

Target CI v1.5

VEILEDNING I CYBERSIKKERHET

Norsk

Oppdatert: september 2025



A Sonova Brand

Innhold

1. INNLEDNING	4
1.1 FORKORTELSER OG DEFINISJONER:.....	4
2. ANDRE RESSURSER.....	4
2.1 KUNDESUPPORT	4
2.2 AB PRO PORTAL	4
2.3 AVANSERT INSTALLASJONSVEILEDNING	4
2.4 MDS2	5
2.5 BRUKSANVISNING (IFU).....	5
2.6 HIMSA	5
3. NETTVERKS- OG KONTEKSTDIAGRAMMER.....	5
3.1 UTPLASSERINGSMODDELL 1: FRITTSTÅENDE	6
3.2 UTPLASSERINGSMODDELL 2: NOAH DISTRIBUTED	6
3.3 UTPLASSERINGSARTEFAKTER	7
3.4 SYSTEMSAMMENKOBLINGER.....	8
4. SYSTEMKRAV	9
5. INSTALLASJONS-.....	10
5.1 KRAV	10
5.2 INSTALLASJONSPROGRAMTYPER	10
6. SIKKERHETSKONTROLLER	10
6.1 AUTENTISERING – FRITTSTÅENDE UTPLASSERING.....	10
6.2 AUTENTISERING – NOAH-UTPLASSERING	10
6.3 AUTORISASJON	11
6.4 REVISJON – FRITTSTÅENDE UTPLASSERING	11
6.5 REVISJON – NOAH-UTPLASSERING.....	11
6.6 FJERNTILGANG	11
7. INFORMASJONSBEKYTTELSE	11
7.1 PERSONVERNERKLÆRING FOR ADVANCED BIONICS	11
7.2 AMERIKANSKE FØDERALE STANDARDER FOR INFORMASJONSBEHANDLING (FIPS)	11
7.3 SIKKERHET UNDER OVERFØRING.....	12
7.4 SIKKERHET FOR LAGREDE DATA	12
8. PROGRAMVAREINTEGRITET	14
8.1 VERIFISERING AV NEDLASTET INSTALLASJONSMEDIUM.....	14
8.2 MANUELL VERIFISERING AV TILPASNINGSPROGRAMVAREN FØR INSTALLASJON	15

8.3	AUTOMATISK VERIFISERING AV INTEGRITETEN TIL INSTALLERT TILPASNINGSPROGRAMVARE	16
8.4	MANUELL VERIFISERING AV INTEGRITETEN TIL INSTALLERT TILPASNINGSPROGRAMVARE.....	16
9.	PROGRAMVAREOPPDATERINGER OG PATCHER.....	17
10.	DATABEHANDLING	18
10.1	DATABASER.....	18
10.2	DATAMIGRASJON	18
10.3	KONFIGURASJONER AV HØREAPPARATER	18
10.4	DATADESTRUKSJON	18
11.	SIKKERHETSMILJØ – DELT ANSVAR.....	18
12.	PRODUKSJONS- OG PROGRAMVAREUTVIKLINGSPROSESS	20
13.	PROGRAMVAREKOMPONENTER OG STYKKLISTE	20
14.	REFERANSER.....	27

1. INNLEDNING

Dette dokumentet gir teknisk informasjon om sikkerhet og personvern for Target CI v1.5 programvaresystem fra Advanced Bionics, heretter kalt «tilpasningsprogramvaren.» Tilpasningsprogramvaren er utviklet for bruk av kvalifiserte audiografer for å konfigurere (dvs. tilpasse) høreapparater for pasienter som har fått cochleaimplantater fra Advanced Bionics.

Dette dokumentet fokuserer spesielt på hensynene til cybersikkerhet og personvern som er relevante for bruken av tilpasningsprogramvaren. Den inkluderer en evaluering av sikkerhets- og personvernkontrollene som for øyeblikket er integrert i programvaren, samt de som forventes å bli brukt og konfigurert i IT-miljøet der produktet skal brukes til det tiltenkte formålet.

Dette dokumentet inneholder ikke teknisk sikkerhets- og personverninformasjon om:

- Tidligere versjoner av AB-tilpasningsprogramvaren
- Annen AB-programvare enn Target CI v1.5
- AB-nettsteder
- AB mobilapplikasjoner
- AB høreapparater

1.1 FORKORTELSER OG DEFINISJONER:

Forkortelse	Begrep
FSW	Tilpasningsprogramvare
HCP	Audiograf
SaMD	Programvare som medisinsk utstyr
AB	Advanced Bionics
IFU (Bruksanvisning)	Bruksanvisning

2. ANDRE RESSURSER

2.1 KUNDESUPPORT

For de som befinner seg innenfor USA og Canada, tilbyr Advanced Bionics et gratis telefonnummer for teknisk støtte (877-271-6727) der dedikert profesjonell support er tilgjengelig fra mandag til fredag fra kl. 05.00 til 17.00 (PST).

Hvis du befinner deg utenfor USA og Canada, leveres teknisk support lokalt. Hvis du har spørsmål om tilpasningsprogramvaren, tilhørende maskinvare eller andre programmeringsspørsmål, kontakter du din lokale AB-representant.

2.2 AB PRO PORTAL

Tilpasningsprogramvaren og tilhørende dokumentasjon kan lastes ned fra <https://www.abproportal.com> eller Sonova Web Client. En kontoinnlogging er nødvendig. Denne ressursen er muligens ikke tilgjengelig i alle markeder. Kontakt din AB-representant for mer informasjon.

2.3 AVANSERT INSTALLASJONSVEILEDNING

Den avanserte installasjonsveiledningen for Target CI v1.5 er tilgjengelig på forespørsel. Veiledningen gir teknisk informasjon om installasjonsprogrammet for tilpasningsprogramvaren, inkludert kommandolinjealternativer for stille og automatiserte installasjoner.

2.4 MDS2

Produsentens erklæring om sikkerhet for medisinsk utstyr (MDS2) er et bransjestandard skjema som inneholder svar om sikkerhet og personvern om ABs tilpasningsprogramvare. Skjemaet er tilgjengelig på forespørsel.

2.5 BRUKSANVISNING (IFU)

Bruksanvisningen leveres med programvareinstallasjonsmediet. For enkelte markeder er den elektroniske bruksanvisningen tilgjengelig for nedlasting på www.advancedbionics.com/ifu

Følgende avsnitt i bruksanvisningen kan være relevante for IT-fagfolk:

- Produktbeskrivelse
- Minimumskrav for system og ytelsesegenskaper
- Retningslinjer for IT-sikkerhet
- Installasjonsinstruksjoner
- Teknisk support

2.6 HIMSA

HIMSA er en tredjeparts programvareleverandør som produserer Noah System 4, et programvaresystem utviklet for hørselsbransjen som gir audiografer et leverandøruavhengig system for å utføre klientrelaterte oppgaver.

Tilpasningsprogramvaren kan eventuelt konfigureres til å bruke Noah System 4 til datalagring i stedet for en lokal database.

HIMSAs sikkerhetsnettside gir svar på vanlige IT-sikkerhetsspørsmål om Noah System 4.

<https://www.himsa.com/support/noah-enterprise-support/security-questionnaire-support/>

<https://www.himsa.com/support/noah-enterprise-support/security-considerations/>

Se sikkerhetsdelen av HIMSA-læringssenteret for ytterligere sikkerhetsinformasjon:

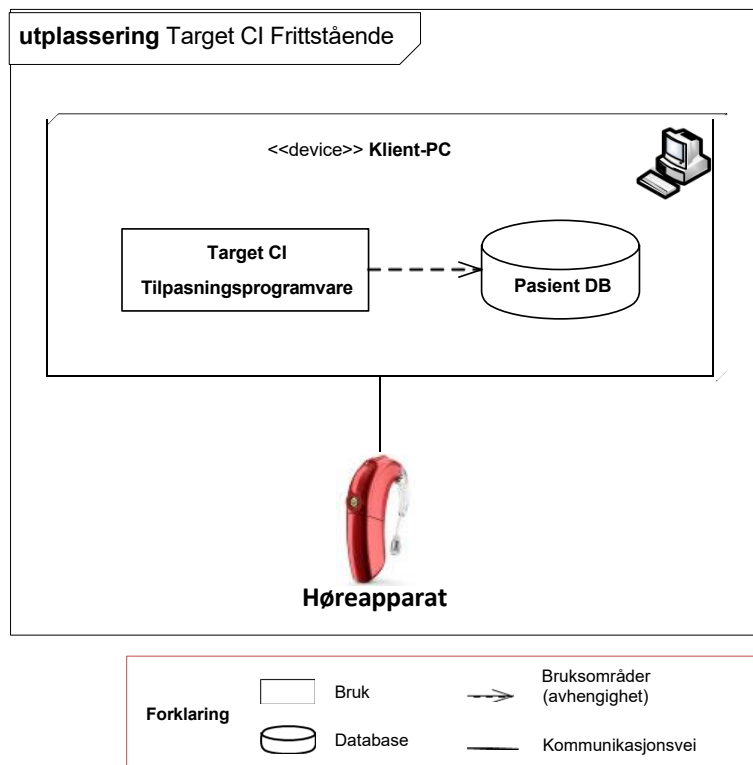
<https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/>

3. NETTVERKS- OG KONTEKSTDIAGRAMMER

To distribusjonsmodeller støttes for tilpasningsprogramvaren, som er et klientprogram (SaMD) installert på en kommersielt tilgjengelig, standard Microsoft Windows-PC. Programvaren inkluderer ikke maskinvare eller operativsystem.

