Target CI v1.5

VEJLEDNING I CYBERSIKKERHED

Dansk

Opdateret: september 2025

A Sonova Brand

Indhold

1. INTRODUKTION

Dette dokument indeholder tekniske sikkerhedsoplysninger og oplysninger vedrørende fortrolighed om Target CI v1.5-softwaresystemet fra Advanced Bionics, herefter kaldet "tilpasningssoftware". Tilpasningssoftwaren er udviklet med henblik på at blive brugt af kvalificerede høreapparatspecialister med henblik på at konfigurere (dvs. tilpasse) høreapparater til patienter, der har fået cochlear implantater fra Advanced Bionics.

Dette dokument fokuserer specifikt på de cybersikkerhedsrelaterede overvejelser og overvejelser vedrørende fortrolighed, der er relevante for brugen af tilpasningssoftwaren. Det omfatter en evaluering af de sikkerhedskontroller og kontroller vedrørende fortrolighed, der i øjeblikket er integreret i softwaren, samt dem, der forventes anvendt og konfigureret i det IT-miljø, hvor produktet vil blive brugt i henhold til det tilsigtede formål.

Dette dokument indeholder ikke tekniske sikkerhedsoplysninger og fortrolige oplysninger om:

- Tidligere versioner af AB-tilpasningssoftware
- Anden AB-software end Target CI v1.5
- AB-websites
- AB-mobilapps
- Høreapparater fra AB

1.1 FORKORTELSER OG DEFINITIONER:

Akronym	Begreb
FSW	Tilpasningssoftware
HCP	Tekniker
SaMD	Software som medicinsk udstyr
AB	Advanced Bionics
IFU	Brugsanvisning

2. ANDRE RESSOURCER

2.1 KUNDESERVICE

Personer i USA og Canada kan ringe til Advanced Bionics på et gratis telefonnummer (877-271-6727), hvor et professionelt supportteam sidder klar ved telefonerne mandag-fredag fra kl. 05.00-17.00 (Pacific Time).

Personer, som ikke befinder sig i USA eller Canada, har adgang til lokal support. Hvis du har spørgsmål vedrørende Target CI, relateret hardware eller andre programmeringsspørgsmål, er du meget velkommen til at kontakte din lokale Advanced Bionics-repræsentant.

2.2 AB-PORTALEN FOR SPECIALISTER

Tilpasningssoftwaren og tilhørende dokumentation kan downloades fra https://www.abproportal.com eller Sonova Web Client. En konto er påkrævet for at logge på. Denne ressource er muligvis ikke tilgængelig i alle lande. Kontakt din AB-repræsentant for yderligere oplysninger.

2.3 AVANCERET INSTALLATIONSVEJLEDNING

Den avancerede installationsvejledning til Target CI v1.5 er tilgængelig på anmodning. Vejledningen indeholder tekniske oplysninger om installationsprogrammet til tilpasningssoftwaren, herunder kommandolinjeindstillinger til lydløse og automatiske installationer.

2.4 MDS2

Producentens erklæring vedrørende sikkerhed af medicinsk udstyr (MDS2) er en branchestandardformular, der indeholder sikkerhedsrelaterede og privatlivsmæssige svar med hensyn til tilpasningssoftwaren fra AB. Formularen kan fås på anmodning.

2.5 BRUGSANVISNING

Brugsanvisningen leveres sammen med softwareinstallationsmediet. I nogle lande kan den elektroniske brugsanvisning downloades på www.advancedbionics.com/ifu

Følgende afsnit i brugsanvisningen kan være relevante for IT-specialister:

- Produktbeskrivelse
- Systemminimumkrav og ydelseskarakteristik
- Vejledning vedr. IT-sikkerhed
- Installationsvejledning
- Teknisk support

2.6 HIMSA

HIMSA er en tredjeparts softwareleverandør, der producerer Noah System 4, et softwaresystem udviklet til hørespecialister med det formål at give dem et leverandøruafhængigt system, så de kan udføre klientrelaterede opgaver.

Tilpasningssoftwaren kan eventuelt konfigureres til at bruge Noah System 4 til datalagring i stedet for en lokal database.

HIMSAs webside om sikkerhed giver svar på almindelige spørgsmål vedrørende IT-sikkerhed ved Noah System 4.

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

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

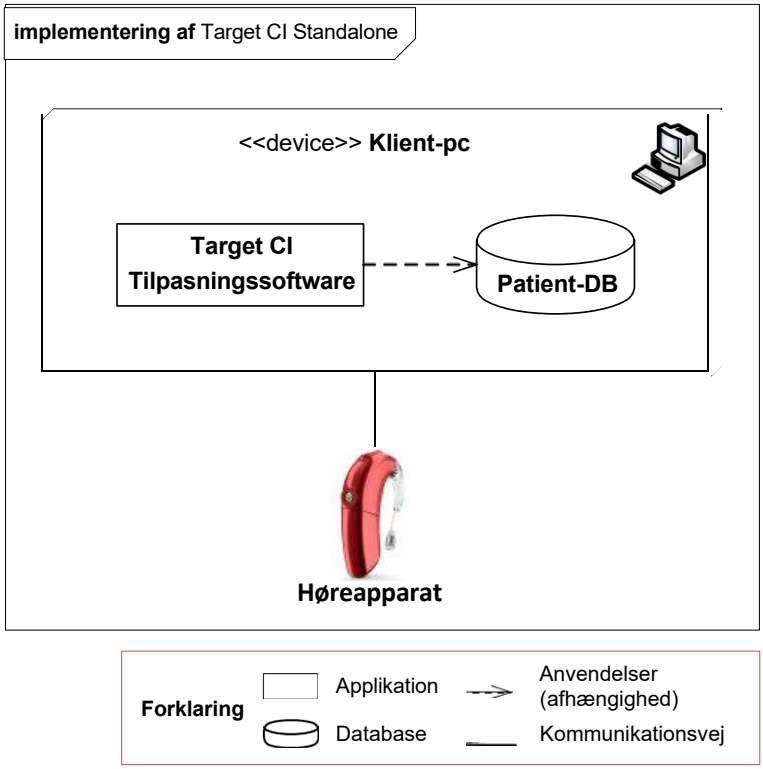
Se afsnittet om sikkerhed i HIMSA Learning Center for yderligere sikkerhedsoplysninger:
https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/

3. NETVÆRKS- OG KONTEKSTDIAGRAMMER

Der understøttes to implementeringsmodeller til tilpasningssoftwaren, som er en klientapplikation (SaMD), der er installeret på en kommercielt tilgængelig standard Microsoft Windows-pc. Softwaren inkluderer ikke nogen form for hardware eller et operativsystem.

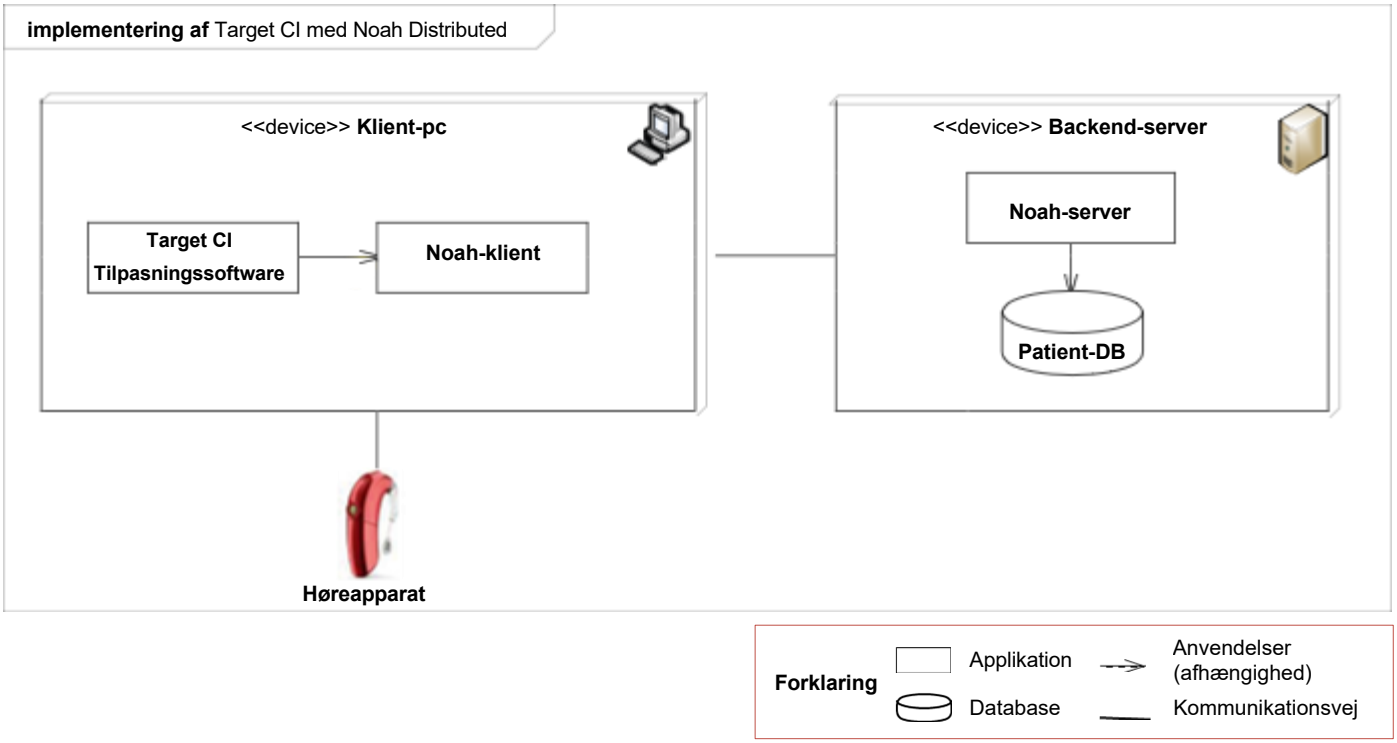
3.1 IMPLEMENTERINGSMODEL 1: SELVSTÆNDIG VERSION

