Beveiliging Nedap Ons

Document

Last review date	17 Dec 2022
Classification	**PUBLIC**

Inleiding

Nedap Healthcare levert software-as-a-service (SaaS) oplossingen voor klanten in de Nederlandse zorgsector. De informatie (persoonlijke gezondheidsinformatie) die in Nedap Ons wordt verwerkt eist een goede vorm van beveiliging. In de SLA (Service Level Agreement) van de dienstverlening van Nedap Ons wordt verwezen naar dit document. Dit document is een samenvatting waarin de belangrijkste elementen van onze interne documentatie en processen op het gebied van informatiebeveiliging met betrekking tot Nedap Ons beschreven staan. Aanvullingen en wijzigingen aan dit document worden zoveel mogelijk doorgevoerd in relatie met de SLA: wijzigingen aan de beveiliging van Nedap Ons zullen zoveel mogelijk gericht zijn op het behouden en verbeteren van de dienstverlening.

Nedap Healthcare is ISO 27001 en NEN 7510 gecertificeerd. Dat betekent dat een externe auditor regelmatig toetst of Nedap Healthcare voldoet aan alle eisen rondom informatiebeveiliging. De ISO 27001 en NEN 7510 certificaten van Nedap Healthcare zijn te downloaden van het Supportportaal van Nedap Healthcare of op te vragen bij de accountmanager van Nedap Healthcare.

Fysieke toegang

Nedap Ons wordt gehost door Nedap Healthcare zelf. Voor de housing (koeling, redundante stroomvoorziening en ruimte) wordt gebruik gemaakt van 4 verschillende datacenters van twee juridisch volledig gescheiden organisaties in Nederland met een grote geografische spreiding:

- Amsterdam (datacenter van Equinix Netherlands B.V.)
- Enschede (datacenter van Equinix Netherlands B.V.)
- Hengelo, Overijssel (datacenter van Previder B.V.)
- Zwolle (datacenter van Equinix Netherlands B.V.)

Alle servers en netwerkapparatuur die gebruikt wordt voor de dienstverlening van Nedap Ons zijn eigendom van Nedap Healthcare. Voor selecte, specifieke functionaliteiten binnen Nedap Ons kan in sommige gevallen gebruik gemaakt worden van uitbesteding van dienstverlening; deze gevallen zijn specifiek benoemd in een document "Leveranciers en subverwerkers" dat op te vragen is bij Nedap Healthcare.

Voor alle datacenters geldt dat er strikte eisen zijn gesteld aan de (fysieke) toegang tot de datacenters en dat alleen personeel van Nedap Healthcare bepaalt wie er toegang heeft tot de servers. Ook voldoen alle datacenters aan de strengste eisen op het gebied van toegangsbeveiliging, klimaatbeheersing, brandpreventie en stroom-redundantie (UPS, generatoren). De datacenters waar Nedap Healthcare gebruik van maakt zijn in ieder geval ISO 27001 gecertificeerd. Daarnaast bezitten de datacenters over een SOC en/ of ISAE verklaring voor Data Center Hosting Services (of vergelijkbaar).

Logische toegang (authenticatie en autorisatie)

De klantorganisatie is verantwoordelijk voor passende technische en organisatorische maatregelen voor de beveiliging van de klantinfrastructuur (netwerk, werkplekken, etc.). Ook is de klantorganisatie verantwoordelijk voor een passende inrichting van de authenticatie tot Ons. Dit geldt zowel voor productie- als voor (geanonimiseerde) testomgevingen. Nedap Ons biedt verschillende en uitgebreide mogelijkheden om - met in achtneming van wet- en regelgeving - authenticatie van gebruikers in te richten.

De informatie die wordt verwerkt in Nedap Ons is (persoonlijke) gezondheidsinformatie en valt daarmee in de categorie van informatie waarvoor de Autoriteit Persoonsgegevens en het NCSC hebben vastgesteld dat Multi-Factor authenticatie (MFA) of Twee-Factor authenticatie (2FA) altijd verplicht moet zijn. Voor toegang tot Nedap Ons geldt dat ook: gebruikers moeten een persoonlijk account gebruiken en 2FA is verplicht. Er mag geen twijfel bestaan over wie (natuurlijk persoon) is ingelogd in Nedap Ons en daarmee wie (bepaalde) acties heeft gedaan op een cliënt-dossier (zie ook NEN7510, paragraaf 9.4).