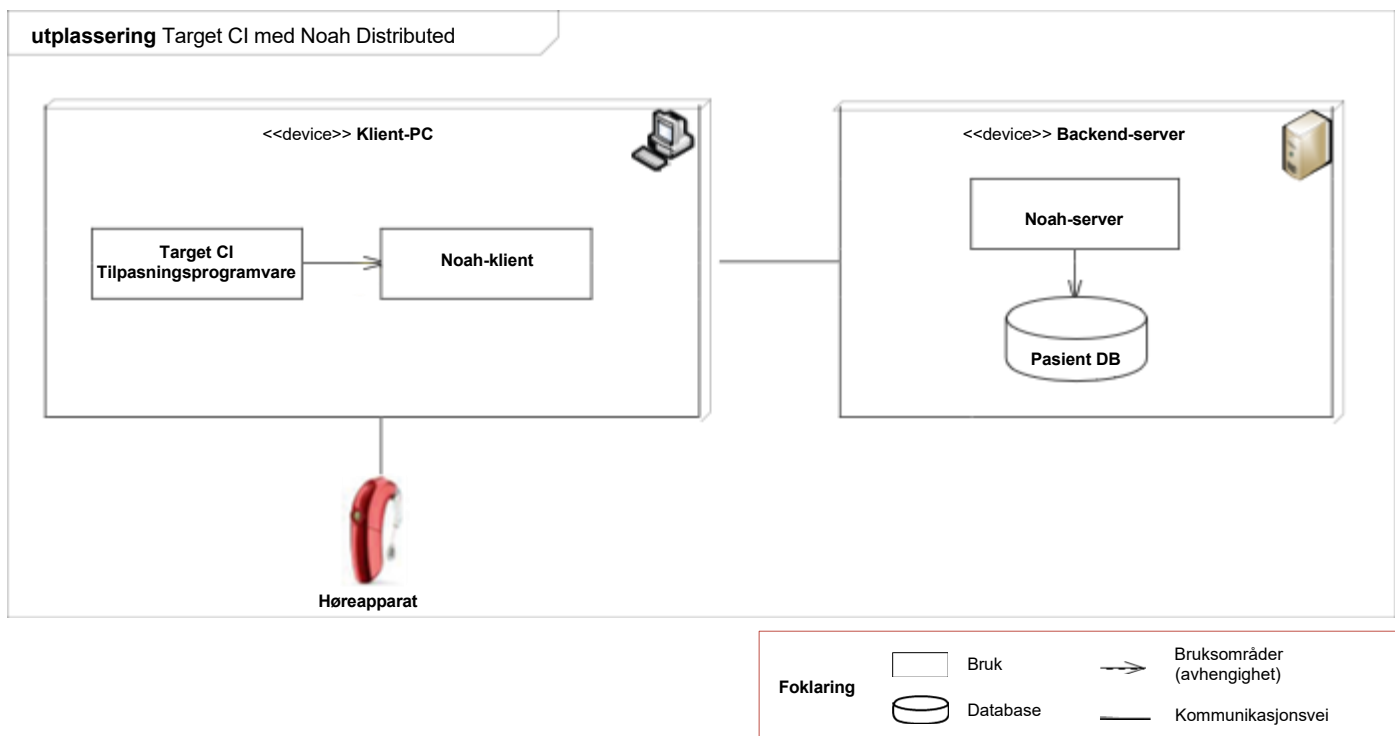
3.1 UTPLASSERINGSMODELL 1: FRITTSTÅENDE

I den frittstående utplasseringsmodellen installeres tilpasningsprogramvaren på en klient-PC. Pasientdatabasen lagres på samme PC og installeres sammen med tilpasningsprogramvaren.



3.2 UTPLASSERINGSMODELL 2: NOAH DISTRIBUTED

I Noah Distributeds utplasseringsmodell installeres tilpasningsprogramvaren til én eller flere klient-PC-er. Noah, et tredjeparts pasientbehandlingssystem, er utplassert på en intern server som er tilgjengelig for klient-PC-ene. Pasientdatabasen lagres på Noah-serveren og er tilgjengelig over nettverket fra én eller flere klient-PC-er.



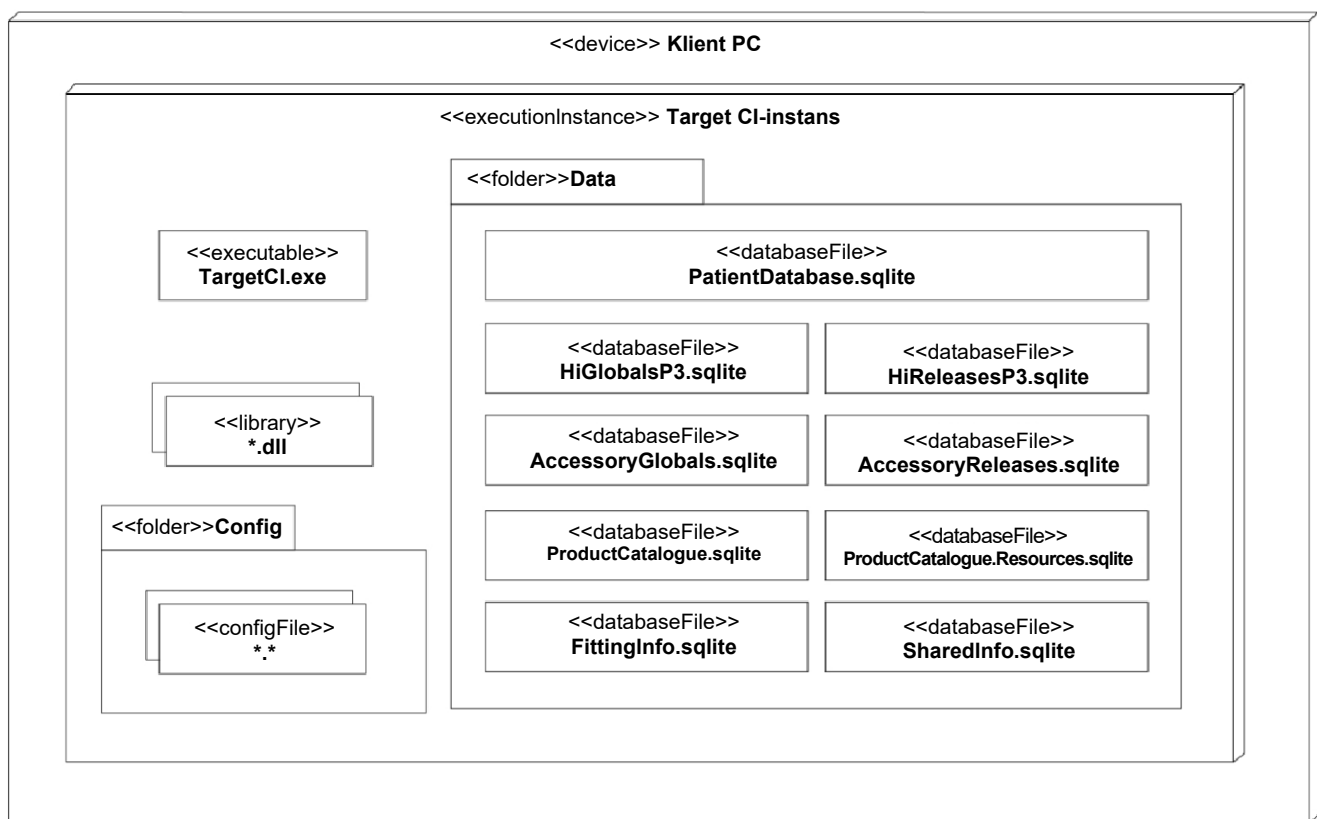
3.3 UTPLASSERINGSARTEFAKTER

Tilpasningsprogramvaren installeres med en kjørbar fil og et sett tilhørende filer, inkludert komponent-DLL-er, konfigurasjonsfiler og SQLite-databasefiler. Konfigurasjonsfilene er installert i mappen «%ProgramData%\ Advanced Bionics\Target CI\Target CI\Config» og databasefiler er installert i mappen “%ProgramData%\Advanced Bionics\Target CI\Target CI\Data.» Mappen Data inneholder én transaksjonsdatabasefil og flere informasjonsdatabasefiler.

Transaksjonsdatabasen, PatientDatabase.sqlite, lagrer pasientens demografiske data og tilpasningsdata, og installeres kun når tilpasningsprogramvaren utplasseres i frittstående modus.