I den selvstændige implementeringsmodel implementeres tilpasningssoftwaren på en klient-pc. Patientdatabasen lagres på den samme pc og installeres sammen med tilpasningssoftwaren.



3.2 IMPLICERINGSMODEL 2: NOAH DISTRIBUTED

I implementeringsmodellen Noah Distributed implementeres tilpasningssoftwaren på en eller flere klient-pc'er. Noah, et tredjeparts patientstyringssystem, implementeres på en intern server, der er tilgængelig for klient-pc'erne. Patientdatabasen lagres på Noah-serveren og tilgås via netværket fra en eller flere klient-pc'er.

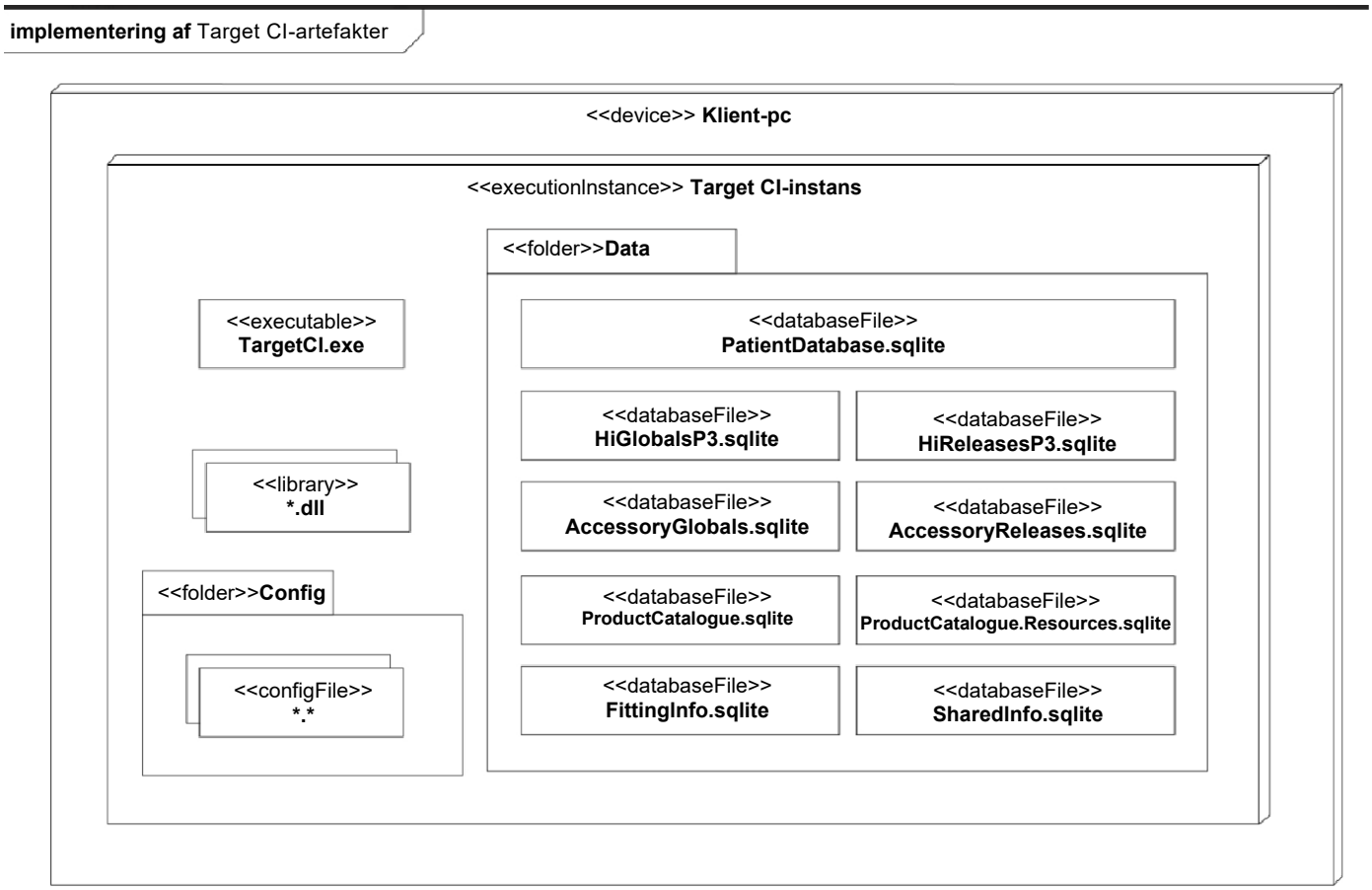


3.3 IMPLEMENTERINGSARTEFAKTER

Tilpasningssoftwaren installeres med en EXE-fil og et sæt tilhørende filer, herunder komponent-DLL'er, konfigurationsfiler og SQLite-databasefiler. Konfigurationsfilerne er installeret i mappen "%ProgramData%\ Advanced Bionics\Target CI\Target CI\Config" og databasefilerne er installeret i mappen "%ProgramData%\Advanced Bionics\Target CI\Target CI\Data". Datamappen indeholder en enkelt transaktionsdatabasefil og flere infodatabasefiler.

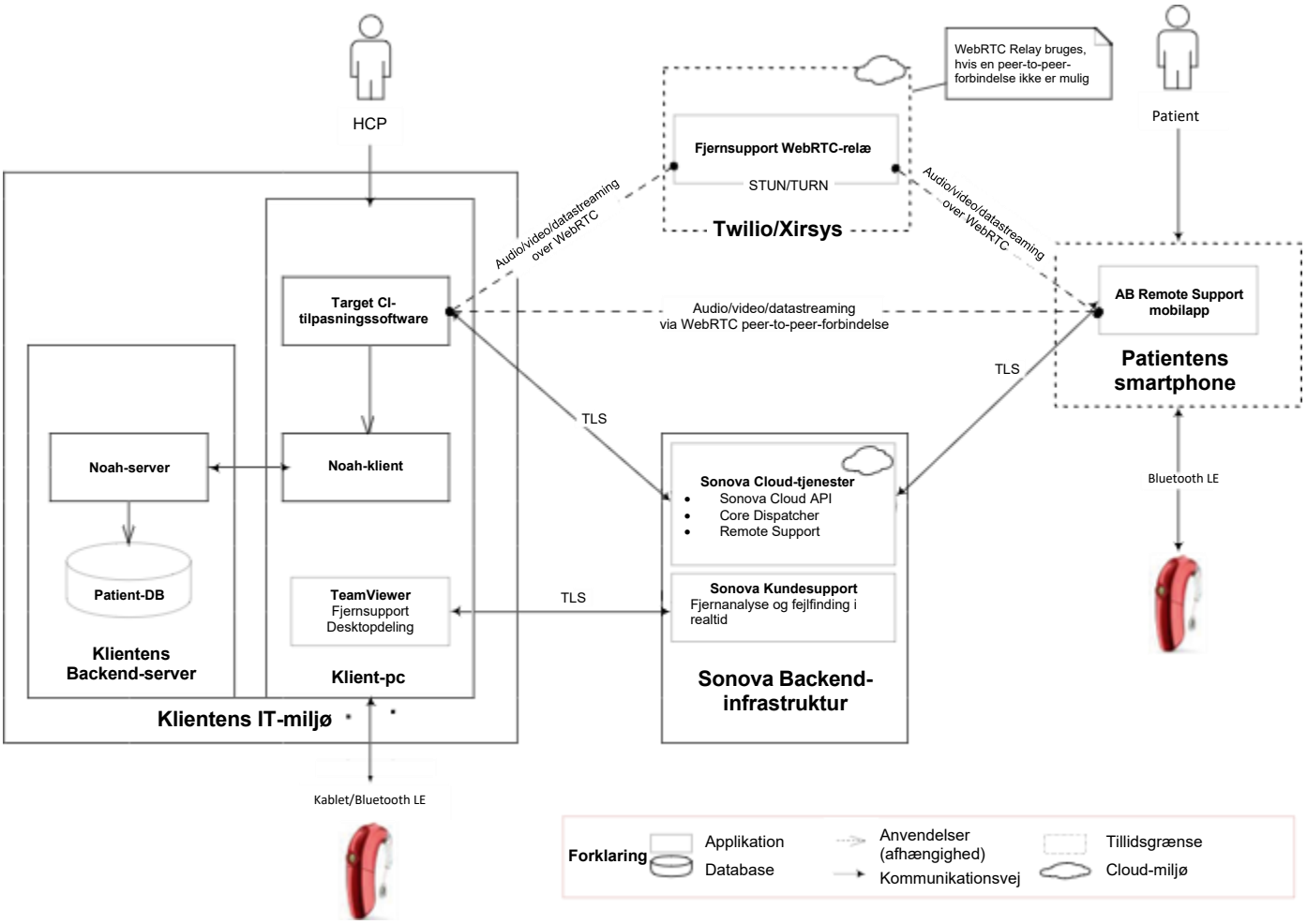
Transaktionsdatabasen, PatientDatabase.sqlite, gemmer patientens demografiske oplysninger og tilpasningsdata og installeres kun, når tilpasningssoftwaren implementeres i en selvstændig version.

