen lyd	Kontroller at enhetens (helseinstitusjonens) mikrofon- og høyttalervolumer er justert til egnede nivåer. Kontroller om nettleseren har tillatelse til å bruke lyd og mikrofon. Kontroller om headsettet er tilkoblet og fungerer som det skal.
Lydløst	Kontroller utstyrets elektriske tilkoblinger og nettverkstilkoblinger. Oppdater nettlesersiden ved å trykke på Ctrl+F5 og logg på igjen. Hvis problemet vedvarer, kan du prøve å logge ut av plattformen, tømme hurtigbufferen, lukke nettleseren og deretter logge på igjen.
CHAT	
Chat vises ikke	Kontroller at nettleseren ikke er minimert. Ellers åpner du chatten etter å ha logget på nCommand Lite-plattformen. Kontroller at enheten (helseinstitusjonen) er valgt, og at brukeren er autorisert til å aktivere chatkommunikasjon. Kontroller at nettleserens lyd- og mikrofontillatelser er godkjent. Kontroller kabeltilkoblingene, som kan være frakoblet. Oppdater nettlesersiden ved å trykke på Ctrl+F5 og koble til plattformen igjen. Kontroller om nettstedets chat er åpen i mer enn én fane. I så fall lukker du fanen som ikke brukes.
Chat-forsinkelse	Oppdater nettlesersiden ved å trykke på Ctrl+F5 og koble til plattformen igjen. Hvis problemet vedvarer, kan du prøve å logge ut av plattformen, tømme hurtigbufferen, lukke nettleseren og deretter logge på igjen. Kontroller kabeltilkoblingene, som kan være frakoblet.

Problem med å sende lydmeldinger	Kontroller nettlesertillatelsene for lyd og mikrofon, og sørg for at både mikrofon- og lydenheter er koblet til datamaskinen. Hvis nettlesertillatelsene må justeres, trykker du på Ctrl+F5 for å be nettleseren om å gjenkjenne endringene når siden lastes inn på nytt.
Taleanrop startet ikke	Kontroller internettforbindelsen og se om det ble vist noe varsel som forklarer årsaken til at anropet ikke startet. Kontroller at du har en tilkoblet lydenhet, og at lyd- og mikrofontillatelser er tillatt i nettleseren. Hvis problemet vedvarer, oppdaterer du siden med Ctrl+F5 for å prøve igjen.
Brukeren ikke funnet i chatten	Hvis du ikke finner en bruker i chatten, klikker du på fanen «Others» (Andre) for å sikre at de ikke er oppført der. Brukere tilknyttet andre kontrakter vises separat i kontaktlisten. Hvis brukeren ikke vises i kontaktlisten etter at enheten er valgt, trykker du på Ctrl+F5 for å oppdatere skjermbildet og velger på nytt. Kontroller at du har en internettforbindelse.
BE OM TILGANG TIL ENHETEN	
Plattformen gjenkjente ikke at den lokale teknikeren er tilkoblet	Kontroller under alternativet «Others» (Andre) for å bekrefte om den lokale brukeren er tilkoblet. Hvis brukeren faktisk er tilkoblet, men du fortsatt mottar meldingen om at den lokale brukeren ikke er koblet til skanneren, oppdaterer du skjermen ved å trykke på Ctrl+F5 og be den lokale brukeren gjenta samme instruksjon. Deretter velger du enheten igjen og ber den lokale brukeren om å velge enheten på nytt også. Hvis problemet vedvarer, kontakter du kundestøtte for å kontrollere nettverket.
Tilgangsforespørsel sendes ikke	Oppdater siden ved å trykke på Ctrl+F5 og bekreft med den lokale brukeren via chat om tilgangsforespørselen mottas. Hvis problemet vedvarer, kontakter du kundestøtte for ytterligere assistanse.
STRØMMEENHET (e-KVM-DATAMASKIN)	
Strømmeenheden (e-KVM-DATAMASKINEN) fungerer ikke	Klikk på knappen «Reload streaming» (Last inn strømming på nytt) på plattformen. Kontroller at den avbruddsfrie og stabiliserte strømforsyningen (helseinstitusjonen) og/eller strømmeenheden er riktig tilkoblet og slått på.