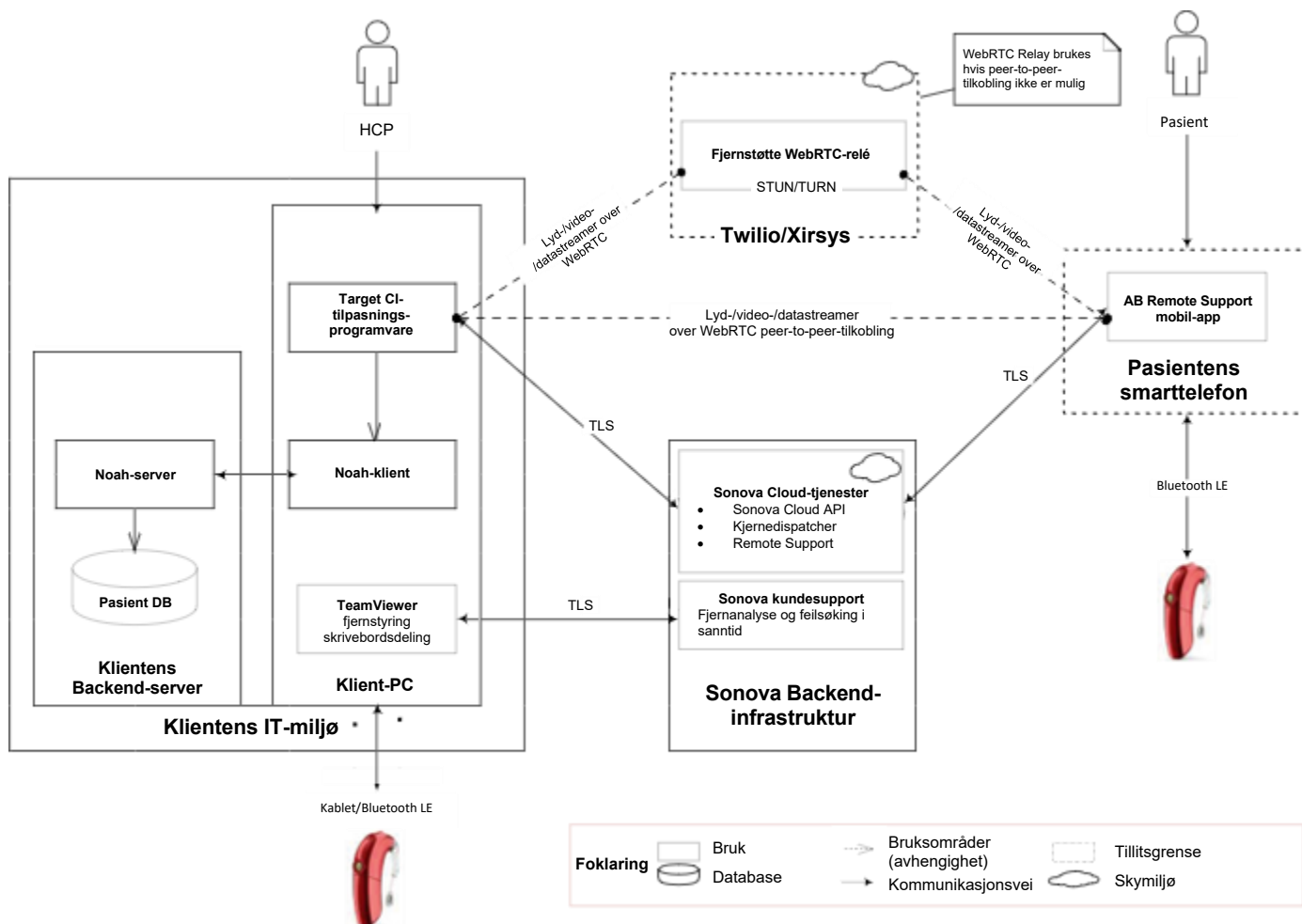
Når tilpasningsprogramvaren utplasseres som en Noah-modul, leverer Noah-systemet de nødvendige tjenestene for lagring av pasientdata til tilpasningsprogramvaren. De resterende sqlite-filene er en integrert del av tilpasningsprogramvaren og kreves for alle utplasseringsmodeller.

utplassering Target CI-artefakter



3.4 SYSTEMSAMMENKOBLINGER

Diagrammet og tabellen nedenfor illustrerer de primære systemsammenkoblingene. Vanligvis blir bare en del av de tilgjengelige sammenkoblingene utnyttet.



Kilde / destinasjon	Tjeneste	Protokoll	Port	Beskrivelse
Høreapparater	Kommunikasjon med høreapparater	Kablet tilkobling / Bluetooth® Lav energi	Ikke tilgjengelig	Brukes til kommunikasjon med høreapparater for kontroll, konfigurasjon og lesing av status og data.
Noah	Noah 4 ModuleAPI	.NET Remoting	Ikke tilgjengelig	Primærgrensesnittet for modulen som brukes til å få tilgang til Noah-programvaren (kun i Noah distribuert utplasseringsmodell)
Sonova Cloud-tjenester	Sonova Cloud API, kjernedispatcher, fjernstøtte	SOAP, REST	443	Sonova-tjenester som ligger i et Microsoft Azure-datasenter brukes til å: - hente konfigurasjonsdata for tilpasningsprogramvareklienten fra Sonovas backend-lagring - overføre logg- og analysedata

Kilde / destinasjon	Tjeneste	Protokoll	Port	Beskrivelse
				opprette fjerntilpasningsøker i sanntid
Twilio/Xirsys, AB Remote Support mobilapp	Remote Support	WebRTC	Liste over porter tilgjengelig på forespørsel	Twilios skykommunikasjonstjenester driftes på tredjeparts skyplattformer, nærmere bestemt Amazon Web Services (AWS) og Google Cloud Platform (GCP). Disse tjenestene brukes utelukkende av fjernstøttefunksjonen i tilpasningsprogramvaren, som muliggjør WebRTC-signaler og fjerntilpasningsøker i sanntid.
AB kundesupport	Skrivebordsdeling	TeamViewer proprietær protokoll	5938, 443, 80 Se TeamViewerPorts	Brukes til å utføre ekstern sanntidsanalyse og feilsøking av problemer som påvirker installasjoner av tilpasningsprogramvare. Se avsnitt 6.6 FJERNSERVICE for mer informasjon.

4. SYSTEMKRAV

Operativsystem	64-bit Windows 10 Pro/Enterprise
.NET Framework	Versjon 4.8
CPU	Intel® Core™ i5 eller tilsvarende med lik eller bedre ytelse
RAM	4 GB eller mer
Harddiskplass	3 GB eller mer
Minimumskrav for skjerm	1280 x 1024 oppløsning (maksimal skalering 125 %) 24-bits farge
Enhetsdrivere	- Noahlink Wireless-driver (nyeste versjon tilgjengelig fra HIMSA kreves hvis du bruker et tredjeparts USB-tilkoblet Noahlink Wireless-programmeringsgrensesnitt). - CPI-3-driver (påkrevd hvis du bruker et USB-tilkoblet CPI-3-programmeringsgrensesnitt).
Database	SQLite eller Noah System 4 (versjon 4.14 eller høyere)
Internett-tilkobling	Internett-tilkobling kreves for fjernstøtte og analyselogging, se avsnitt 4.4 Systemtilkoblinger; intranett kreves ved bruk av nettverkstilkoblet Noah System 4.
Nettverksporter	Se avsnitt 3.4 Systemsammenkoblinger; se avsnitt 3. Andre ressurser – HIMSA for porter brukt av Noah System 4.

5. INSTALLASJONS-

5.1 KRAV

En administratorkonto er nødvendig for å installere tilpasningsprogramvaren. Når programvaren er installert, kan den kjøres uten administratorrettigheter eller utvidede tillatelser.

Se avsnitt 8, Programvareintegritet, for informasjon om validering av programvarens integritet før installasjon.

Før installasjon anbefales det at systemadministratorer sørger for at:

- versjonen av tilpasningsprogramvaren som skal installeres er den nyeste tilgjengelige.
- det underliggende operativsystemet er oppdatert.

5.2 INSTALLASJONSPROGRAMTYPER

To installasjonsprogrammer er tilgjengelige for å installere tilpasningsprogramvaren:

- Installasjonsprogrammet Standard
- Installasjonsprogrammet IT Professional

Installasjonsprogrammet IT Professional er én MSI-fil og ekskluderer nødvendige komponenter, men er ellers tilsvarende installasjonsprogrammet Standard.

Forutsetningskomponenter inkluderer Microsoft .NET Framework v4.8 og Microsoft Visual C++ Omdistribuerbare pakker.

Begge installasjonsprogrammene støtter avanserte installasjonsscenarier, inkludert stille installasjon.

Installasjonsprogrammet IT Professional bør bare brukes hvis organisasjonen din krever at nødvendige komponenter installeres og administreres av organisasjonen din, og ikke av installasjonsprogrammet til tilpasningsprogramvaren. Installasjonsprogrammet Standard bør brukes i alle andre tilfeller.

Installasjonsprogrammet IT Professional kan fås fra ABs kliniske representant. Installasjonsprogrammet IT Professional kan ikke brukes til å reparere, installere på nytt eller avinstallere installasjoner fra standardinstallasjonsprogrammet. Installasjonsprogrammet Standard kan ikke brukes til å reparere, installere på nytt eller avinstallere installasjoner av IT-profesjonelle installasjonsprogrammer.

6. SIKKERHETSKONTROLLER

Tilpasningsprogramvaren er et klientprogram som er installert på en kommersiell Microsoft Windows-PC. Tilpasningsprogramvaren kan installeres som et frittstående program eller som en Noah-modul.

6.1 AUTENTISERING – FRITTSTÅENDE UTPLASSERING

Når tilpasningsprogramvaren installeres som et frittstående program, er den avhengig av tilgangskontrollmekanismene som tilbys av vertsoperativsystemet. Vertsoperativsystemet kan konfigureres av kundens IT-personell til å administrere autentisering. Tilpasningsprogramvaren har ingen slik integralfunksjon. Advanced Bionics anbefaler at hver bruker logger seg på verts-OS-et med en unik konto per bruker.

6.2 AUTENTISERING – NOAH-UTPLASSERING

Når tilpasningsprogramvaren installeres som en Noah-modul, leveres tilgangskontroll av Noah System 4. Se www.HIMSA.com for revisjonskontroller som brukes av Noah System 4.

6.3 AUTORISASJON

Tilpasningsprogramvaren begrenser ikke tilgangen til funksjonene basert på rollene til individuelle brukere. Programvaren støtter én hovedfunksjon med å tilpasse pasientens høreapparater og én rolle som tilpasningspersonell. Rollebasert tilgangskontroll er ikke relevant.