Når tilpasningssoftwaren implementeres som et Noah-modul, leverer Noah-systemet de nødvendige patientdatapersistenstjenester til tilpasningssoftwaren. De resterende sqlite-filer er en integreret del af tilpasningssoftwaren og er påkrævet til alle implementeringsmodeller.



3.4 SYSTEMSAMMENKOBLINGER

Diagrammet og tabellen nedenfor illustrerer de primære systemsammenkoblinger. Typisk udnyttes kun en del af de tilgængelige sammenkoblinger.



Kilde/ destination	Service	Protokol	Port	Beskrivelse
Høreapparater	Kommunikation med høreapparat	Kablet forbindelse/ Bluetooth® Low Energy	N/A	Bruges til at kommunikere med høreapparater med henblik på betjening, konfiguration og udlæsning af status og data
Noah	Noah 4 Module API	.NET Remoting	N/A	Primær grænseflade for det modul, der bruges til at få adgang til Noah-softwaren (kun i implementeringsmodellen Noah Distributed)
Sonova Cloud-tjenester	Sonova Cloud API, Core Dispatcher, Remote Support	SOAP, REST	443	Sonova-tjenester, der hostes på et Microsoft Azure-datacenter, bruges til at:

Kilde/ destination	Service	Protokol	Port	Beskrivelse
				• hente klientens konfigurationsdata i tilpasningssoftwaren fra Sonovas backend-lager • overføre logging- og analysedata • etablere fjerntilpasningssessioner i realtid
Twilio/Xirsys, AB Remote Support-mobilapp	Remote Support	WebRTC	Liste over tilgængelige porte ved anmodning	Twilios cloudkommunikationstjenester hostes på tredjeparts cloudplatforme, nærmere bestemt Amazon Web Services (AWS) og Google Cloud Platform (GCP). Disse tjenester bruges udelukkende af fjernsupportfunktionen i tilpasningssoftwaren, som muliggør WebRTC-signaltjeneste og fjerntilpasningssessioner i realtid.
AB Kundeservice	Deling af skrivebord	TeamViewer, patenteret protokol	5938, 443, 80 Se TeamViewerPorts	Bruges til at udføre fjernanalyse i realtid og fejlfinding af problemer, der påvirker installationer af tilpasningssoftware. Se afsnit 6.6 FJERNSERVICE for yderligereinformation.

4. SYSTEMKRAV

Operativsystem	64-bit Windows 10 Pro/Enterprise
.NET Framework	Version 4.8
CPU	Intel® Core™ i5 eller lignende med samme eller bedre ydeevne
RAM	4 GB eller mere
Ledig plads på harddisk	3 GB eller mere
Minimumskrav til skærmopløsning	• 1280 x 1024 opløsning (maksimal skalering på 125 %) • 24-bit farve
Enhedsdrivere	• Noahlink Wireless-driver (den seneste version, der er tilgængelig fra HIMSA, kræves, hvis du bruger en tredjeparts USB-tilsluttet Noahlink Wireless-programmeringsgrænseflade). • CPI-3-driver (påkrævet ved brug af en USB-tilsluttet CPI-3-programmeringsgrænseflade).
Database	SQLite eller Noah System 4 (version 4.14 eller nyere)
Internetforbindelse	Der kræves en internetforbindelse til fjernsupport og analyselogging, se afsnit 4.4 Systemsammenkoblinger; intranet påkrævet ved brug af netværksforbundet Noah System 4.
Netværksporte	Se afsnit 3.4 Systemsammenkoblinger; se afsnit 3. Andre ressourcer — HIMSA for porte anvendt af Noah System 4.

5. INSTALLATION

5.1 KRAV

Der kræves en administratorkonto for at installere tilpasningssoftwaren. Når softwaren er installeret, kan den køres uden administratorrettigheder eller udvidede tilladelser.

Se afsnit 8, Softwareintegritet, for oplysninger om validering af softwarens integritet før installation.

Før installation anbefales det, at systemadministratorer sikrer sig, at:

• Den version af tilpasningssoftwaren, der skal installeres, er den senest tilgængelige.

• Det underliggende operativsystem er opdateret.

5.2 TYPER AF INSTALLATIONSPROGRAMMER

Der findes to installationsprogrammer til installation af tilpasningssoftwaren:

• Standardinstallationsprogram

• Installationsprogram fra IT Professional

Installationsprogram fra IT Professional er en enkelt MSI-fil og ekskluderer nødvendige komponenter, men svarer ellers til standardinstallationsprogrammet.

Nødvendige komponenter inkluderer Microsoft .NET Framework v4.8 og Microsoft Visual C++ Redistributable-pakker.

Begge installationsprogrammer understøtter avancerede installationsscenarier, herunder lydløs installation.

Installationsprogrammet IT Professional bør kun bruges, hvis din organisation kræver, at nødvendige komponenter installeres og administreres af din organisation og ikke af installationsprogrammet til tilpasningssoftware. Standardinstallationsprogrammet bør anvendes i alle andre tilfælde.

Installationsprogrammet IT Professional kan fås gennem den kliniske repræsentant fra AB. Installationsprogrammet IT Professional kan ikke bruges til at reparere, geninstallere eller afinstallere installationer fra standardinstallationsprogrammet. Standardinstallationsprogrammet kan ikke bruges til at reparere, geninstallere eller afinstallere installationer foretaget af installationsprogrammet IT Professional.

6. SIKKERHEDSKONTROLLER

Tilpasningssoftwaren er et klientprogram, der er installeret på en kommerciel standard Microsoft Windows-pc. Tilpasningssoftwaren kan installeres som et selvstændigt program eller som et Noah-modul.

6.1 GODKENDELSE – SELVSTÆNDIG IMPLEMENTERING

Når tilpasningssoftwaren installeres som et selvstændigt program, er den afhængig af adgangskontrolmekanismerne fra hostoperativsystemet. Hostoperativsystemet kan konfigureres af kundens IT-personale til at administrere godkendelser. Der er ikke integreret en sådan funktion i tilpasningssoftwaren. Advanced Bionics anbefaler, at hver bruger logger på hostoperativsystemet med en unik konto for hver enkelt bruger.

6.2 GODKENDELSE – NOAH-IMPLEMENTERING

Når tilpasningssoftwaren installeres som et Noah-modul, leveres adgangskontrollen af Noah System 4.
Se www.HIMSA.com for revisionskontroller, der anvendes af Noah System 4.

6.3 AUTORISATION

Tilpasningssoftwaren begrænser ikke adgangen til dens funktioner baseret på de enkelte brugeres roller. Softwaren understøtter én hovedfunktion med tilpasning af patientens høreapparater og én rolle som tilpasningsspecialist. Rollebaserede adgangskontroller er ikke relevante.