Nedap Ons biedt zelf 3 mogelijkheden van 2FA voor gebruikers:

- SMS verificatie
- Verificatie via een vast telefoonnummer
- Een toegangscode app op een mobiele telefoon

Daarnaast is het ook mogelijk om 2FA in te richten met een Single-Sign-On (SSO) provider. In dat geval wordt de authenticatie bij Nedap Ons niet langer uitgevoerd door Nedap Ons maar door de SSO provider. Dit biedt voor een zorgaanbieder de mogelijkheid om authenticatie en gebruikersbeheer te centraliseren. Ook in het geval van het gebruik van een SSO-provider blijft de verplichting voor 2FA van kracht. Om te voorkomen dat gebruikers na het inloggen met een SSO nogmaals een tweede factor in moeten voeren, ondersteunt Nedap Ons de OpenID Connect standaard met AMR (Authentication Method Reference). Door goedkeurde SSO-provider uitgevoerde twee-factor authentications worden dan vertrouwd door Nedap Ons.

Vrijwel alle moderne SSO providers ondersteunen OpenID Connect en AMR. Denk daarbij aan Azure AD van Microsoft, HelloID van Tools4Ever, Okta en vele anderen. Kijk op het Nedap Ons Supportportaal voor de actuele lijst.

De klantorganisatie is verantwoordelijk voor het toekennen en beheren van autorisaties in Ons aan gebruikers. Ons Autorisatie is de aparte applicatie van Ons - bedoeld voor applicatiebeheerders - waarin organisaties autorisaties van gebruikers voor alle Ons applicaties kunnen beheren vanaf één centrale plek. Op het Supportportaal kan de klant terecht voor meer informatie over de opzet van Ons Autorisatie, voor uitleg over de verschillende autorisatiemechanismes, het werken met rollen en bereik en veelvoorkomende begrippen.

Beveiliging van gegevens tijdens transport

Toegang tot webapplicaties van Nedap Ons is enkel mogelijk via een beveiligde (https) verbinding. Voor de configuratie van deze beveiligde verbinding hanteren we nationale en internationale richtlijnen. In Nederland zijn met name de richtlijnen van het Nationaal Cyber Security Centrum (NCSC) leidend en Nedap Ons voldoet dan ook aan de door het NCSC gepubliceerde "ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)".

Voor de gebruikte (externe) libraries die zorgen voor de TLS verbindingen geldt dat door leveranciers beschikbaar gestelde beveiligingsupdates (uiterlijk) binnen 24 uur na beschikbaar stellen worden geïnstalleerd; in de praktijk veelal zelfs sneller.

Tussen de verschillende datacenters zijn volledig redundante, fysiek volledig gescheiden glasvezelverbindingen aangelegd. Al deze glasvezelverbindingen zijn bovendien volledig versleuteld door middel van de industry-standard technologie IEEE 802.1AE. Dit betekent dat iemand die toegang krijgt tot

één van de glasvezelverbindingen tussen onze datacenters daarmee nog steeds geen toegang kan krijgen tot informatie die tussen de datacenters wordt getransporteerd.

Mobiele applicaties

De mobiele applicaties van Nedap Ons zijn gratis en onbeperkt te downloaden uit de Apple Appstore voor iOS en uit de Google Play Store voor Android devices. Voordat met de applicaties toegang verkregen kan worden tot gegevens in Ons, moet het device eerst gekoppeld worden aan een gebruiker in Ons. Dit moet de gebruiker zelf doen. Na deze eenmalige koppeling is er met het betreffende device alleen toegang mogelijk tot gegevens waar de gemachtigde gebruiker ook toegang toe heeft. In de mobiele applicaties wordt de gebruikers na 15 minuten van inactiviteit opnieuw om een PIN code gevraagd.

De mobiele applicaties halen via beveiligde verbindingen de gegevens op uit Nedap Ons die noodzakelijk zijn voor die medewerker en voor die betreffende applicatie. De gegevens die worden opgehaald worden versleuteld opgeslagen op het mobiele apparaat. De mobiele applicaties zijn alleen te gebruiken na het invoeren van een PIN code. In het geval van diefstal of verlies van het device is het mogelijk om op afstand het device weer te ontkoppelen. Hierbij worden ook de versleutelde gegevens van het apparaat verwijderd. Ook worden gegevens die niet (meer) nodig zijn automatisch verwijderd van het mobiele apparaat.

Nedap Ons maakt geen verschil tussen privé- of bedrijfstoestellen. Het uitgangspunt is dat veiligheid altijd geborgd is in de applicaties zelf; onafhankelijk van andere beveiliging op het toestel. Zo is het bijvoorbeeld mogelijk om de koppeling met een toestel te verbreken zonder dat daarvoor het toestel zelf nodig is. Dit is nodig in het geval van verlies of diefstal, en kan door de gebruiker zelf worden gedaan in een webportaal. Ook een applicatiebeheerder (of iemand die daarvoor de juiste rechten heeft) kan een mobiel apparaat van een medewerker ontkoppelen.