6.4 REVISJON – FRITTSTÅENDE UTPLASSERING

Når tilpasningsprogramvaren installeres som et frittstående program, er den avhengig av revisjonsmekanismene som tilbys av vertsoperativsystemet. Tilpasningsprogramvaren har ingen slik integralfunksjon. Vertsoperativsystemet kan konfigureres av kundens IT-personell til å logge oppstarter/bruk av tilpasningsprogramvaren og brukerpålogginger. Advanced Bionics anbefaler at hver bruker logger seg på verts-OS-et med en unik konto per bruker for å forenkle revisjon.

6.5 REVISJON – NOAH-UTPLASSERING

Når tilpasningsprogramvaren installeres som en Noah-modul, leveres revisjonslogger av Noah-systemet. Se <https://www.himsa.com/> for revisjonskontroller brukt av Noah System 4.

6.6 FJERNILGANG

Funksjonen for deling av skrivebord muliggjør fjernanalyse og feilsøking i sanntid av problemer som påvirker installasjoner av tilpasningsprogramvaren. Denne funksjonen er basert på tredjepartsverktøyet TeamViewer QuickSupport (distribuert som standard sammen med tilpasningsprogramvare) og lar ABs kundesupportmedarbeidere eksternt koble seg til audiografens datamaskin og få full kontroll over den på skrivebordet, inkludert tilgang til det underliggende operativsystemet og filsystemet.

For å opprette en skrivebordsdelingsøkt kreves det interaksjon fra audiografen. Audiografen skal først kjøre TeamViewer QuickSupport-verktøyet (f.eks. gjennom tilpasningsprogramvaren Target CI) og kommunisere TeamViewer ID-legitimasjonen sin til AB-supportteamet via en eksternt kommunikasjonskanal (f.eks. telefonsamtale).

Navnet og TeamViewer-ID-en til AB-supportmedlemmet vises som standard på audiografens dataskjerm under hver aktive skrivebordsdelingsøkt.

All nettverkstrafikk for deling av skrivebord er sikret og oppfyller eller overgår standarder for kryptografiske protokoller og algoritmer (RSA) public/private nøkkelutveksling og AES 256-bits øtkryptering).

TeamViewer QuickSupport kan fjernes manuelt uten at det påvirker andre funksjoner i Target FSW. Target FSW-installasjonsprogrammet støtter en kommandolinjeparameter for å tillate en Target FSW-kommandolinjeinstallasjon uten å inkludere TeamViewer QuickSupport-verktøyet.

7. INFORMASJONSBEKYTTELSE

7.1 PERSONVERNERKLÆRING FOR ADVANCED BIONICS

Personvernerklæringen som beskriver hvordan Advanced Bionics samler inn, overfører, lagrer og bruker personopplysninger, kan lastes ned fra: AdvancedBionics.com/privacy.

Advanced Bionics verken er vert for, lagrer, sikkerhetskopierer eller har tilgang til data som er lagret i tilpasningsprogramvaren eller Noah-databasene, med mindre dataene uttrykkelig sendes til Advanced Bionics.

7.2 AMERIKANSKE FØDERALE STANDARDER FOR INFORMASJONSBEHANDLING (FIPS)

Target CI v1.5 er kompatibel med FIPS 140-2-krypteringsstandardene.

7.3 SIKKERHET UNDER OVERFØRING

Kommunikasjonssikkerhet er sikret og aktivert i all innkommende og utgående nettverkskommunikasjon for tilpasningsprogramvaren. Med unntak av fjernstøttefunksjonen (som bruker WebRTC-protokollen) og Bluetooth-kommunikasjon med høreapparater og tilbehør, alle andre tilkoblinger er beskyttet av Transport Layer Security (TLS)-protokollen som gir konfidensialitet, integritet og autentisitet.

TLS

TLS-konfigurasjonen er i samsvar med gjeldende beste praksis og sikkerhetsanbefalinger dokumentert i BCP 195 – Anbefalinger for sikker bruk av TLS og DTLS, BCP195, inkludert:

- støtter ikke SSL- og TLS-versjoner før 1.2
- støtter ikke krypteringspakker som bruker kryptografiske algoritmer som tilbyr mindre enn 128 bits sikkerhet
- støtter anbefalte TLS-utvidelser av BCP 195
- støtter ikke usikre utvidelser av BCP 195

DTLS

Kryptering er en obligatorisk funksjon i WebRTC og håndheves på alle mediestrømmer som sendes over WebRTC. Krypteringsprotokollen som brukes avhenger av kanaltypen; datastrømmer krypteres med DTLS og mediestrømmer krypteres med Secure Real-time Transport Protocol (SRTP) som brukes fordi det er et lettere alternativ enn DTLS.

Se følgende lenke for mer detaljert informasjon om sikkerhetskongfigurasjon av Remote Support WebRTC:

<https://developer.liveswitch.io/liveswitch-server/server/security.html>

BLE

Trådløs Bluetooth Low Energy-kommunikasjon med høreapparater og tilbehør er kryptert og integritetsbeskyttet som standard (med unntak av bruk i identifikasjons- og deteksjonstilfeller). I tillegg til dette er varigheten av høreapparatets Bluetooth-paringsmodus tidsbegrenset. Se tilgjengelig dokumentasjon for høreapparater for mer detaljert beskrivelse av sikkerheten til Bluetooth-kommunikasjonskanalen.

7.4 SIKKERHET FOR LAGREDE DATA

Pasientdatabase – Frittstående utplasseringsmodell

Hvis tilpasningsprogramvaren installeres som et frittstående program, lagres pasientdatabasen lokalt på:
C:\ProgramData\Advanced Bionics\Target CI\Target CI\Data

Disse postene krypteres ikke som standard når de er lagret. Beskyttet helseinformasjon (PHI) og personlig identifiserbar informasjon (PII) lagres i en database som er intern i tilpasningsprogramvaren og overføres ikke over nettverket.

I enkelte jurisdiksjoner kan forskrifter kreve kryptering av alle pasientdata for å unngå potensielle ansvarsforhold i tilfelle datatap eller tyveri. Aktiver BitLocker eller tilsvarende fulldiskkryptering (på OS-nivå eller maskinvarebasert) for å beskytte dataene mot uautorisert tilgang eller kopiering mens dataene er lagret.

BitLocker er en innebygd Windows-funksjon som krypterer hele harddisken og krever autentisering for å få tilgang. Se alltid Microsofts offisielle veiledning og organisasjonens IT-sikkerhetspolicy før du aktiverer BitLocker.

Slik aktiverer du BitLocker

Det kreves administratorrettigheter for å administrere BitLocker.

1. Søk etter «Administrer BitLocker»

Åpne Start-menyen, skriv inn «Administrer BitLocker», og velg den fra søkeresultatene.

2. Velg systemstasjonen

Velg stasjonen der Windows er installert for å konfigurere krypteringsinnstillinger.

3. Velg en opplåsningsmetode

Velg ett av de følgende alternativene:

- Kun TPM
- TPM + PIN-kode
- TPM + USB-nøkkel

Følg Microsofts beste praksis og organisasjonens IT-sikkerhetspolicy når du velger opplåsningsmetode.

4. Sikkerhetskopier gjenopprettingsnøkkelen

Sikkerhetskopier gjenopprettingsnøkkelen ved hjelp av sikre, bedriftsgodkjente metoder. Anbefalte alternativer inkluderer:

- Lagring i Microsoft Entra ID (tidligere Azure AD) eller Active Directory for domenetilknyttede enheter
- Lagring på en sikker, tilgangskontrollert nettverksplassering med kryptering og revisjonslogging
- Bruk av en administrert nøkkeldeponeringsløsning godkjent av organisasjonen din

Unngå å lagre nøkkelen på lokale stasjoner, USB-er eller skrive den ut med mindre det er uttrykkelig tillatt i retningslinjene. Gjenopprettingsnøkler må beskyttes med samme strenghet som annen sensitiv påloggingsinformasjon og roteres umiddelbart hvis de blir eksponert.

5. Start kryptering

Velg:

- Hele harddisken – anbefales for de fleste bedriftsscenarioer. Krypterer alle sektorer, også ubrukt plass, slik at slettede data ikke kan gjenopprettes.

Pasientdatabase – Noah Distributed Deployment-modul

Når tilpasningsprogramvaren installeres som en Noah-modul, lagres PII i pasientdatabasen som Noah drifter.

Pasientdatabasen som Noah drifter, kan ligge på en annen maskin. PII og andre pasientdata vedlikeholdes av Noah-programvaren, og krypteringen av pasientens lagrede data er sikret av Noah-systemet. Tilpasningsprogramvaren kan sende eller motta PII over en kablet eller trådløs nettverkstilkobling når en Noah-database er konfigurert for nettverkstilgang.

PII lagret i den nettverkstilkoblede Noah-databasen vil være synlig for andre enhetsbrukere på forskjellige PC-er som har tillatelser til den samme nettverkstilkoblede databasen. Noah-databasen kan også konfigureres for ikke-nettverkstilgang og installeres på samme PC som tilpasningsprogramvaren.

Noah hindrer tilpasningsprogramvaren i å få tilgang til pasientjournaldatabasen. Når en bruker åpner en pasient i tilpasningsprogramvaren via Noah-klienten, kan tilpasningsprogramvaren bare lese fra og skrive til den gjeldende åpne pasientjournalen, og den kan ikke få tilgang til andre pasientjournaler i Noah-databasen.

Se avssnitt www.HIMSA.com for krypteringsstandarder som brukes av Noah System 4.