6.4 REVISION – SELVSTÆNDIG IMPLEMENTERING

Når tilpasningssoftwaren installeres som et selvstændigt program, er den afhængig af de revisionsmekanismer, der stilles til rådighed af hostoperativsystemet. Der er ikke integreret en sådan funktion i tilpasningssoftwaren. Hostoperativsystemet kan konfigureres af kundens IT-personale til at logge start/kørsler af tilpasningssoftwaren samt brugerlogon. Advanced Bionics anbefaler, at hver bruger logger på hostoperativsystemet med en unik konto for hver enkelt bruger for at udføre revision.

6.5 REVISION – NOAH-IMPLEMENTERING

Når tilpasningssoftwaren installeres som et Noah-modul, leveres revisionslogfiler af Noah-systemet. Se https://www.himsa.com/ for revisionskontroller anvendt af Noah System 4.

6.6 FJERNADGANG

Funktionen til skrivebordsdeling gør det muligt at udføre fjernanalyse i realtid og fejlfinding af problemer, der påvirker installationer af tilpasningssoftware. Denne funktion er baseret på tredjepartsværktøjet TeamViewer QuickSupport (installeret som standard sammen med tilpasningssoftware) og giver medarbejderne fra AB Kundeservice mulighed for at oprette fjernforbindelse til teknikerens computer og få fuld kontrol over dennes desktop, herunder adgang til det underliggende operativsystem og filsystem.

For at etablere en skrivebordsdelingssession kræves der interaktion med teknikeren. Teknikeren skal først køre TeamViewer QuickSupport-værktøjet (f.eks. via Target CI-tilpasningssoftwaren) og videregive TeamViewer ID-legitimationsoplysningerne til AB Support-teamet via en ekstern kommunikationskanal (f.eks. et telefonopkald).

Navnet og TeamViewer-ID'et på teammedlemmet fra AB Support vises som standard på teknikerens computerskærm under hver aktiv session med skrivebordsdeling.

Al netværkstrafik under skrivebordsdeling er sikret og opfylder eller overgår kryptografiske protokoller og algoritmer (RSA offentlig/privat nøgleudveksling og AES 256-bit sessionskryptering).

TeamViewer QuickSupport kan fjernes manuelt, uden at det påvirker andre Target FSW-funktioner. Target FSW-installationsprogrammet understøtter en kommandolinjeparameter til installation af Target FSW via kommandolinjen uden at inkludere TeamViewer QuickSupport-værktøjet.

7. INFORMATIONSBESKYTTELSE

7.1 ADVANCED BIONICS FORTROLIGHEDSPOLITIK

Fortrolighedspolitikken, der beskriver, hvordan Advanced Bionics indsamler, videresender, opbevarer og bruger personoplysninger, kan downloades fra: AdvancedBionics.com/privacy.

Advanced Bionics hverken hoster, opbevarer, sikkerhedskopierer eller har adgang til data, der er gemt i tilpasningssoftwaren eller Noah-databaserne, medmindre dataene udtrykkeligt sendes til Advanced Bionics.

7.2 FØDERALE STANDARDER FOR INFORMATIONSBEHANDLING (FIPS)

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

7.3 SIKKERHED VED OVERFØRSEL

Kommunikationen er sikret og aktiveret ved al indgående og udgående netværkskommunikation ved brug af tilpasningssoftwaren. Bortset fra funktionen Remote Support (som bruger WebRTC-protokollen) og Bluetooth-kommunikation med høreapparater & tilbehør, er alle andre forbindelser beskyttet af TLS-protokollen (Transport Layer Security), som sikrer fortrolighed, integritet og autenticitet.

TLS

TLS-konfigurationen er i overensstemmelse med gældende bedste praksis og sikkerhedsanbefalinger, der er dokumenteret i BCP 195 – Anbefalinger til sikker brug af TLS og DTLS, BCP195, herunder:

- Understøtter ikke SSL- og TLS-versioner før 1.2
- Understøtter ikke krypteringspakker, der bruger kryptografiske algoritmer, der tilbyder mindre end 128-bit-sikkerhed
- Understøtter anbefalede TLS-udvidelser af BCP 195
- Understøtter ikke usikre udvidelser af BCP 195

DTLS

Kryptering er en obligatorisk funktion i WebRTC og håndhæves under alle mediestreams, der sendes via WebRTC. Den anvendte krypteringsprotokol afhænger af kanaltypen; datastreaming krypteres ved hjælp af DTLS, og mediestreaming krypteres ved hjælp af Secure Real-time Transport Protocol (SRTP), fordi det er en mere enkel løsning end DTLS.

Se følgende link for mere detaljerede oplysninger om sikkerhedskonfiguration af Remote Support WebRTC:

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

BLE

Trådløs kommunikation via Bluetooth Low Energy med høreapparater og tilbehør er krypteret, og integriteten er som standard beskyttet (undtagen i tilfælde af identifikation og registrering). Derudover er varigheden af høreapparatets Bluetooth-parringstilstand tidsbegrænset. Se den tilgængelige dokumentation til høreapparatet for en mere detaljeret beskrivelse af sikkerheden ved Bluetooth-kommunikationskanalen.

7.4 SIKKERHED I HVILETILSTAND

Patientdatabase – Selvstændig implementeringsmodel

Hvis tilpasningssoftwaren installeres som et selvstændigt program, gemmes patientdatabasen lokalt på: C:\ProgramData\Advanced Bionics\Target CI\Target CI\Data

Disse poster er som standard ikke krypteret i hviletilstand. Beskyttede sundhedsoplysninger (PHI) og personligt identificerbare oplysninger (PII) gemmes i en database, der ligger i tilpasningssoftwaren og ikke videresendes over netværket.

Nogle lokale bestemmelser og love kan kræve kryptering af alle patientdata for at undgå et potentielt ansvar i tilfælde af datatab eller tyveri. Aktivér BitLocker eller tilsvarende komplet diskkryptering (på OS-niveau eller hardwarebaseret) for at beskytte dataene mod uautoriseret adgang eller kopiering, mens dataene er at rest.

BitLocker er en indbygget Windows-funktion, der krypterer hele drevet, og hvor der kræves godkendelse for at få adgang. Se altid Microsofts officielle vejledning og din organisations IT-sikkerhedspolitik, før du aktiverer BitLocker.

Sådan aktiveres BitLocker

Det er nødvendigt at have administratorrettigheder for at administrere BitLocker.

1. Søg efter "Manage BitLocker" (Administrer BitLocker)

   Åbn menuen Start, skriv "Manage BitLocker" (Administrer BitLocker), og vælg den fra søgeresultaterne.

2. Vælg System Drive (Systemdrev)

   Vælg det drev, hvor Windows er installeret, for at konfigurere krypteringsindstillinger.

3. Vælg en Unlock Method (Oplåsningsmetode)

   Vælg en af følgende valgmuligheder:

   - Kun TPM
   - TPM + PIN-kode
   - TPM + USB-nøgle

   Følg Microsofts vejledning om bedste praksis og din organisations IT-sikkerhedspolitik, når du vælger oplåsningsmetoden.

4. Sikkerhedskopiér gendannelsesnøglen

   Sikkerhedskopiér gendannelsesnøglen ved hjælp af sikre, virksomhedsgodkendte metoder. Anbefalede muligheder omfatter:

   - Lagring i Microsoft Entra ID (tidligere Azure AD) eller Active Directory for domænetilsluttede enheder
   - Lagring på en sikker, adgangskontrolleret netværksplacering med kryptering og revisionslogging

- Brug af en sikkerhedskonto til nøgler hos en tredjepart, der er godkendt af din organisation

Undgå at gemme nøglen på lokale drev, USB-nøgler eller udskrive den, medmindre det udtrykkeligt er tilladt i henhold til retningslinjerne. Gendannelsesnøgler skal beskyttes med samme strenghed som andre følsomme legitimationsoplysninger og roteres straks, hvis de eksponeres.

5. Start kryptering

Vælg:

- Hele drevet – anbefales til de fleste virksomhedsscenarier. Krypterer alle sektorer, herunder ubrugt plads, for at forhindre restdata.

Patientdatabase – Noah Distributed-implementeringsmodul

Når tilpasningssoftwaren installeres som et Noah-modul, gemmes PII i patientdatabasen, som Noah hoster. Patientdatabasen, som Noah hoster, kan muligvis være på en anden maskine. PII og andre patientdata vedligeholdes af Noah-software, og krypteringen af patientdata i hvilende tilstand sikres af Noah-systemet. Tilpasningssoftwaren kan evt. sende/modtage PII via en kablet eller trådløs netværksforbindelse, når en Noah-database konfigureres til netværksadgang.

PII gemt i den netværksforbundne Noah-database vil være synlige for andre enhedsbrugere på forskellige pc'er, der har tilladelser til den samme netværksforbundne database. Noah-databasen kan også blive konfigureret til ikke-netværksadgang og installeres på den samme pc som tilpasningssoftwaren.

