Nedap N.V.
Parallelweg 2
7141 DC Groenlo
The Netherlands

T: + 31 544 471 111
info@nedap.com
nedap.com

Reactie van Nedap Healthcare op consultatie wetsvoorstel Diaz

We zijn blij met het voornemen om betrouwbare en eenduidige identificatie en authenticatie in de zorg breed mogelijk te maken. De tekst van het voorstel biedt over het algemeen goede handvatten om dit te gaan bewerkstelligen. Het bieden van moderne alternatieven voor de UZI-pas die in meer gevallen bruikbaar zijn, is noodzakelijk voor verdere samenwerking tussen zorgaanbieders, en biedt vele nieuwe mogelijkheden voor uitwisseling.

Echter op een aantal punten zien we praktische bezwaren of zorgen over privacy en beschikbaarheid. Punt 1 en 3 van onderstaande maken de uitrol bij kleine organisaties potentieel erg moeilijk of kostbaar - terwijl deze wet ook voor hen zeer relevant is.

1. Elk middel moet geaccepteerd kunnen worden door zorgaanbieders. Voor sommige middelen echter zijn extra kosten nodig voordat het gebruikt mag worden. Bij DigiD bijvoorbeeld is een pki-overheid certificaat nodig per zorgaanbieder. Er is nu geen garantie opgenomen dat het accepteren van middelen door zorgaanbieders kan zonder verdere kosten voor die zorgaanbieder. Het is de vraag of dit hierdoor haalbaar is voor vooral de kleinere zorgaanbieders.

2. Voor onder andere de technische interoperabiliteit van middelen wordt nu verwezen naar de NEN 7518. Echter, deze norm is nog niet af. Het is daardoor niet goed te beoordelen wat de impact van deze wetswijziging gaat zijn, zonder deze norm te kennen. Met name het gebruik van zorgaanbieder-specifieke middelen brengt mogelijk een wildgroei van middelen, die allemaal afzonderlijk getest, goedgekeurd en geaccepteerd moeten worden door alle partijen. Een dienst als TVS verlicht dit, maar ook andere implementaties zullen mogelijk moeten zijn. De vraag is of dit praktisch uitvoerbaar is, of dat extra garanties aan de interoperabiliteit van inlogmiddelen nodig zullen zijn voor een praktisch uitvoerbaar voorstel.

3. De mogelijkheid tot wallets wordt genoemd. Die bieden grote voordelen: in voorbeelden wordt bij DigiD 10 keer inloggen per dag genoemd - waarschijnlijk ook vanwege de zeer beperkte sessieduur van DigiD. Een zo groot aantal keer inloggen betekent een grote extra last voor zorgverleners: tijd voor inloggen, plus de tijd die kwijtgeraakt wordt omdat aandacht voor het daadwerkelijke werk wordt onderbroken bij elke poging tot inloggen. Een wallet kan dit probleem oplossen. Ook kan een wallet ervoor zorgen dat er toegang blijft op het moment dat de centrale voorzieningen niet te bereiken zijn. Het is echter de vraag hoe eenvoudig of ingewikkeld het zal zijn om een zorgverlener van zo'n wallet te voorzien. De praktische uitvoerbaarheid staat of valt bij hoe een afgeleid middel zoals een wallet uitgegeven kan worden, ook voor kleine zorgaanbieders en voor zorgverleners die niet regelmatig op een centrale locatie zijn. Dat lijkt nu niet voldoende duidelijk.

4. Een centrale log van inlogpogingen bij het CIBG is een behoorlijke inperking op de privacy van medewerkers. Het staat bovendien haaks op wat er in de eIDAS staat, waar wallets op geen enkele manier mogen zien wie er waar ingelogd heeft. Mogelijk speelt dit bezwaar ook bij private middelen. Eisen daarvoor zouden opgenomen kunnen worden in de NEN 7518 of het goedkeuringsproces - maar dit staat niet in dit wetsvoorstel beschreven. Het toevoegen van eisen aan zo'n proces wat betreft privacy in de wet specifiek voor de zorg zou dit kunnen oplossen.

5. De continue werking van het centrale register wordt in dit systeem cruciaal. Bij serviceonderbrekingen van het centrale register functioneren middelen die direct inloggen niet meer. Bovendien is het niet mogelijk kort geldige wallets aan te maken. Hoe korter de geldigheid van sessies, hoe hoger de beschikbaarheid zal moeten zijn. Tevens heeft inbreuk in dit systeem verregaande gevolgen, bijvoorbeeld het lekken van logging. Is er voldoende stilgestaan bij deze risico's, en worden daar de juiste maatregelen voor genomen?