Koppelingen met derde partijen

In de praktijk maakt Nedap Ons onderdeel uit van een applicatie-landschap waarbij gegevens worden uitgewisseld met derde partijen en koppelingen worden gelegde tussen Nedap Ons en derde partijen. De aard van deze koppelingen verschilt, maar de (technische) beveiliging is voor al deze koppelingen hetzelfde. Voor koppelingen met derde partijen geldt dat voordat een derde partij volledige toegang krijgt tot de API’s van Nedap Ons wordt een proces doorlopen waarbij de (potentiële) koppeling wordt getoetst op functioneren en wordt getoetst of de technische beveiliging van de koppeling voldoet aan onze eisen.

Ook ligt aan elke koppeling een overeenkomt ten grondslag, de zogenaamde "Aansluitvoorwaarden". Hier worden tussen Nedap en de derde partij afspraken gemaakt over de eisen die worden gesteld aan de (beveiliging van de) koppeling. De technische beveiliging van de API's van Nedap Ons is gebaseerd op twee-weg TLS (zogenaamde cliënt-certificaten). De transportbeveiliging voor de API's van Nedap Ons is gelijk aan die van overige gebruikers (zie "Beveiliging van gegevens tijdens transport").

Certificaten voor toegang tot de API's van Nedap Ons hebben een geldigheidsduur van maximaal een (1) jaar en moeten dus elk jaar actief worden vernieuwd. Certificaten voor toegang tot de API's van Nedap Ons worden enkel uitgegeven in opdracht van een klant van Nedap Ons. Voor de opdracht wordt gebruik gemaakt van het het ticketsysteem (self-service portal) van Nedap Ons. Hiermee wordt geborgd dat het *altijd* de klant is die bepaalt welke derde partijen toegang hebben tot welke gegevens via een koppeling. Elke klant van Nedap Ons kan op elk moment de toegang van een derde partij intrekken door een certificaat ongeldig te (laten) verklaren of in te trekken.

Let op! Zodra gegevens door een koppeling vanuit Ons zijn verstrekt aan een derde partij, heeft Nedap geen controle meer over de beveiliging van die gegevens. Hierover moet de klant *zelf* afspraken maken met de derde partij. Andersom geldt ook dat zodra een derde partij data naar Nedap Ons stuurt, Nedap niet verantwoordelijk kan zijn voor de inhoud van die informatie. Ook hierover moet de klant zelf afspraken maken met de derde partij.

Toegang tot gegevens door Nedap

Het inzien van persoonlijke gezondheidsgegevens door (medewerkers van) Nedap wordt zoveel mogelijk voorkomen. In het kader van de dienstverlening van Nedap Ons is inzage in persoonlijke gezondheidsgegevens echter niet helemaal te voorkomen (denk hierbij bijvoorbeeld aan het verlenen van tweedelijns support, of het onderzoeken van een melding die niet met geanonimiseerde gegevens te reproduceren is). Nedap Healthcare onderzoekt voortdurend mogelijkheden om de noodzaak tot inzage van gegevens (verder) terug te dringen. Hiervoor worden zowel technische als organisatorische maatregelen getroffen. Nieuwe medewerkers of ander personeel moet een VOG overleggen bij indiensttreding bij Nedap Healthcare waarbij - ondanks dat Nedap Healthcare zelf geen zorgverlener is - óók wordt gescreend op aspecten die met zorg te maken hebben, zoals "zorg voor minderjarigen", "zorg voor hulpbehoevende personen" en "zorg voor personen zoals ouderen en gehandicapten". Hiermee sluiten we zoveel mogelijk aan bij de screening zoals zorginstellingen deze ook uitvoeren. Nedap Healthcare heeft ook BIG-geregistreerde zorgverleners in dienst om de juiste en zorgvuldige omgang met persoonlijke gezondheidsgegevens te beoordelen met de zorginhoudelijke kant van de dienstverlening.

Toegang tot gegevens door medewerkers van Nedap Healthcare via de Nedap Ons applicaties wordt op dezelfde wijze ge-audit en gelogd als toegang tot gegevens door medewerkers van de zorginstelling zelf.

Toegang tot de IT-componenten die persoonlijke gezondsheidsgegevens opslaan of verwerken is alleen mogelijk met persoonlijke gebruikersaccounts. Medewerkers van Nedap Healthcare die voor het uitvoeren van hun werk toegang nodig hebben tot de IT-componenten krijgen deze alleen met een persoonlijk account zodat acties altijd tot een persoon te herleiden zijn. Twee-factor authenticatie wordt (ook) afgedwongen voor toegang tot de IT-componenten die persoonlijke gezondsheidsgegevens opslaan of verwerken. Gebruik van deze persoonlijke accounts wordt gelogd. Tot slot worden de toegangsrechten tot IT-componenten regelmatig gecontroleerd door het Privacy- & Security team van Nedap Healthcare.