Noah forhindrer tilpasningssoftwaren i at få adgang til patientjournaldatabasen. Når en bruger åbner en patient i tilpasningssoftwaren via Noah-klienten, kan tilpasningssoftwaren kun læse fra og skrive til den aktuelt åbne patientjournal og kan ikke få adgang til andre patientjournaler i Noah-databasen.

Se afsnittet www.HIMSA.com for krypteringsstandarder, der anvendes af Noah System 4.

RMA-eksportfiler

Tilpasningssoftwaren gør det muligt at eksportere klientoplysninger til en fil. RMA-filen kan sendes til Advanced Bionics for at løse RMA-problemer eller relaterede supportproblemer.

RMA-filen er asymmetrisk RSA-krypteret med en 512-bits nøglelængde. Tilpasningssoftwaren har ingen funktion til at dekryptere en RMA-fil.

Anonymiserede eksportfiler

Tilpasningssoftwaren gør det muligt at eksportere klientoplysninger til en klientanonymiseret fil. Klientens personligt identificerbare oplysninger, såsom fødselsdato og navn, erstattes med generiske værdier. Filen er ikke krypteret og kan importeres til den samme instans eller en anden version af tilpasningssoftwaren.

Standardeksportfiler

Tilpasningssoftwaren gør det muligt at eksportere klientoplysninger til en standardeksportfil. Filen bruger et patenteret binært format og er ikke krypteret. Filen kan importeres til den samme eller en anden version af tilpasningssoftwaren. Når brugere af tilpasningssoftwaren bruger denne funktion, skal de sikre, at standardeksportfiler håndteres i henhold til deres lokale IT-retningslinjer for håndtering af ukrypterede personoplysninger.

Høreapparat

Tilpasningssoftwaren gemmer klientoplysninger på klientens høreapparat. Personligt identificerbare oplysninger såsom klientens navn og fødselsdato gemmes ikke på høreapparatet. Andre ikke personligt identificerbare oplysninger gemmes ved hjælp af PBKDF2-kryptering med en 128-bit nøgle.

Tilpasningssoftwaren kan evt. sende/modtage ikke personligt identificerbare oplysninger til/fra et høreapparat via en patenteret kablet enhed (f.eks. CPI-3), AB Remote Support mobilapplikation eller Noahlink Wireless-enhed. Noahlink Wireless-enheden opretter forbindelse til høreapparatet ved hjælp af Bluetooth Low Energy (BLE) via en standard BLE 128-bit AES-krypteret kanal.

8. SOFTWAREINTEGRITET

8.1 BEKRÆFTELSE AF DOWNLOADEDE INSTALLATIONSMEDIER

Installationsmediet til Target CI-tilpasningssoftwaren kan i nogle regioner downloades fra Advanced Bionics' Pro Portal eller Sonova Web Client. Det downloadede installationsmedie kan godkendes ved hjælp af et hvilket som helst pålideligt SHA-256 hashing-værktøj.

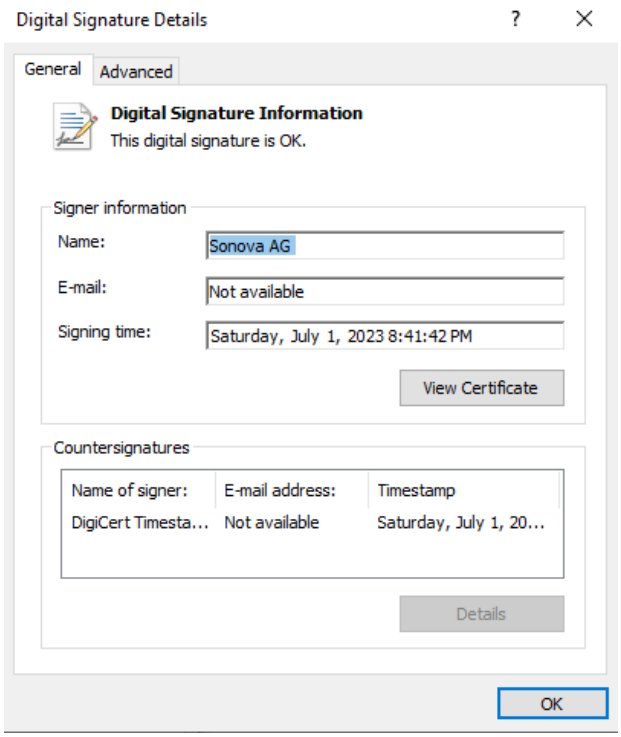
SHA256-hashen for standardinstallations-zip-filen er:
A42B8F41A5A4111D1CDF67394FFBBFBCDF2FB6215EC2696DB310B3AED6D4DD83

SHA256-hashen til IT Professional-installations-zip-filen er:
DDAD362CC3213EFEA702D9F4A61740B34EDF794FE997811B6B2C908CE754B25F

8.2 MANUEL BEKRÆFTELSE AF TILPASNINGSSOFTWARE FØR INSTALLATION

Brugere kan udføre følgende trin for at bekræfte tilpasningssoftwarens integritet og ægthed før installation:

1. Åbn Windows Stifinder, og naviger til rodmappen for installationssoftwarens installationsmedie. Hvis dit installationsmedie er et USB-drev, skal du sætte det i en USB-port og navigere til roden. Hvis dit installationsmedie er en zip-fil, skal du pakke den ud til en mappe og navigere til den pågældende mappe.
2. Højreklik på SonovaVerify.exe, og vælg Properties (Egenskaber) i genvejsmenuen.
3. Vælg fanen Digital Signatures (Digitale signaturer).
4. Dobbeltklik på SHA256 "Sonova AG"-signaturen.
5. Bekræft, at elementerne i signaturen er gyldige. Kontrollér især, at meddelelsen "The digital signature is OK." (Den digitale signatur er OK.) vises nær toppen, og at underskriverens navn og underskriftstidspunkt matcher følgende billede:



1. Luk dialogboksene, og dobbeltklik på SonovaVerify.exe.
2. Bekræft, at "NO ERRORS DETECTED" (INGEN FEJL FUNDET) vises som vist på følgende billede:

Billedet viser, at SonovaVerify har godkendt og bekræftet digitale signaturer af alle filer på installationsmediet, inklusive installationsprogrammet. Dette bekræfter, at installationsmediet ikke er blevet manipuleret med, beskadiget eller på anden måde kompromitteret. SonovaVerify viser advarsler eller fejlmeddelelser, hvis filer eller mapper mangler, eller hvis uventede filer eller mapper er blevet føjet til installationsmediet.

8.3 AUTOMATISK BEKRÆFTELSE AF INTEGRITET AF INSTALLERET TILPASNINGSSOFTWARE

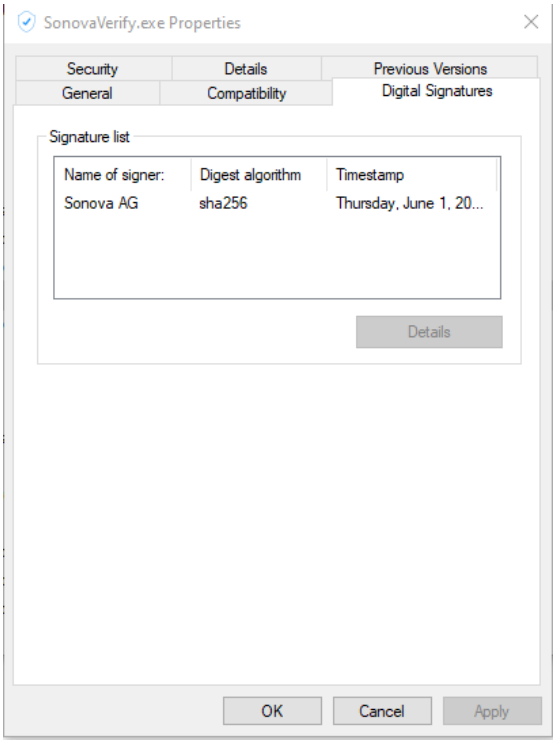
SonovaVerify er integreret med tilpasningssoftwaren og køres, hver gang programmet startes, for at bekræfte integriteten af tilpasningssoftwarens programfiler. Programfiler signeres digitalt ved hjælp af branchestandardpraksis og certifikater udstedt af en betroet certifikatmyndighed. Softwaren underretter brugeren via advarselsmeddelelser, hvis programfiler er kompromitteret.