	Slå av strømmeenheten og alt annet utstyr og slå dem på igjen. Oppdater plattformen.
Strømmeenheten er treg	Klikk på knappen «Reload streaming» (Last inn strømming på nytt) på plattformen. Oppdater siden med Ctrl+F5 og koble til plattformen igjen. Kontroller kvaliteten på nettverksforbindelsen. For å validere nettverksstatusen er det mulig å utføre en pingtest på enheten for å se om det er pakketap. Etter internettproblemer kan det hende at plattformen ikke fungerer som tiltenkt. Oppdater nettsiden og be om tilgang til den lokale brukeren igjen.
Tap av videoutgang	Det kan hende at en elektrostatisk utladning forårsaker tap av bilde. Etter en omstart av systemet skal kommunikasjonen og videostrømmingen gjenopprettes automatisk.

Seksjon 3.10 - Rengjøringsmetoder for maskinvare

- ☐ Sørg for at alt utstyr er koblet fra stikkontakten før rengjøringsprosessen startes.
- ☐ Ikke bruk slipende produkter.
- ☐ Ikke senk noe utstyr eller ekstrautstyr ned i noen form for væske.
- ☐ Kasser rengjøringsmaterialene i henhold til forskrifter for kassering av farlig avfall.
- ☐ Det anbefales ikke å bruke desinfeksjonsmiddel med spray, siden damp kan trenge inn i utstyret og forårsake kortslutning eller korrosjon.
- ☐ Dette produktet er ikke-sterilt

Kapittel 4 Cybersikkerhet og personvern

Seksjon 4.1 - Sikkerhets- og personvernrisikoer

nCommand Lite-systemet implementerer flere tekniske og organisatoriske tiltak for å beskytte behandlet informasjon.

Systemet er sertifisert i henhold til ISO/IEC 27001 og ISO/IEC 27701 og følger en tilnærming basert på personvern. Støtter overholdelse av lover om databeskyttelse i helsevesenet og cybersikkerhetsforskrifter som gjelder i EU, USA, Storbritannia, Sveits, Brasil, De forente arabiske emirater og Saudi-Arabia.

Men brukere må ta i bruk beste praksis for å forhindre unødvendig eksponering av sensitive data.

- Unngå å dele personlig eller sensitiv informasjon, med mindre det er strengt nødvendig.
- Sikre at kommunikasjon og systemtilgang finner sted i sikre miljøer.
- Hvis du mistenker skadelig aktivitet, varsler du det ansvarlige teamet umiddelbart.

Seksjon 4.2 - Personvern (GDPR / HIPAA Compliance)

nCommand Lite System overholder **GDPR, HIPAA, LGPD og ISO/IEC 27701**, som begrenser innsyn i behandlet data. All databehandling styres under rollen som «behandler» som definert av GDPR, med regional segregering (USA, EU, Brasil) for å forhindre grenseoverskridende overføringer.

Hvilke opplysninger samles inn?

- **Brukere:** Navn, e-post og bedrift (utelukkende for autentisering og tilgangsstyring).
- **Pasientdata:** Bare overføring av medisinske undersøkelser via strømming i sanntid, uten datalagring

Hvordan blir opplysningene lagret og beskyttet?

- Opplysningene brukes kun for **autentisering, tilgangskontroll og øktsporing**.
- Informasjonoverføring sikres via **AES-256-kryptering for lagring og TLS 1.3 for dataoverføring**.
- **Tilgangen er begrenset** og følger **prinsippet om minste privilegium (RBAC)**.
- Ende-til-ende-kryptering sikret for P2P-video og kontrollstrømmer via WebRTC.
- Autoriserte skyleverandører (f.eks. Microsoft Azure) behandler begrensede data under strenge kontraktsmessige sikkerhetstiltak.