RMA-eksportfiler

Tilpasningsprogramvaren tillater eksport av klientinformasjon til en fil. RMA-filen kan sendes til Advanced Bionics for å løse RMA- eller relaterte støtteproblemer.

RMA-filen er asymmetrisk RSA-kryptert med en nøkkellengde på 512 bit. Tilpasningsprogramvaren har ingen funksjon for å dekryptere en RMA-fil.

Anonymiserte eksportfiler

Tilpasningsprogramvaren tillater eksport av klientinformasjon til en klientanonymisert fil. Klientens personlig identifiserbare informasjon, som fødselsdato og navn, erstattes med generiske verdier. Filen er ikke kryptert og kan importeres til enten samme eller en annen installasjon av tilpasningsprogramvaren.

Standard eksportfiler

Tilpasningsprogramvaren tillater eksport av klientinformasjon til en standard eksportfil. Filen bruker et proprietært binært format og er ikke kryptert. Filen kan importeres til samme eller en annen installasjon av tilpasningsprogramvaren. Når denne funksjonen brukes, må brukere av tilpasningsprogramvaren sørge for at standard eksportfiler håndteres i henhold til deres lokale IT-policyer for håndtering av ukryptert personopplysninger.

Høreapparat

Tilpasningsprogramvaren lagrer klientinformasjon på klientens høreapparat. Personlig identifiserbar informasjon som klientens navn og fødselsdato lagres ikke på høreapparatet. Annen informasjon som ikke er personlig identifiserende informasjon lagres ved hjelp av PBKDF2-kryptering med en 128-biters nøkkel.

Tilpasningsprogramvaren kan sende eller motta ikke-personidentifiserbar klientinformasjon til eller fra et høreapparat via en proprietær kablet enhet (f.eks. CPI-3), mobilappen AB Remote Support eller en Noahlink Wireless-enhet. Noahlink Wireless-enheten kobles til høreapparatet ved hjelp av Bluetooth Low Energy (BLE) via en standard BLE-kanal med 128-bit AES-kryptering.

8. PROGRAMVAREINTEGRITET

8.1 VERIFISERING AV NEDLASTET INSTALLASJONSMEDIUM

Installasjonsmediet for Target CI-tilpasningsprogramvaren kan i enkelte regioner lastes ned fra Advanced Bionics' Pro Portal eller Sonova Web Client. Det nedlastede installasjonsmediet kan autentiseres ved hjelp av et hvilket som helst pålitelig SHA-256 hashing-verktøy.

SHA256-hashen for standard zip-fil for installasjon er:

A42B8F41A5A4111D1CDF67394FFBBFBCDF2FB6215EC2696DB310B3AED6D4DD83

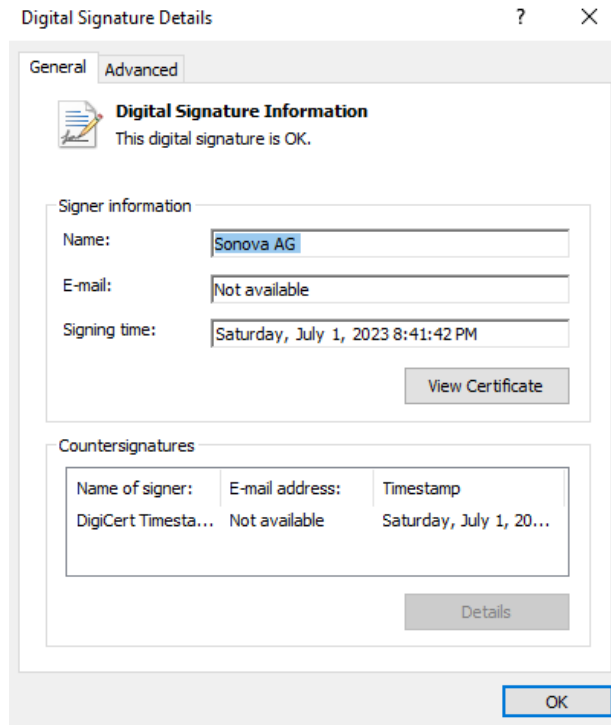
SHA256-hashen for zip-filen for IT Professional-installasjoner er:

DDAD362CC3213EFEA702D9F4A61740B34EDF794FE997811B6B2C908CE754B25F

8.2 MANUELL VERIFISERING AV TILPASNINGSPROGRAMVAREN FØR INSTALLASJON

Brukere kan utføre følgende trinn for å bekrefte tilpasningsprogramvarens integritet og autentisitet før installasjon:

1. Åpne Windows Explorer og gå til rotmappen på installasjonsmediet for tilpasningsprogramvaren. Hvis installasjonsmediet er en minnepenn, setter du den inn i en USB-port og går til rotmappen. Hvis installasjonsmediet er en zip-fil, pakk den ut til en mappe og gå til den mappen.
2. Høyreklikk på SonovaVerify.exe, og velg Egenskaper fra hurtigmenyen.
3. Velg fanen Digitale signaturer.
4. Dobbeltklikk på SHA256 «Sonova AG»-signaturen.
5. Bekreft at elementene i signaturen er gyldige. Kontroller spesielt at meldingen «The digital signature is OK.» (Den digitale signaturen er OK) vises nær toppen, og at underskriverens navn og signeringstidspunkt samsvarer med det følgende bildet:



1. Lukk popup-dialogboksene og dobbeltklikk på SonovaVerify.exe.
2. Bekreft at «NO ERRORS DETECTED.» (INGEN FEIL OPPDAGET) vises som vist på bildet nedenfor:

```
FILES PROCESSED: 79
IGNORED FILES: 1
.\sonovaverify.dat
NO ERRORS DETECTED.
Press any key to continue . . .
```

Bildet viser at SonovaVerify har autentisert og verifisert digitale signaturer for alle filer på installasjonsmediet, inkludert installasjonsprogrammet. Dette bekrefter at installasjonsmediet ikke har blitt tuklet med, ødelagt eller på annen måte kompromittert. SonovaVerify vil vise advarsler eller feilmeldinger hvis filer eller mapper mangler, eller uventede filer eller mapper er lagt til installasjonsmediet.

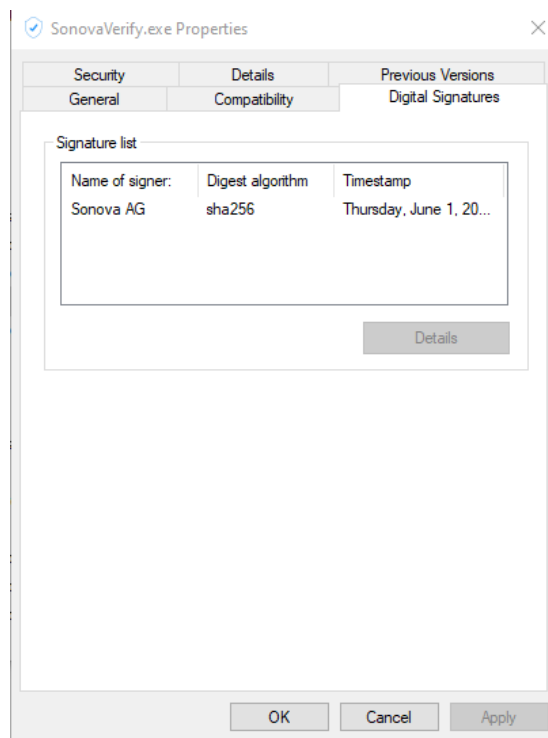
8.3 AUTOMATISK VERIFISERING AV INTEGRITETEN TIL INSTALLERT TILPASNINGSPROGRAMVARE

SonovaVerify er integrert med tilpasningsprogramvaren og kjører hver gang programmet startes for å bekrefte integriteten til tilpasningsprogramvarens programfiler. Programfilene signeres digitalt ved hjelp av bransjestandardpraksis og sertifikater utstedt av en pålitelig sertifiseringsinstans. Programvaren varsler brukeren via advarselmeldinger hvis programfiler er kompromittert.

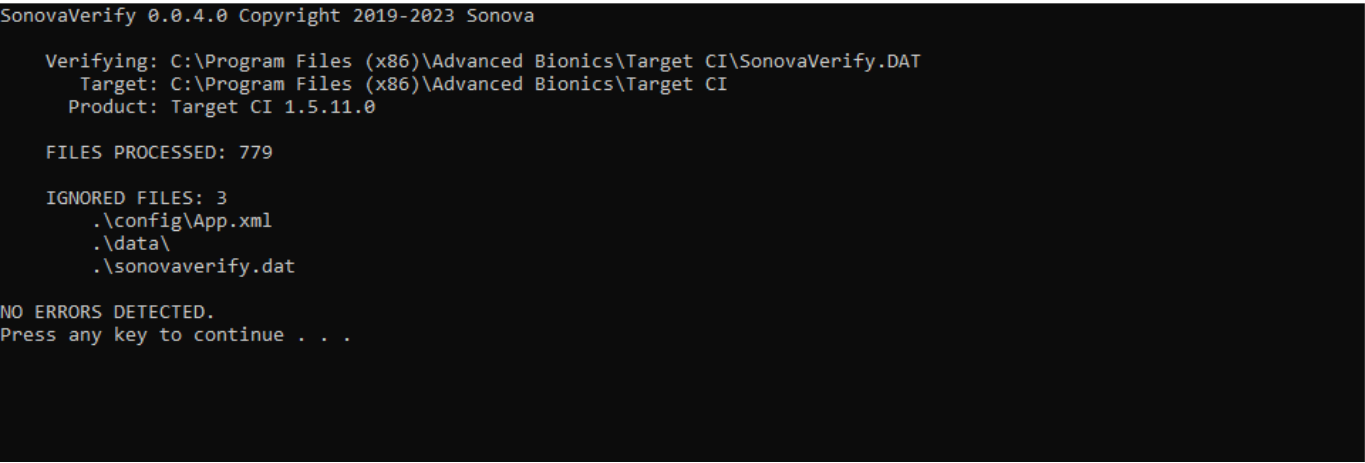
8.4 MANUELL VERIFISERING AV INTEGRITETEN TIL INSTALLERT TILPASNINGSPROGRAMVARE

Brukerne kan når som helst utføre følgende trinn for å bekrefte den installerte tilpasningsprogramvarens integritet og autentisitet uten å måtte starte tilpasningsprogramvaren:

1. Åpne Filutforskeren og gå til den kjørbare mappen for tilpasningsprogramvaren, vanligvis plassert i:
C:\Program Filer (x86)\Advanced Bionics\Target CI\
2. Høyreklikk på SonovaVerify.exe, og velg Egenskaper fra hurtigmenyen.
3. Velg fanen Digitale signaturer.
4. Dobbeltklikk på SHA256 «Sonova AG»-signaturen.
5. Bekreft at elementene i signaturen er gyldige, spesielt at meldingen «The digital signature is OK.» (Den digitale signaturen er OK) vises nær toppen, og at underskriverens navn og signeringstidspunkt samsvarer med følgende bilde:



1. Lukk popup-dialogboksene og dobbeltklikk på SonovaVerify.exe.
2. Bekreft at «NO ERRORS DETECTED.» (INGEN FEIL OPPDAGET) vises som vist på bildet nedenfor:



```
SonovaVerify 0.0.4.0 Copyright 2019-2023 Sonova

Verifying: C:\Program Files (x86)\Advanced Bionics\Target CI\SonovaVerify.DAT
Target: C:\Program Files (x86)\Advanced Bionics\Target CI
Product: Target CI 1.5.11.0

FILES PROCESSED: 779

IGNORED FILES: 3
.\config\App.xml
.\data\
.\sonovaverify.dat

NO ERRORS DETECTED.
Press any key to continue . . .
```

Bildet viser at SonovaVerify har autentisert og verifisert digitale signaturer for alle installerte programfiler. Dette bekrefter at tilpasningsprogramvaren ikke har blitt tuklet med, ødelagt eller på annen måte kompromittert. SonovaVerify vil vise advarsler eller feilmeldinger hvis filer eller mapper mangler, eller hvis uventede filer eller mapper er lagt til i programfilmappen.

9. PROGRAMVAREOPPDATERINGER OG PATCHER

Automatiske oppdateringer støttes ikke.

10. DATABASEHANDLING

10.1 DATABASES

Tilpasningsprogramvaren bruker en transaksjonsdatabase for lagring av pasientdata, samt et sett med informasjonsdatabaser som leverer metadata-konfigurasjoner som kreves av applikasjonen.

Se avsnitt 3. Nettverks- og kontekstdiagrammer – Utplasseringsartefakter for en detaljert liste over alle databaser som er utplassert av tilpasningsprogramvaren.

Når tilpasningsprogramvaren installeres som et frittstående program, er pasientdatabasen intern i tilpasningsprogramvaren. Pasientdatabasen, lagret i filen PatientDatabase.sqlite, ligger på samme maskin som tilpasningsprogramvaren og fungerer som lagringsplass for pasientdata. For å sikkerhetskopiere programdata når Target CI distribueres som et frittstående program må du opprette en sikkerhets kopi av hele mappen som ligger på %ProgramData%\Advanced Bionics\Target CI\Target CI\Data. Beskytt sikkerhetskopier av data ikke bare mot datatap, men også mot tyveri. Når tilpasningsprogramvaren installeres som en Noah-modul, lagres pasientdata i databasen som leveres av Noah-systemet. Noah-databasen kan være konfigurert for nettverkstilgang. Noah-databasen kan også konfigureres for ikke-nettverkstilgang og installeres på samme PC som tilpasningsprogramvaren. Konfigurer Noah-databasekryptering for å beskytte data (se HIMSA-dokumentasjonen).

For Noahs distribuerte distribusjonsmodus, se følgende lenke for instruksjoner om sikkerhetskopiering og gjenoppretting av Noah-pasientdatabasen:

<https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/backing-up-and-restoring-the-data-in-your-noah-database/>

10.2 DATAMIGRASJON

Tilpasningsprogramvaren lar brukere migrere pasientjournaler fra ABs tidligere tilpasningsprogramvare, SoundWave 3.2. Pasientjournalene må være tilgjengelige fra en SoundWave 3.2-installasjon på samme datamaskin som Target CI for å kunne migreres.

10.3 KONFIGURASJONER AV HØREAPPARATER

Tilpasningsprogramvaren muliggjør eksport og import av enhetskonfigurasjon og -innstillinger.

10.4 DATADESTRUKSJON

Instruksjoner for datadestruksjon finnes i bruksanvisningen eller på følgende nettsted for Noah-implementeringer: <https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/deleting-patient-records/>

11. SIKKERHETSMILJØ – DELT ANSVAR

Tilpasningsprogramvaren er utviklet for en tiltenkt bruk der risikostyring for cybersikkerhet anses som et delt ansvar mellom interessenter i hele økosystemet for hørselspleie, som inkluderer, men ikke er begrenset til brukere av høreapparater, foreldre eller foresatte til barn som bruker høreapparater, audiografer, IT-administratorer, hørselsinstitusjoner og -leverandører, leverandører av høreapparater og programmeringsutstyr.

Her følger en liste over beste vanlige praksisanbefalinger og sikkerhetskontroller for tilpasningsmiljøet der tilpasningsprogramvaren skal brukes:

OS-nivå

- Bruk tilgangskontroller på OS-nivå, f.eks.:
 - Fjern gjestekontoer
 - Aktiver Windows-brukerpålogging
 - Før en liste over autoriserte operatører for å kontrollere tilgang til systemet
 - Angi tilpassede brukere og roller
 - Bruk krav til sterke passord, og hold påloggingsinformasjon hemmelig
- Bruk revisjonskontroller på OS-nivå
- Hold operativsystemet oppdatert.
- Hold den installerte versjonen av tilpasningsprogramvaren oppdatert.
- Aktiver oppdatert beskyttelse mot skadelig programvare og antivirus
- Aktiver hvitelisting av apper

Personvern

- Krypter pasientdata ved hjelp av tredjepartsverktøy eller -kontroller på OS-nivå, f.eks. ved å bruke diskkryptering (f.eks. gratisversjonen av Microsoft BitLocker) for å beskytte alle data. For Noah-utplasseringer, bør du vurdere å bruke Noah databasekryptering.
- Eksterne medier som inneholder data eksportert fra tilpasningsprogramvare, inkludert rapporter og logger, bør sikres. Når dataene ikke lenger brukes, bør de slettes på en sikker måte og/eller mediet bør slettes på en sikker måte.
- Bruk USB-lagringsmedier med innebygd sikkerhetsfunksjonalitet, som krypterte USB-stasjoner med integrert tastatur.
- Sørg for å alltid holde dataene trygge:
 - Når du overfører data gjennom usikre kanaler, bør du enten sende anonyme data eller kryptere dem.
 - Beskytt sikkerhetskopier av data ikke bare mot datatap, men også mot tyveri.
 - Fjern alle data fra datamediet som ikke lenger er i bruk eller som skal kastes.
- Godkjente prosedyrer og verktøy skal benyttes av brukere for sikker sletting av data lagret på flyttbart lagringsmedium i henhold til gjeldende regelverk og retningslinjer for håndtering av pasientinformasjon / personlig identifiserbar informasjon (PII) / beskyttet helseinformasjon (PHI)

IT-infrastruktur

Bruk tilpasningsprogramvaren i et sikkert nettverksmiljø beskyttet mot uautorisert inntrenging. Det finnes mange effektive teknikker for å isolere og beskytte medisinske informasjonssystemer, blant annet implementering av brannmur, demilitariserte soner (DMZ), virtuelle lokalnettverk (VLAN) og nettverksenklaver. Oppretthold en aktiv nettverkstilkobling for å motta oppdateringer til operativsystemet.

Fysisk nivå

- Arbeidsstasjonen der tilpasningsprogramvaren er installert, skal være fysisk sikret på en måte slik at den ikke er tilgjengelig for utilsiktede brukere.
- Sørg for at uautorisert personell ikke tukler med systemet.
- Tilgang til skrivere som er koblet til arbeidsstasjonen skal kontrolleres.
- Skjermen på arbeidsstasjonen der tilpasningsprogramvaren er installert, skal plasseres på en måte som begrenser synligheten av skjerminnholdet til kun brukeren.

Organisasjonsnivå

- Kun yrkesopplært, fullt kvalifisert personell har tillatelse til å bruke systemet. Før en person får tillatelse til å bruke systemet, må det bekreftes at personen har lest og fullt ut forstår bruksanvisningen som følger med tilpasningsprogramvaren.
- Hvis du oppdager mistenkelig aktivitet på kontoene dine for tilpasningsprogramvaren eller uventede operasjoner, kontakt Advanced Bionics. Se avsnitt 2.1 for mer informasjon.

For mer informasjon om delt ansvar og for en mer detaljert liste over anbefalinger for beste praksis og sikkerhetskontroller for tilpasningsmiljøet der tilpasningsprogramvaren skal brukes på ulike nivåer, se:

- EHIMA-hviteboken «Beste praksis for sikker tilpasning av høreapparater», [EHIMAWhitePaper](#)

12. PRODUKSJONS- OG PROGRAMVAREUTVIKLINGSPROSESS

Cybersikkerhet vurderes gjennom hele programvareutviklingsprosessen. Tilpasningsprogramvaren er utviklet i samsvar med standardene IEC 62304 og IEC 82304.