8.4 MANUEL BEKRÆFTELSE AF INTEGRITET AF INSTALLERET TILPASNINGSSOFTWARE

Brugere kan udføre følgende trin for at bekræfte den installerede tilpasningssoftwares integritet og ægthed når som helst uden at skulle starte tilpasningssoftwaren:

1. Åbn Windows Stifinder, og naviger til tilpasningssoftwarens EXE-mappe, som normalt kan findes i: C:\Program Files (x86)\Advanced Bionics\Target CI\
2. Højreklik på SonovaVerify.exe, og vælg Properties (Egenskaber) i genvejsmenuen.
3. Vælg fanen Digital Signatures (Digitale signaturer).

4. Dobbeltklik på SHA256 "Sonova AG"-signaturen.
5. Bekræft, at elementerne i signaturen er gyldige, især at meddelelsen "The digital signature is OK." (Den digitale signatur er OK.) vises nær toppen, og at underskriverens navn og underskriftstidspunkt matcher følgende billede:



1. Luk dialogboksene, og dobbeltklik på SonovaVerify.exe.
2. Bekræft, at "NO ERRORS DETECTED" (INGEN FEJL FUNDET) vises som vist på følgende billede:

Billedet viser, at SonovaVerify har godkendt og bekræftet digitale signaturer på alle installerede programfiler. Dette bekræfter, at tilpasningssoftwaren ikke er blevet manipuleret med, beskadiget eller på anden måde er kompromitteret. SonovaVerify viser advarsler eller fejlmeddelelser, hvis filer eller mapper mangler, eller hvis uventede filer eller mapper er blevet føjet til programmappen.

9. SOFTWAREPATCHES OG -OPDATERINGER

Automatiske opdateringer understøttes ikke.

10. DATAADMINISTRATION

10.1 DATABASER

Tilpasningssoftwaren bruger en transaktionsdatabase til lagring af patientdata og et sæt informationsdatabaser, der leverer metadatakonfigurationer, som programmet kræver.

Se afsnit 3. Netværks- og kontekstdiagrammer – Implementeringsartefakter for en detaljeret liste over alle databaser, der er implementeret af tilpasningssoftwaren.

Når tilpasningssoftwaren installeres som et selvstændigt program, er patientdatabasen intern i tilpasningssoftwaren. Patientdatabasen, der er gemt i filen PatientDatabase.sqlite, findes på den samme maskine som tilpasningssoftwaren og fungerer som lagringsplads for patientdata. For at sikkerhedskopiere programdata, når Target CI implementeres som et separat program, skal du oprette en sikkerhedskopi af hele mappen, der findes på %ProgramData%\Advanced Bionics\Target CI\Target CI\Data. Sikkerhedskopier af data skal ikke kun beskyttes mod datatab, men også mod tyveri. Når tilpasningssoftwaren installeres som et Noah-modul, gemmes patientdata i den database, der leveres af Noah-systemet. Noah-databasen kan være konfigureret til netværksadgang. Noah-databasen kan også blive konfigureret til ikke-netværksadgang og installeres på den samme pc som tilpasningssoftwaren. Konfigurer Noah-databasekryptering for at beskytte data (se HIMSA-dokumentation).

For Noah Distributed-implementeringstilstand henvises til følgende link for anvisninger om sikkerhedskopiering og gendannelse af Noah-patientdatabasen:

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 DATAMIGRERING

Tilpasningssoftwaren giver brugerne mulighed for at migrere patientjournaler fra AB's tidligere tilpasningssoftware, SoundWave 3.2. Patientjournaler skal være tilgængelige fra en SoundWave 3.2-installation på den samme computer som Target CI for at kunne migreres.

10.3 HØREAPPARATKONFIGURATIONER

Tilpasningssoftwaren gør det muligt at eksportere og importere enhedens konfiguration og indstillinger.

10.4 BORTSKAFFELSE AF DATA

Anvisninger om bortskaffelse af data kan findes i brugsanvisningen eller på følgende website for Noah-implementeringer: https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/deleting-patient-records/

11. SIKKERHEDSMILJØ – DELT ANSVAR

Tilpasningssoftwaren er designet til en tilsigtet anvendelse, hvor håndtering af cybersikkerhedsrisici betragtes som et delt ansvar blandt interessenter på tværs af hele høreapparatøkosystemet, herunder, men ikke begrænset til, brugere af høreapparater, forældre eller værger til børn, der er høreapparatbrugere, sundhedspersonale, IT-administratorer, høreklinikker og hørespecialister, leverandører af høreapparater og programmeringsudstyr.

Her følger en liste over bedste anbefalinger for almindelig praksis og sikkerhedskontroller for det tilpasningsmiljø, hvor tilpasningssoftwaren skal bruges:

OS-niveau

- Anvend adgangskontroller på OS-niveau, f.eks.:
    - Fjern gæstekonti
    - Aktivér Windows-brugerlogon
    - Vedligehold en liste over autoriserede brugere til at kontrollere adgang til systemet
    - Angiv brugerdefinerede brugere og roller
    - Benyt krav til stærke adgangskoder, og sørg for, at logonoplysninger er hemmelige
- Anvend revisionskontroller på OS-niveau
- Sørg for, at operativsystemet er opdateret.
- Sørg for, at den installerede version af tilpasningssoftwaren er opdateret.
- Aktivér opdateret malware- og antivirusbeskyttelse
- Aktivér hvidlistning af apps

Databeskyttelse

- Krypter patientdata ved hjælp af tredjepartsværktøjer eller -kontroller på OS-niveau, f.eks. ved at bruge drevkryptering (f.eks. den gratis Microsoft BitLocker) med henblik på at beskytte alle data. Ved brug af Noah kan du overveje at bruge Noah-databasekryptering.
- Eksterne medier, der indeholder data eksporteret fra tilpasningssoftware, herunder rapporter og logfiler, bør sikres. Når dataene ikke længere bruges, skal de slettes sikkert, og/eller mediet skal slettes sikkert.
- Brug USB-lagringsmedier med indbygget sikkerhedsfunktionalitet, f.eks. krypterede USB-drev med integreret tastatur.
- Sørg for, at data altid holdes sikre:
    - Når du overfører data via usikre kanaler, skal du enten sende anonyme data eller kryptere dem.
    - Sikkerhedskopier af data skal ikke kun beskyttes mod datatab, men også mod tyveri.
    - Fjern alle data fra datamediet, som ikke længere bruges, eller som skal bortskaffes.
- Brugere bør anvende godkendte procedurer og værktøjer til sikker fjernelse af data, der er gemt på flytbare medier, i henhold til gældende regler og retningslinjer for håndtering af patientoplysninger/personligt identificerbare oplysninger (PII)/beskyttede sundhedsoplysninger (PHI)

IT-infrastruktur

Anvend tilpasningssoftwaren i et sikkert netværksmiljø beskyttet mod uautoriseret indtrængen. Der findes mange effektive teknikker til at isolere og beskytte medicinske informationssystemer, herunder implementering af firewallbeskyttelse, demilitariserede zoner (DMZ'er), virtuelle lokale netværk (VLAN'er) og netværksenklaver. Oprethold en aktiv netværksforbindelse for at modtage opdateringer til operativsystemet.

Fysisk niveau

- Arbejdspladsen, hvor tilpasningssoftwaren er installeret, skal være fysisk sikret på en måde, så den ikke er tilgængelig for utilsigtede brugere.
- Sørg for, at uautoriseret personale ikke manipulerer med systemet.
- Adgang til printere, der er tilsluttet arbejdsstationen, bør kontrolleres.
- Skærmen på den arbejdsstation, hvor tilpasningssoftwaren er installeret, bør placeres på en måde, der begrænser skærmens synlighed, så kun brugeren kan se indholdet.

Organisatorisk niveau

- Kun professionelt oplært, fuldt kvalificeret personale er autoriseret til at betjene systemet. Før nogen får tilladelse til at betjene systemet, skal det sikres, at personen har læst og fuldt ud forstået den betjeningsvejledning, der følger med tilpasningssoftwaren.
- Hvis du bemærker mistænkelig aktivitet på dine tilpasningssoftwarekonti eller uventede handlinger, skal du kontakte Advanced Bionics. Se afsnit 2.1 for yderligere oplysninger.

For yderligere oplysninger om delt ansvar og en mere detaljeret liste over anbefalinger til bedste praksis og sikkerhedskontroller i tilpasningsmiljøet, hvor tilpasningssoftwaren skal anvendes på forskellige niveauer, henvises til:

- EHIMA Whitepaper "Bedste praksis for sikker tilpasning af høreapparater", EHIMAWhitepaper

12. PROCES FOR FREMSTILLING OG SOFTWAREUDVIKLING

Cybersikkerhed inddrages under hele processen for softwareudvikling. Tilpasningssoftwaren er udviklet i overensstemmelse med standarderne IEC 62304 og IEC 82304.

Tilpasningssoftwaren scannes for virus og malware som en del af fremstillingsprocessen.

