# NTA 7516 - vastlegging eisen door zorgorganisatie

In overleg met professional [NAAM ZORGMEDEWERKER] heeft [ORGANISATIE] de volgende minimale eisen vastgesteld met betrekking tot de criteria uit NTA 7516:

|  |  |  |  |
| --- | --- | --- | --- |
| **Groep** | **Criterium** | **Minimale eis van [ORGANISATIE]** | **Onderbouwing** |
| BESCHIKBAARHEID | Minimale beschikbaarheid | Minstens 99,8 % per jaar moet ad-hoc berichtenverkeer beschikbaar zijn. | Deze eis moet eraan bijdragen dat er niet wordt overgegaan op een onveilig alternatief. |
| Maximale uitvalduur | De hoogst aanvaardbare aaneengesloten uitvalduur is 24 uur. | Deze eis moet eraan bijdragen dat er niet wordt overgegaan op een onveilig alternatief. |
| Maximaal gegevensverlies | Geen enkel verlies is acceptabel, tenzij verzender binnen 24 uur na verzending geïnformeerd wordt. | Binnen de gestelde 24 uur is het nog haalbaar om informatie opnieuw te verzenden. |
| INTEGRITEIT | Herkomst-bevestiging | Er moet minimaal gebruik worden gemaakt van een 2-factorauthenticatie met gecontroleerd uitgifteproces. | Deze eis moet ervoor zorgen dat de verzender daadwerkelijk degene is die zich als zodanig uitgeeft. De eis kan worden geborgd op basis van [ONDERBOUWING – *bijv. Single Sign On via Active Directory met 2FA]*. |
| Data-integriteit | Wijzigen van de inhoud van een ad-bericht tussen verzending en ontvangst is niet toegestaan. | Deze eis moet borgen dat de ontvangen inhoud gelijk is aan de verzonden inhoud. |
| Onweerlegbaar-heid verzender | De herkomst van een ad-hocbericht kan niet door de verzender worden ontkend. Concreet betekent dit het inregelen van anti-spoofing maatregelen. | De ontvanger moet visueel kunnen vaststellen welke persoon of professional de afzender is van een ad-hocbericht. |
| Autorisatie verzender | De autorisatie van de verzendende medewerker moet worden gegarandeerd door [ORGANISATIE]. | Medewerkers worden geautoriseerd volgens interne procedures. |
| VERTROUWELIJKHEID | Gegevens-vertrouwelijkheid | Toegang tot opgeslagen berichten is verboden voor onbevoegden, berichten moeten worden versleuteld. | Met deze eis wordt de vertrouwelijkheid gewaarborgd. Deze eis geldt niet leveranciers voor leveranciers met wie een overeenkomst is afgesloten. |
| Toegangs-vertrouwelijkheid | Voor toegang tot ad-hocberichten geldt een minimale eis van 2-factorauthenticatie. | Vertrouwelijkheid wordt gegarandeerd door een betrouwbare autorisatie die past bij de verzonden gegevens. De eis kan worden geborgd op basis van [ONDERBOUWING – *bijv. Single Sign On via Active Directory met 2FA]*. |
| Communicatie-vertrouwelijkheid | Toegang voor onbevoegden tot berichten gedurende het transport (*in transit*) moet onmogelijk zijn. | Zonder deze eis is de vertrouwelijkheid niet gewaarborgd. |
| Verzendingsgrond | Er moet een beleid zijn met beschrijving van redenen om informatie te mogen delen (verzendingsgrond) en er moet worden gecontroleerd op de uitvoering van dat beleid. | De verzender bepaalt of een ontvanger gerechtigd is om het bericht te ontvangen. Het beleid van [ORGANISATIE] is dat medewerkers zijn gebonden aan geheimhouding, maar gegevens mogen delen als dat nodig is om de zorg voor cliënten of patiënten te leveren. Uiteraard alles met inachtneming van (zorg)wetten. |
| Internationaal ad‐hocberichten-verkeer | Verwerking buiten de Europese Economische Ruimte (EER) mag alleen conform regels AVG. | Wettelijke regels gelden ook voor [ORGANISATIE]. |
| GEBRUIKSVRIENDELIJKHEID | Continuïteit van ad‐hocberichten-verkeer – beantwoorden | Een ontvanger moet visueel kunnen zien of een bericht veilig is verzonden. | Deze eis stelt de ontvanger in de gelegenheid om via een veilige weg te reageren op het bericht. |
| Continuïteit van ad‐hocberichten-verkeer – doorsturen | De ontvanger van een bericht is zelf verantwoordelijk voor veilige verzending als deze een bericht doorstuurt. (Dit is strikt genomen geen grens, zo erkent NTA 7516.) | Als doorsturen niet veilig kan, moet de gebruiker hierop worden gewezen. Dit is in het bijzonder van nut als een cliënt of patiënt een veilig ontvangen bericht van [ORGANISATIE] wil doorsturen naar een naaste. |
| Veiligheid als gemak | Instellingen moeten standaard op veilig staan. | Deze eis is een implementatie van het principe ‘security by default’. |
| Leesbaarheid | De inhoud van berichten (zonder bijlagen) moet zonder aanvullende software of het maken van een account zichtbaar zijn voor de ontvanger. Als een persoon de informatie ontvangt, dan moet de online omgeving voldoen aan de eisen voor digitale toegankelijkheid (EN 301 549). | Het moet voor ontvangers niet nodig zijn om ergens een account aan te maken. Dit verlaagt de drempel om het bericht te openen. De omgeving moet ook leesbaar zijn voor mensen met een visuele beperking. |
| Eigen kopie | Het moet makkelijk zijn voor de ontvanger om een eigen kopie op te slaan. | De ontvanger van een ad-hocbericht moet het veilig en eenvoudig kunnen opslaan op een zelfgekozen locatie. |
| INTEROPERABILITEIT | Dossierkoppeling | De volgende eis wordt niet van toepassing verklaard voor [ORGANISATIE], omdat het volgens NTA 7516 niet verplicht is: *Het bericht moet makkelijk en veilig gekoppeld kunnen worden door de ontvanger en aan het juiste dossier.* | n.v.t. |

[ORGANISATIE] heeft regels vastgesteld (beleid) over hoe medewerkers gebruik mogen maken van geïmplementeerde communicatiemogelijkheden in [BELEID].

De naleving van dit beleid wordt continu gemonitord door het lijnmanagement en is onderdeel van interne audits op bewustzijn. Jaarlijks worden de leveranciers van ad-hocberichten vergeleken met de criteria die hierboven zijn vastgelegd.