Tilpasningsprogramvaren skannes for virus og skadelig programvare som en del av produksjonsprosessen.

Sårbarheter i tredjepartskomponenter som er oppført i NISTs nasjonale sårbarhetsdatabase (NVD), vurderes og reduseres under utviklingsprosessen, og overvåkes når tilpasningsprogramvaren er lansert på markedet.

13. PROGRAMVAREKOMPONENTER OG STYKKLISTE

Tilpasningsprogramvaren inneholder visse kommersielle, standard programvarekomponenter.

Tabellen nedenfor viser all SOUP (programvare av ukjent opprinnelse) som distribueres med tilpasningsprogramvaren.

SOUP-ELEMENT	FUNKSJONALITETSBEKRIVELSE	PRODUSENT	VERSJON
ciAD hørselstapsimulator	Bibliotek for simulatorer for hørselstap for mediespiller	ciAD (Jurg Haubold)	1.0.0.1
CredentialManagement	Pakken for legitimasjonshåndtering er et omslag (wrapper) for Windows Credential Management API.	iLya Lozovyy	1.0.2
CSharpAnalytics	Brukes til Google Analytics.	Angrepsmønster	1.6.1
Dapper	ORM	Sam Saffron, Marc Gravell, Nick Craver	2.0.78
Deconstructurama.Attributed	Brukes av Nephele-biblioteker.	Serilog Contributors	3.0
DirectShow 2005	Gir tilgang til Microsofts DirectShow-funksjonalitet fra .NET-applikasjoner.	Microsoft	2.0
DSL4	DSL 4 Fitting formula library	National Centre for Audiology, Canada	4.2
DSL5	DSL 5 Fitting formula library	National Centre for Audiology, Canada	5.0.34
GNOtometrics.Aurical	GNOtometrics.Aurical ompakket for Sonova	GNOtometrics	2.0.1.9
IceLink	Brukes til WebRTC audio/video konferanseintegrasjon	FM (Frozen Mountain)	3.8.0.22151
IdentityModel	OpenID Connect & OAuth 2.0-klientbiblioteket som brukes av Kona.CommonServices.Authentication-komponenten for OAuth 2-autentisering.	Dominick Baier, Brock Allen	5.0.1
IMCInterfaces	Noah grensesnittbibliotek for kommunikasjon mellom moduler	HIMSA II K/S	4.4.0.2266
LibGit2Sharp	Brukes av biblioteker som kommer fra Sonova for å kommunisere med Git	LibGit2Sharp-bidragstere	0.26.1
Mapster	Brukes til kartlegging av objekter i kode	chaowlert,eric_swann	7.2.0.0
MathNet.Numerics	Brukes for tilpasning av algoritmer (signalbane, målmatching, osv.)	Christoph Ruegg, Marcus Cuda, Jürgen Van Gael og bidragstere	4.11.0
Microsoft.Bcl.AsyncInterfaces	Tilbyr IEnumerable<T>- og IDisposable-grensesnittene samt hjelpeklasser for .NET Standard 2.0.	Microsoft	5.0.0
Microsoft.CodeAnalysis.Common	Brukes av bibliotekene som kommer fra Sonova.HardwareAbstraction. Palio.Trafo	Microsoft	3.9
Microsoft.CodeAnalysis.CSharp	Brukes av bibliotekene som kommer fra Sonova.HardwareAbstraction. Palio.Trafo	Microsoft	3.9

SOUP-ELEMENT	FUNKSJONALITETSBESKRIVELSE	PRODUSENT	VERSJON
Microsoft.Identity.Client	MSAL-biblioteket for .NET er en del av Microsofts identitetsplattform for utviklere (tidligere kalt Azure AD) v2.0. Det gjør det mulig å skaffe sikkerhetstokener for å kalle beskyttede API-er. Biblioteket benytter industristandardene OAuth2 og OpenID Connect.	Microsoft	4.38.0.0
Microsoft.Identity.Client.Extensions.Msal	Sikker tverrplattform-tokenbuffer for MSAL offentlige klientapplikasjoner.	Microsoft	2.19.3.0
Microsoft.IdentityModel.JsonWebTokens	Inkluderer typer som gir støtte for oppretting, serialisering og validering JSON Web Tokens. Brukes av komponenter som kommuniserer med backend-tjenester som bruker JSON Web Tokens for autentisering.	Microsoft	6.8.0
Microsoft.IdentityModel.Logging	Avhengighet av Microsoft.IdentityModel.Tokens	Microsoft	6.8.0
Microsoft.IdentityModel.Tokens	Avhengighet av SOUP Microsoft.IdentityModel.JsonWebTokens	Microsoft	6.8.0
Microsoft.Win32.TaskScheduler.dll	Brukes for FSW-sikkerhetskopieringsverktøyet (automatiske sikkerhetskopier).	David Hall	2.5.11.0
Microsoft.Xaml.Behaviors.Wpf	XAML Behaviors er en enkel metode for å legge til vanlig og gjenbrukbar interaktivitet i WPF-applikasjonene dine med minimal kode.	xamlexperienceteam, Microsoft	1.0.1
MS VC++ 2008 Redistributable	Microsoft Visual C++ 2008 Redistributable	Microsoft	9.0.30729.6161
Microsoft Visual C++ 2010 x86 Redistributable	Microsoft Visual C++ 2010 Redistributable	Microsoft	10.0.40219.325
Microsoft Visual C++ 2012 Redistributable	Microsoft Visual C++ 2012 Redistributable	Microsoft	11.0.61030.0
Microsoft Visual C++ 2017 Redistributable (x86)	Microsoft Visual C++ 2017 Redistributable	Microsoft	14.16.27024.1
MS-VisualC++ 7.1 kjøretidsbiblioteker	Microsoft Visual C++ kjøretidsbiblioteker	Microsoft	7.10.6030.0
NAL-NL1	NAL-NL1 Fitting formula library	Australian Hearing	1.1.0.0
NAL-NL2	NAL-NL2 Fitting formula library	Australian Hearing	2.0.11
NAudio.dll	Brukes til å justere volum og spille av lydfiler.	Åpen kilde	1.9
.NET Framework	.NET runtime framework	Microsoft	4.8.3928.0
Newtonsoft.Json	Brukes til JSON-serialisering og deserialisering.	James Newton-King	12.0.3

SOUP-ELEMENT	FUNKSJONALITETSBESKRIVELSE	PRODUSENT	VERSJON
Nibelung	NoahLink Wireless tilpasningsbiblioteker	GN ReSound	1.3.16.1
Nlogg	Dette er en avhengighet av HIMSA Nibelung.CPD (Noahlink Wireless)	Kim Christensen	4.4.0
NoahLink	NoahLink-driver for tilpasningsenhet	HIMSA	1.55.6.166
NoahLink Wireless	Noahlink trådløs driver for tilpasningsenhet	HIMSA	2.0.0.68
Otometrics.HiPro2	HiPro-kommunikasjonsbiblioteker	GNOtometrics	2.0.0.4
Otometrics.REMaccess	Otometrics' abstraksjonslag over Noah Inter-Module Communication Interface Library	GN Otometrics	1.0.0.10
Pdfium.Net.SDK	PDF-biblioteket for C# for å opprette og redigere PDF-dokumenter i .NET-applikasjoner.	Patagames.com	4.54.2704.0
Polly	Bibliotek som lar utviklere uttrykke motstandskraft og håndtering av midlertidige feil med strategier som Retry, Circuit Breaker, Bulkhead Isolation og Fallback på en flytende og trådsikker måte.	App vNext	7.2.1
Polly.Extensions.Http	Et bibliotek som inneholder meningsfulle hjelpefunksjoner for å konfigurere Polly-strategier for håndtering av midlertidige feil typiske for anrop gjennom HttpClient.	App vNext	3.0
Polly.Contrib.WaitAndRetry	Et bibliotek for Polly som inneholder hjelpefunksjoner for ulike vent-og-prøv-på-nytt-strategier.	Grant Dickinson, App vNext	1.1.1
Portable.BouncyCastle	Dette er en avhengighet av HIMSA Nibelung.CPD (Noahlink Wireless)	BouncyCastle.Crypto	1.8.10.0
protobuf-net.dll	Serialiseringsrammeverk brukt for RC-blob.	Åpen kilde	2.0.0.668
Serilog	Loggkomponenten som brukes for hele Chinook-applikasjonen.	Serilog Contributors	2.10.0
Serilog.Enrichers.Thread	Berik Serilog-hendelser med egenskaper fra gjeldende tråd.	Serilog Contributors	3.1
Serilog.Expressions	Uttrykksbasert hendelsesfiltrering for Serilog.	Serilog Contributors	2.0
Serilog.Sinks.Console	En Serilog-sink som skriver logghendelser til konsollen/terminalen.	Serilog Contributors	4.0.0.0
Serilog.Sinks.Debug	En Serilog-sink som skriver logghendelser til debug-utdata-vinduet.	Serilog Contributors	2.0
Serilog.Sinks.File	Skriv Serilog-hendelser til tekstfiler i vanlig format eller JSON-format.	Serilog Contributors	4.1
Serilog.Sinks.Trace	Den diagnostiske trace-sink-en for Serilog.	Serilog Contributors	2.1