Brukere tildeles følgende rettigheter:

- **Tilgang og korrigering** av personlig informasjon.

- **Forespørsel om datasletting**, hvor det er aktuelt.

Hvis du har spørsmål, kan du kontakte oss på privacy@ionic.health via e-post for å nå Health DPO. Alle forespørsler håndteres innen 30 dager, og kan utvides i henhold til GDPR.

Seksjon 4.3 - Tilgangsbehandling og autentisering

Brukere er ansvarlige for å definere **tilgangsroller og tillatelser** for teamene sine, og for å sikre jevnlig gjennomgang og dokumentasjon av innvilget tilgang.

Beste praksiser og kontroller

- Følg prinsippet om **minst privilegium (RBAC)**, som sikrer at brukere bare har tilgang til det som er relevant for deres roller.
- **Autentisering med flere faktorer (MFA)** er obligatorisk for administrativ tilgang og anbefales for alle brukere.
- **Sterke passord** kreves, med minst **8 tegn, inkludert store og små bokstaver, tall og tegn**.
- **Ikke del innloggingsdetaljer**.
- Tilgangstillatelser overvåkes og gjennomgås med jevne mellomrom.

Overvåking: Tilgang, tillatelsesendringer og viktige aktiviteter dokumenteres i systemets sikkerhetslogg. Logger oppbevares i minimum 6 år, i tråd med HIPAA, GDPR og andre gjeldende forskrifter. De støtter intern revisjon, rettsmedisinsk analyse og regulatorisk rapportering. Logger er beskyttet mot tukling og lagres i sikre miljøer med adgangskontroll.

Seksjon 4.4 - Datasikkerhet og integritet

nCommand Lite-systemet sikrer konfidensialiteten, integriteten og tilgjengeligheten av data gjennom industristandardiserte sikkerhetspraksiser.

Brukere bør sikre overholdelse av sikkerhetsprotokoller, jevnlig gjennomgå tilgangspolicyer og rapportere eventuelle avvik. Systemet overvåker kontinuerlig aktiviteter, og administratorer må håndheve sikkerhetspolicyer for å opprettholde et robust forsvar mot potensielle trusler.

Systemet er beskyttet av overvåking døgnet rundt gjennom et dedikert Security Operations Center (SOC) med SIEM-funksjoner for trusseldeteksjon og respons.

Seksjon 4.5 - Respons til sikkerhetshendelser

Systemet inkluderer en dokumentert hendelsesresponsplan, i tråd med ISO 27035 og NIST CSF.

I tilfelle det oppstår sikkerhetshendelser, som for eksempel uautorisert tilgang eller systemfeil, må brukerne følge disse trinnene:

Hvordan identifiserer jeg en hendelse?

- **Uautorisert tilgang** oppdaget i aktivitetslogg.
- **Mistenkelig forsøk på pålogging** eller gjentatte mislykkede autentiseringer.
- **Unormal systematferd**, f.eks. uventede handlinger eller feil.

Hvordan rapporterer jeg en hendelse?

Loggfør umiddelbart hendelsen via tilgjengelige støttekanaler (Kapittel 5).

Hvis et brudd på personopplysninger bekreftes, vil plattformens DPO varsle kontrolløren innen 48 timer og gi bevis og avbøtende detaljer.

Kapittel 5 Servicekanaler

Enten du trenger hjelp med et teknisk problem, et uklart trinn i prosessen eller ytterligere veiledning, er teamet vårt klart til å hjelpe deg. Du kan kontakte oss via telefon, e-post eller ITSM-plattformen, avhengig av hva som er mest praktisk for deg. Spesialistene våre er opplært i å tilby personlig assistanse, slik at eventuelle problemer løses raskt og effektivt.