Sårbarheder i tredjepartskomponenter, der er anført i NISTs National Vulnerability Database (NVD), vurderes og afhjælpes under udviklingsprocessen og overvåges, når tilpasningssoftwaren er blevet frigivet på markedet.

13. SOFTWAREKOMPONENTER OG MATERIALELISTE

Tilpasningssoftwaren har visse kommercielle, standardsoftwarekomponenter integreret.

Følgende tabel angiver al SOUP (software af ukendt oprindelse), der distribueres sammen med tilpasningssoftwaren.

SOFTWAREELEMENT AF UKENDT OPRINDELSE	FUNKTIONSBESKRIVELSE	PRODUCENT	VERSION
ciAD Hearingloss Simulator	Hørenedsættelsessimulator – medieafspillerbibliotek	ciAD (Jurg Haubold)	1.0.0.1
CredentialManagement	Legitimationsstyringspakken er en del af Windows Credential Management API.	iLya Lozovyy	1.0.2
CSharpAnalytics	Bruges til Google Analytics.	Attack Pattern	1.6.1
Dapper	ORM	Sam Saffron, Marc Gravell, Nick Craver	2.0.78
Destructurama.Attributed	Bruges af Nephele-biblioteker.	Serilog Contributors	3.0
DirectShow 2005	Giver adgang til Microsofts DirectShow-funktionalitet fra .NET-applikationer.	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 nyudviklet til Sonova	GNOtometrics	2.0.1.9
IceLink	Bruges til integration af WebRTC audio/videokonference	FM (Frozen Mountain)	3.8.0.22151
IdentityModel	OpenID Connect & OAuth 2.0-klientbibliotek brugt af Kona.CommonServices.Authentication-komponent til OAuth 2-godkendelse.	Dominick Baier, Brock Allen	5.0.1
IMCInterfaces	Noah Inter-Module kommunikationsgrænsefladebibliotek	HIMSA II K/S	4.4.0.2266
LibGit2Sharp	Bruges af biblioteker fra Sonova til at kommunikere med Git	LibGit2Sharp-bidragsydere	0.26.1
Mapster	Bruges til at kortlægge objekter i kode	chaowlert,eric_swann	7.2.0.0
MathNet.Numerics	Bruges til tilpasningsalgoritmer (signalsti, målmatchning osv.)	Christoph Ruegg, Marcus Cuda, Jurgen Van Gael og bidragsydere	4.11.0
Microsoft.Bcl.AsyncInterfaces	Leverer IAsyncEnumerable<T> og IAsyncDisposable-grænseflader og hjælpemidler til .NET Standard 2.0.	Microsoft	5.0.0
Microsoft.CodeAnalysis.Common	Bruges af bibliotekerne fra Sonova.HardwareAbstraction. Palio.Trafo	Microsoft	3.9
Microsoft.CodeAnalysis.CSharp	Bruges af bibliotekerne fra Sonova.HardwareAbstraction. Palio.Trafo	Microsoft	3.9

SOFTWAREELEMENT AF UKENDT OPRINDELSE	FUNKTIONSBESKRIVELSE	PRODUCENT	VERSION
Microsoft.Identity.Client	MSAL-biblioteket til .NET er en del af Microsoft-identitetsplatform for udviklere (tidligere kaldet Azure AD) v2.0. Det giver dig mulighed for at erhverve sikkerhedstokens til at kalde beskyttede API'er. Den bruger branchestandarden OAuth2 og OpenID Connect.	Microsoft	4.38.0.0
Microsoft.Identity.Client.Extensions.Msal	Sikker token-cache på tværs af platforme til offentlige MSAL-klientapps.	Microsoft	2.19.3.0
Microsoft.IdentityModel.JsonWebTokens	Inkluderer typer, der understøtter oprettelse, serialisering og validering JSON Web Tokens. Bruges af komponenter, der kommunikerer med backend-tjenester, der bruger JSON Web Tokens til godkendelse.	Microsoft	6.8.0
Microsoft.IdentityModel.Logging	Afhængighed af Microsoft.IdentityModel.Tokens	Microsoft	6.8.0
Microsoft.IdentityModel.Tokens	Afhængighed af SOUP Microsoft.IdentityModel.JsonWebTokens	Microsoft	6.8.0
Microsoft.Win32.TaskScheduler.dll	Bruges til FSW-backupværktøj (automatiske backups).	David Hall	2.5.11.0
Microsoft.Xaml.Behaviors.Wpf	XAML Behaviors er en brugervenlig metode til at føje almindelig og genanvendelig interaktivitet til dine WPF-applikationer med minimal kode.	xamlexperiencesteam, 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 runtime-biblioteker	Microsoft Visual C++ runtime-biblioteker	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	Bruges til at justere lydstyrken og afspille lydfiler.	Open Source	1.9
.NET Framework	.NET runtime framework	Microsoft	4.8.3928.0
Newtonsoft.Json	Bruges til JSON-serialisering og deserialisering.	James Newton-King	12.0.3

SOFTWAREELEMENT AF UKENDT OPRINDELSE	FUNKTIONSBESKRIVELSE	PRODUCENT	VERSION
Nibelung	NoahLink Wireless-tilpasningsbiblioteker	GN ReSound	1.3.16.1
Nlog	Dette er en afhængighed af HIMSA Nibelung.CPD (Noahlink Wireless)	Kim Christensen	4.4.0
NoahLink	NoahLink-tilpasningsenhedsdriver	HIMSA	1.55.6.166
NoahLink Wireless	NoahLink Wireless-tilpasningsenhedsdriver	HIMSA	2.0.0.68
Otometrics.HiPro2	HiPro-kommunikationsbiblioteker	GNOtometrics	2.0.0.4
Otometrics.REMaccess	Otometrics' abstraktionslag over Noah Inter-Module-kommunikationsgrænsefladebibliotek	GN Otometrics	1.0.0.10
Pdfium.Net.SDK	C# PDF-bibliotek til at oprette og redigere PDF-dokumenter i .Net-applikationer.	Patagames.com	4.54.2704.0
Polly	Bibliotek, der giver udviklere mulighed for at definere politikker for robusthed og håndtering af forbigående fejl såsom Retry, Circuit Breaker, Bulkhead Isolation og Fallback på en flydende og trådsikker måde.	App vNext	7.2.1
Polly.Extensions.Http	EEt bibliotek med målrettede hjælpefunktioner til at konfigurere Polly-politikker til håndtering af forbigående fejl, som typisk opstår ved kald via HttpClient.	App vNext	3.0
Polly.Contrib.WaitAndRetry	Et bibliotek til Polly, der indeholder hjælpemetoder til en række forskellige vent-og-forsøg-igen-strategier.	Grant Dickinson, App vNext	1.1.1
Portable.BouncyCastle	Dette er en afhængighed af HIMSA Nibelung.CPD (Noahlink Wirelesss)	BouncyCastle.Crypto	1.8.10.0
protobuf-net.dll	Serialiseringsframework brugt til RC-blob.	Open Source	2.0.0.668
Serilog	Loggingkomponenten, der bruges til hele Chinook-applikationen.	Serilog Contributors	2.10.0
Serilog.Enrichers.Thread	Forbedring af Serilog-hændelser med egenskaber fra den aktuelle tråd	Serilog Contributors	3.1
Serilog.Expressions	Udtryksbaseret hændelsesfiltrering for Serilog.	Serilog Contributors	2.0
Serilog.Sinks.Console	Et Serilog-område, der skriver loghændelser til konsol/terminal.	Serilog Contributors	4.0.0.0
Serilog.Sinks.Debug	Et Serilog-område, der skriver loghændelser til fejlfindingsoutputvinduet.	Serilog Contributors	2.0
Serilog.Sinks.File	Skriv Serilog-hændelser til tekstfiler i almindeligt format eller JSON-format.	Serilog Contributors	4.1
Serilog.Sinks.Trace	Det diagnostiske sporingsområde for Serilog.	Serilog Contributors	2.1