Backups en restores

Naast de preventieve maatregelen zijn er ook correctieve maatregelen getroffen om in het geval van calamiteiten terug te kunnen vallen op manieren om eventuele ernstige incidenten op te kunnen vangen. De belangrijkste correctieve maatregel is het maken van backups. Door het maken van backups (reservekopieën) van de data van alle klanten kan in het geval van een incident een eerdere situatie worden hersteld. Dit zal in de regel gepaard gaan met data-verlies. Nedap Healthcare maakt (minimaal) 4 keer per dag een volledige backup van elke database van elke klant. Dit geldt niet alleen voor productie-omgevingen, maar ook voor opleidingsomgevingen, trainingsomgevingen en zelfs voor testomgevingen. De retentie van backups van testomgevingen is wel (iets) korter. Backups van omgevingen worden zowel on-site als off-site opgeslagen en gedurende 18 maanden bewaard.

Van de backups die gemaakt worden, wordt regelmatig getoetst of deze ook te gebruiken zijn om een hersteloperatie (restore) mee uit te voeren. Klanten kunnen een verzoek doen om een kopie van een productie-omgeving (al dan niet geanonimiseerd) beschikbaar te maken in een testomgeving. Hiervoor wordt een backup van de productie-omgeving teruggezet op een testomgeving. Dit proces kan (op aanvraag) elke dag worden uitgevoerd, inclusief het weekend. Door het grote aantal klanten van Nedap Healthcare, wordt deze functionaliteit voortdurend gebruikt en worden hiermee in de praktijk (vrijwel) dagelijks back-up-restores uitgevoerd.

Dreigingsinformatie

Nedap is deelnemer van Cyber Weerbaarheidscentrum Brainport (CWB). CWB is een zogenaamde OKTT voor de Nederlandse maak & high-tech industrie. Deelnemers van CWB slaan de handen ineen om samen een front te vormen tegen cybercriminaliteit. Daarnaast ontvangt Nedap dreigingsinformatie over

kwetsbaarheden en dreigingen van het Nationaal Cyber Security Centrum (NCSC). Het NCSC ontvangt dagelijks van diverse open en gesloten bronnen informatie over geïnfecteerde systemen. Vanuit deze positie is het NCSC in staat het CWB in een vroegtijdig stadium te waarschuwen als blijkt dat systemen van deelnemers getroffen zijn. Andersom koppelt Nedap ervaringen met incidenten en kwetsbaarheden terug aan het CWB, zodat het andere deelnemers en via NCSC andere sectoren op de hoogte kan stellen.

Deze dreigingsinformatie gebruikt Nedap bijvoorbeeld om preventief en actief domeinen, IP-adressen en software te blokkeren.

Toetsing, (pen)testen en certificering

Informatiebeveiliging hebben de voortdurende aandacht van onze organisatie. Nedap Healthcare heeft dan ook personeel in dienst met relevante securityervaring en -certificeringen (waaronder CISSP). Regelmatig wordt het onderwerp informatiebeveiliging met alle medewerkers besproken en worden verbeteringen doorgevoerd. Waar nodig wordt externe (specialistische) kennis ingehuurd en worden regelmatig door zowel interne medewerkers als externen testen uitgevoerd op verschillende onderdelen van onze dienstverlening. Daarnaast biedt Nedap Healthcare buitenstaanders (zoals hackers) een manier om eventueel gesignaleerde gebreken in de beveiliging te melden via een Coordinated Vulnerability Disclosure (CVD) programma. CVD stond vroeger ook wel bekend onder de naam "Responsible Disclosure".

General IT-controls (GITC) en de daarbij behorende beveiligingsmaatregelen zoals nodig voor IT-auditors (bijvoorbeeld in het kader van een jaarrekeningcontrole) worden halfjaarlijks door externe IT-auditors en accountants getoetst. Sinds 2018 wordt deze toetsing uitgevoerd door accountantskantoor BDO. Resultaat van deze audits zijn terug te vinden in onze ISAE3402 (Type 2) verklaring. Daarnaast is Nedap Healthcare zelf ISO 27001 en NEN 7510 gecertificeerd. Deze certificaten zijn te downloaden van het Supportportaal van Nedap Healthcare of op te vragen bij de accountmanager van Nedap Healthcare.

In overleg staan we altijd open voor aanvullende onderzoeken door klanten. Zo worden er regelmatig door securitybedrijven in opdracht van onze klanten onderzoeken uitgevoerd. Zolang deze onderzoeken vallen binnen de scope van de dienstverlening van Nedap Ons werken we hier altijd aan mee, om het vertrouwen in (de beveiliging van) onze oplossingen te ondersteunen en onderstrepen.