Telefonnummer

USA	+1 (216) 2421223
Brasil	+55 12 3600 0181
Europa (Portugal)	+351 (300) 528 410

ITSM-plattformen

<https://ionichealth.desk.ms/?LoginPortal>

E-post

helpdesk@ionic.health



ADVARSEL!

Enhver alvorlig hendelse relatert til bruken av denne enheten skal rapporteres til både produsenten og helsemyndigheten / den kompetente myndigheten der enheten er installert.

Kontakt din lokale servicerepresentant eller rapporter til: helpdesk@ionic.health

Angi følgende informasjon:

- ☐ Systemversjonsnummeret, som vises på påloggingsskjermbildet;
- ☐ Hendelsesdato
- ☐ Beskrivelse av hendelsen, inkludert eventuell innvirkning/skade på pasient eller bruker;
- ☐ Kontaktinformasjonen din (institusjon, adresse, kontaktnavn, tittel og telefonnummer).

Kapittel 6 Juridisk og regulatorisk informasjon

Produsent

**IONIC HEALTH TECHNOLOGIES S.A.**

Estrada Dr. Altino Bondesan, 500, Sala 1103-A
Eugênio De Melo, CEP 12247-016, São José Dos Campos-SP, Brasil
CNPJ: 35.594.747/0001-08

+55 12 3600-0181

contato@ionic.health

Teknisk ansvarlig: Alexandre Seiji Fukuda Ribas - **CREA-SP:** 5071085437

ANVISA: 82585300004



nCommand Lite

Importør (USA)

**IONIC HEALTH USA INC.**

11201 Cedar Avenue, STE 600
Cleveland, OH 44106, USA

+1 (216) 242 1223



nCommand Lite System

EU-representant/-importør

**EUROPE IONIC HEALTH DIGITAL TECHNOLOGIES, LDA**

Rua de Raimundo Durães Magalhães, Lote 6/9
4475-189, Maia, Portugal

+351 (300) 528 410



nCommand Lite



Kontrollorganets identifikasjonsnummer: 2803

Grunnleggende UDI-DI: 7898974112NCLITE2L

Autorisert representant i Sveits (CH-REP) / Importør

**FREYR LIFE SCIENCES GMBH**

Bahnhofplatz
CH-6300 Zug
Sveits



nCommand Lite

Forespørsel om et trykt eksemplar

Du vil motta trykte eksemplarer av brukerhåndboken for nCommand Lite på forespørsel uten ekstra kostnad. Kontakt din lokale representant og be om et trykt eksemplar av brukerhåndboken.

Produksjonsdato

Datoen for programvareutgivelsen finnes på påloggingssiden til nCommand Lite, i et MÅNED/ÅR-format.

Kapittel 7 Revisjonshistorikk

Revisjon	Endre beskrivelse	Dato
0	Oppdatert håndbokversjon fra 2.1 til 2.2	15. august 2025

TILLEGG I - Sjekkliste for tjenestestart

1. *Kontroller elektriske tilkoblinger og nettverkstilkoblinger:*

Kontroller at de elektriske tilkoblingene og nettverkspunktene er riktig etablert på e-KVM-datamaskinen, skannerdatamaskinen og den lokale datamaskinen.

2. *Kontroller strømstatus:*

Kontroller at den avbruddsfrie og stabiliserte strømforsyningen og e-KVM-datamaskinen er slått på og fungerer som de skal.

3. *Hurtigtilgang til nC Lite-plattformen:*

Bekreft tilstedeværelsen av snarveien til nC Lite-plattformen på skrivebordet for rask tilgang.

4. *Tilgang til og pålogging på nC Lite-plattformen:*

Åpne nCommand-plattformen og logg på for å sikre full tilgang og riktig funksjonalitet.

5. *Oppsett av chat-applikasjonen:*

Åpne chat-applikasjonen i nC Lite-plattformen i bare én fane og unngå å minimere den for sømløs kommunikasjon.