SOUP-ELEMENT	FUNKSJONALITETSBESKRIVELSE	PRODUSENT	VERSJON
Serilog.Settings.AppSettings	XML-konfigurasjon (System.Configuration < appSettings>) støtte for Serilog.	Serilog Contributors	2.2.2
Security.Cryptography	Utvidelser til sikkerhets-API-ene som følger med .NET-rammeverket	Microsoft	1.7.2
SharpBITS API	SharpBITS.NET er en .NET-innpakning for BITS-API-et og en liten Windows GUI-applikasjon for enklere tilgang til BITS-opplastinger og nedlastinger.	perpetualKid	2.1.0.0
SharpZipLib	#ziplib (SharpZipLib, tidligere NzipLib) er et Zip-, Gzip-, Tar- og Bzip2-bibliotek skrevet utelukkende i C# for .NET-plattformen. Dette biblioteket tilbyr komprimeringsfunksjonalitet (zip, unzip, stream-komprimering osv.). Vi bruker den i Firmware Update-appen.	Åpen kilde	1.1.0.145
Superpower	Et bibliotek for parser-kombinatorer for C#	Datalust, Superpower Contributors, Sprache Contributors	2.3
SQLite.Interop	SQLite er et programvarebibliotek som tilbyr et relasjonsdatabasesystem. «Lite» i SQLite betyr lettvektig når det gjelder oppsett, databaseadministrasjon og behovet for ressurser. SQLite har følgende merkbare egenskaper: selvstendig, serverløs, nullkonfigurasjon, transaksjonsbasert. Det er en database (SQLite 3.32.1) som lagrer informasjon om pasienter (i frittstående modus), våre produktkatalogressurser og metadata for tilpasning, tilbehør og HIs.	SQLite Development Team	1.0.113
System Buffers	Tilbyr ressurspooling av alle typer for ytelseskritiske applikasjoner som ofte allokterer og avallokerer objekter.	23rogramma, dotnetframework	4.5.1
System.Collections.Immutable	Brukes av bibliotekene som kommer fra Sonova.HardwareAbstraction. Palio.Trafo	Microsoft	5.0
System.ComponentModel.Annotations	Inneholder attributter som brukes til å definere metadata for objekter som brukes som datakilder.	23rogramma, dotnetframework	4.7
System.Configuration.Configuration Manager	Tilbyr typer som støtter bruk av konfigurasjonsfiler.	Microsoft	5.0
System.Data.SQLite.Core	Brukes av bibliotekene som kommer fra Sonova.HardwareAbstraction. Palio.Trafo	SQLite Development Team	1.0.113.7
System.Drawing.Common	Gir tilgang til GDI+-grafikkfunksjonalitet.	Microsoft	5.0.1

SOUP-ELEMENT	FUNKSJONALITETSBEKRIVELSE	PRODUSENT	VERSJON
System.IdentityModel.Tokens.Jwt	Inkluderer typer som gir støtte for å opprette, serialisere og validere JSON-webtokens. Brukes av komponenter som kommuniserer med backend-tjenester som bruker JSON Web Tokens for autentisering.	Microsoft	6.8.0
System.IO.Abstractions	Et sett med abstraksjoner som bidrar til å gjøre filsysteminteraksjoner testbare.	Tatham Oddie & friends	12.0.10
System.Numerics.Vectors	Tilbyr maskinvareakselererte numeriske typer, egnet for høytytelsesbehandling og grafikkapplikasjoner.	24rogramma, dotnet framework	4.5
System.Memory	Tilbyr typer for effektiv representasjon og pooling av administrerte, stakk- og native minnesegmenter og sekvenser av slike segmenter, sammen med primitive funksjoner for å analysere og formatere UTF-8-kodet tekst lagret i disse minnesegmentene.	24rogramma, dotnet framework	4.5.4
System.Reactive.Core	Reaktive utvidelser (Rx) for .NET	.NET Foundation	3.1.1
System.Reactive.Grensesnitt	Reaktive utvidelser (Rx) for .NET	.NET Foundation	3.1.1
System.Reactive.Linq	Reaktive utvidelser (Rx) for .NET	.NET Foundation	3.1.1
System.Reactive.PlatformServices	Reaktive utvidelser (Rx) for .NET	.NET Foundation	3.1.1
System.Reactive.Windows.Threading	Reaktive utvidelser (Rx) for .NET	.NET Foundation	3.1.1
System.Reflection.DispatchProxy	Tilbyr en klasse for dynamisk å opprette proxy-typer som implementerer et spesifisert grensesnitt og arver fra en spesifisert DispatchProxy-type. Metodekallinger på den genererte proxy-instansen sendes til den DispatchProxy-basistypen.	Microsoft	4.7.1
System.Reflection.Metadata	Denne pakken gir en lavnivå .NET (ECMA-335) metadata-leser og -skriver. Det er laget for ytelse og er det ideelle valget for å bygge høyere nivå-biblioteker som har til hensikt å tilby sin egen objektmodell, slik som kompilatorer.	Microsoft	5.0
System.Runtime.CompilerServices.Unsafe	Gir System.Runtime.CompilerServices.Unsafe-klassen, som gir generisk, lavnivå funksjonalitet for å manipulere pekere.	24rogramma, dotnetframework	5.0
System.Security.AccessControl	Tilbyr basisklasser som muliggjør administrasjon av tilgangs- og revisjonskontrollister på sikre objekter.	Microsoft	5.0

SOUP-ELEMENT	FUNKSJONALITETSBESKRIVELSE	PRODUSENT	VERSJON
System.Security.Permissions	Tilbyr typer som støtter Code Access Security (CAS).	Microsoft	5.0
System.Security.Principal.Windows	Tilbyr klasser for å hente den nåværende Windows-brukeren og for å samhandle med Windows-brukere og -grupper.	Microsoft	5.0
System.Text.Encoding.CodePages	Tilbyr støtte for kodesidebaserte kodinger, inkludert Windows-1252, Shift-JIS og GB2312.	Microsoft	5.0
System.Text.Encodings.Web	Tilbyr typer for koding og escaping av strenger til bruk i JavaScript, HyperText Markup Language (HTML) og uniform resource locators (URL). Er en avhengighet av SOUP IdentityModel	24rogramma, dotnet framework	5.0
System.Text.Json	Tilbyr høyytelses- og lavallokerings-typer som serialiserer objekter til JavaScript Object Notation (JSON) tekst og deserialiserer JSON-tekst til objekter, med innebygd støtte for UTF-8. Tilbyr også typer for å lese og skrive JSON-tekst kodet som UTF-8, og for å lage en minnebasert dokumentobjektmodell (DOM), som er skrivebeskyttet, for tilfeldig tilgang til JSON-elementene innenfor en strukturert visning av dataene.	Microsoft	5.0.1
System.Threading.Tasks.Extensions	Tilbyr tilleggstyper som forenkler arbeidet med å skrive samtidig og asynkron kode.	25rogramma, dotnet framework	4.5.4
System.ValueTuple	Tilbyr System.ValueTuple-strukturene, som implementerer de underliggende typene for tupler i C# og Visual Basic. Legger til støtte for value tuples siden de kun er inkludert i nyere versjoner av .NET Framework.	25rogramma, dotnet framework	4.5.0
Thrift	Brukt for definisjon av remotelink-protokollen	Apache	0.13.0.0
Unity	Unity Container (Unity) er en fullverdig, utvidbar avhengighetsinjeksjonsbeholder.	Unity Container Project	5.8.13
WAP BT Dongle-driver	WAP BT Dongle-driver (tilpassingsdongle)	iAnywhere Solutions	3.0.0.6095
WebSync	Brukes for integrering av tilpasningsdatakanal	FM (Frozen Mountain)	4.9.32.0
Xps til PDF-gjengivelse (NiXPS)	Konverter 25rogrammatcally XPS-filer til PDF; brukes i tilpasning av app-rapporter.	NiXPS	2.6.7.0

14. REFERANSER

Tittel	Nettsted
Bruksanvisning (elektronisk)	https://ifu.advancedbionics.com/
Advanced Bionics global personvernerklæring	https://advancedbionics.com/privacy
HIMSA	https://www.himsa.com/
Noah System 4	https://www.himsa.com/products/all-about-noah-system-4/
Sikkerhetskopiering og gjenoppretting av data i Noah-databasen din	https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/backing-up-and-restoring-the-data-in-your-noah-database/
Noah-systemets databasekapasitet er nådd.	https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/noah-system-database-capacity-has-been-reached/
TeamViewer – Liste over brukte porter	https://community.teamviewer.com/English/kb/articles/4139-ports-used-by-teamviewer
BCP 195	https://www.rfc-editor.org/info/bcp195
Sikkerhetsdokumentasjon for LiveSwitch-server	https://developer.liveswitch.io/liveswitch-server/server/security.html
Beste praksis for sikker tilpasning av høreapparater EHIMA-hvitbok	https://www.ehima.com/wp-content/uploads/2021/09/EHIMA_Hvitbok_om_nettsikkerhet-FSW-sikkerhet_v1-sep.2021_.pdf

 Advanced Bionics LLC
28515 Westinghouse Place
Valencia, CA 91355, United States
T: +1.661.362.1400

info.us@advancedbionics.com

 Advanced Bionics GmbH
Feodor-Lynen-Strasse 35
D-30625 Hannover

info.switzerland@advancedbionics.com

Hvis du ønsker informasjon om flere AB-kontorer, kan du
gå til *AdvancedBionics.com/contact*

AB – A Sonova brand

Kontakt den lokale AB-representanten vedrørende
offentlig godkjenning og tilgjengelighet i ditt land.

Bluetooth®-ordmerket og -logoene er registrerte
varemerker som eies av Bluetooth SIG, Inc., og all bruk
av disse varemerkene av Sonova AG er lisensiert.