SOFTWAREELEMENT AF UKENDT OPRINDELSE	FUNKTIONSBESKRIVELSE	PRODUCENT	VERSION
Serilog.Settings.AppSettings	XML-konfiguration (System.Configuration <appSettings>) support for Serilog.	Serilog Contributors	2.2.2
Security.Cryptography	Udvidelser til de sikkerheds-API'er, der følger med .NET framework	Microsoft	1.7.2
SharpBITS API	SharpBITS.NET er en .NET-wrapper af BITS API'en og en lille Windows UI-applikation til nemmere adgang til up- og downloads af BITS.	perpetualKid	2.1.0.0
SharpZipLib	#ziplib (SharpZipLib, tidligere NzipLib) er et Zip-, Gzip-, Tar- og Bzip2-bibliotek skrevet udelukkende i C# til .NET-platformen. Dette bibliotek tilbyder komprimeringsfunktioner (zip, unzip, stream-komprimering osv.). Vi bruger den i Firmware Update-appen.	Open Source	1.1.0.145
Superpower	Et parser-kombinatorbibliotek til C#	Datalust, Superpower Contributors, Sprache Contributors	2.3
SQLite.Interop	SQLite er et softwarebibliotek, der leverer et relationelt databasehåndteringssystem. Lite i SQLite betyder letvægt med hensyn til opsætning, databaseadministration og nødvendige ressourcer. SQLite har følgende bemærkelsesværdige funktioner: selvstændig, serverløs, nulkonfiguration, transaktionel. Det er en database (SQLite 3.32.1) til at gemme oplysninger om patienten (i selvstændigt program), vores produktkatalogressourcer og metadata for tilpasning, tilbehør og His.	SQLite Development Team	1.0.113
System.Buffers	Tilbyder samling af ressourser af enhver type til ydeevnekritiske applikationer, der ofte allokerer og deallokerer objekter.	23rogramma,dotnetframework	4.5.1
System.Collections.Immutable	Bruges af bibliotekerne fra Sonova.HardwareAbstraction. Palio.Trafo	Microsoft	5.0
System.ComponentModel.Annotations	Leverer attributter, der bruges til at definere metadata for objekter, der bruges som datakilder.	23rogramma,dotnetframework	4.7
System.Configuration.ConfigurationManager	Tilbyder typer, der understøtter brugen af konfigurationsfiler.	Microsoft	5.0
System.Data.SQLite.Core	Bruges af bibliotekerne fra Sonova.HardwareAbstraction. Palio.Trafo	SQLite Development Team	1.0.113.7
System.Drawing.Common	Giver adgang til GDI+ grafikfunktionalitet.	Microsoft	5.0.1

SOFTWAREELEMENT AF UKENDT OPRINDELSE	FUNKTIONSBESKRIVELSE	PRODUCENT	VERSION
System.IdentityModel.Tokens.Jwt	Inkluderer typer, der understøtter oprettelse, serialisering og validering af JSON-webtokens. Bruges af komponenter, der kommunikerer med backend-tjenester, der bruger JSON Web Tokens til godkendelse.	Microsoft	6.8.0
System.IO.Abstractions	Et sæt abstraktioner, der hjælper med at gøre filsysteminteraktioner testbare.	Tatham Oddie & friends	12.0.10
System.Numerics.Vectors	Leverer hardwareaccelererede numeriske typer, der er velegnede til højtydende behandling og grafikapplikationer.	24rogramma,dotn etfra me work	4.5
System.Memory	Tilbyder typer til effektiv repræsentation og samling af administrerede, stak- og native hukommelsessegmenter og sekvenser af sådanne segmenter, sammen med primitiver til parsing og formatering af UTF-8-kodet tekst gemt i disse hukommelsessegmenter.	24rogramma,dotn etfra me work	4.5.4
System.Reactive.Core	Reaktive udvidelser (Rx) til .NET	.NET Foundation	3.1.1
System.Reactive. Interfaces	Reaktive udvidelser (Rx) til .NET	.NET Foundation	3.1.1
System.Reactive.Linq	Reaktive udvidelser (Rx) til .NET	.NET Foundation	3.1.1
System.Reactive.PlatformServices	Reaktive udvidelser (Rx) til .NET	.NET Foundation	3.1.1
System.Reactive.Windows.Threading	Reaktive udvidelser (Rx) til .NET	.NET Foundation	3.1.1
System.Reflection.DispatchProxy	Leverer en klasse til dynamisk at oprette proxytyper, der implementerer en specificeret grænseflade, og som er afledt af en specificeret DispatchProxy-type. Metodekald på den genererede proxyinstans sendes til den pågældende DispatchProxy-basistype.	Microsoft	4.7.1
System.Reflection.Metadata	Denne pakke tilbyder en .NET (ECMA-335) metadatalæser og -skriver på lavt niveau. Den er optimeret til ydeevne og er det ideelle valg til at bygge biblioteker på et højere niveau, der har til hensigt at levere deres egen objektmodel, såsom kompilatorer.	Microsoft	5.0
System.Runtime.CompilerServices. Unsafe	Leverer System.Runtime. CompilerServices.Unsafe-klassen, som leverer generisk funktionalitet på lavt niveau til manipulation af pointere.	24rogramma, dotnetframework	5.0
System.Security.AccessControl	Indeholder basisklasser, der muliggør administration af adgangs- og revisionskontrollister på sikre objekter.	Microsoft	5.0

SOFTWAREELEMENT AF UKENDT OPRINDELSE	FUNKTIONSBESKRIVELSE	PRODUCENT	VERSION
System.Security.Permissions	Tilbyder typer, der understøtter Code Access Security (CAS).	Microsoft	5.0
System.Security.Principal.Windows	Tilbyder klasser til at hente den aktuelle Windows-bruger og til at interagere med Windows-brugere og -grupper.	Microsoft	5.0
System.Text.Encoding.CodePages	Understøtter tegntabelbaserede kodninger, herunder Windows-1252, Shift-JIS og GB2312.	Microsoft	5.0
System.Text.Encodings.Web	Tilbyder typer til kodning og escape-strenge til brug i JavaScript, HyperText Markup Language (HTML) og URL'er (uniform resource locators). Er en afhængighed af SOUP IdentityModel	24rogramma,dotn etfra me work	5.0
System.Text.Json	Leverer typer med høj ydeevne og reduceret tildeling, der serialiserer objekter til JavaScript Object Notation (JSON)-tekst og deserialiserer JSON-tekst til objekter, med indbygget UTF-8-understøttelse. Indeholder også typer til at læse og skrive JSON-tekst kodet som UTF-8, og til at oprette en dokumentobjektmodel (DOM) integreret i hukommelsen, som er skrivebeskyttet, til tilfældig adgang til JSON-elementerne i en struktureret visning af dataene.	Microsoft	5.0.1
System.Threading.Tasks.Extensions	Indeholder yderligere typer, der forenkler arbejdet med at skrive parallelog asynkron kode.	25rogramma,dotnetfra mework	4.5.4
System.ValueTuple	Leverer System.ValueTuple-strukturerne, som implementerer de underliggende typer for tupler i C# og Visual Basic. Tilføjer værdi til understøttelse af tupler, da de kun er inkluderet i senere .NET framework-versioner.	25rogramma,dotnetfra mework	4.5.0
Thrift	Bruges til definition af fjernlinkprotokol	Apache	0.13.0.0
Unity	Unity Container (Unity) er en fuldt udstyret, udvidelig afhængighedsinjektionscontainer.	Unity Container Project	5.8.13
WAP BT Dongle Driver	WAP BT Dongle Driver (tilpasningsdongle)	iAnywhere Solutions	3.0.0.6095
WebSync	Bruges til integrering af tilpasningsdatakanal	FM (Frozen Mountain)	4.9.32.0
Xps to Pdf render (NiXPS)	Konverterer 25rogrammatically xps-filer til pdf; anvendt ved tilpasning af applikationsrapporter.	NiXPS	2.6.7.0

14. REFERENCER

Titel	Website
Brugsanvisning (elektronisk)	https://ifu.advancedbionics.com/
Advanced Bionics – global fortrolighedspolitik	https://advancedbionics.com/privacy
HIMSA	https://www.himsa.com/
Noah System 4	https://www.himsa.com/products/all-about-noah-system-4/
Sikkerhedskopiering og gendannelse af dataene i din Noah-database	https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/backing-up-and-restoring-the-data-in-your-noah-database/
Kapacitet for Noah-systemdatabase er nået.	https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/noah-system-database-capacity-has-been-reached/
TeamViewer – liste over anvendte porte	https://community.teamviewer.com/English/kb/articles/4139-ports-used-by-teamviewer
BCP 195	https://www.rfc-editor.org/info/bcp195
Dokumentation for LiveSwitch-serversikkerhed	https://developer.liveswitch.io/liveswitch-server/server/security.html
Bedste praksis for sikker tilpasning af høreapparater EHIMA whitepaper	https://www.ehima.com/wp-content/uploads/2021/09/EHIMA Cybersecurity-FSW-Security-Whitepaper v1-Sep2021 .pdf

CE 0123

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

info.us@advancedbionics.com

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

info.switzerland@advancedbionics.com

Du kan finde oplysninger om AB-repræsentanter på
advancedbionics.com/contact

AB – A Sonova brand

Kontakt nærmeste AB-forhandler for at få oplysninger om godkendelse og lanceringsdato i Danmark.

ADVANCED BIONICS
POWERFUL CONNECTIONS

029-S396-08 Rev A 2025-09-15