Geacht informatieberaad zorg,

Hierbij een reactie vanuit ChipSoft op de open consultatie Health Tools Interoperability (HTI) als (kandidaat)bouwsteen voor het duurzaam informatiestelsel in de zorg.

Scope van de reactie:
Graag willen we benadrukken via deze consultatie expliciet niet inhoudelijk te reageren op de ontwikkelingen binnen bijvoorbeeld koppeltaal, waarbij eHealth apps gekoppeld worden aan zorgsystemen. Dit benoemen we graag, omdat er veel raakvlakken en samenwerkingen zijn tussen HTI, koppeltaal (2.0) en bijvoorbeeld MedMij modules (RFC0026).

Context:
internationale ontwikkelingen rondom lanceren van gezondheid (eHealth) apps:
Deze HTI standaard baseert zich op een internationale standaard uit de onderwijswereld. Het omarmen van internationale standaarden is essentieel in de zorg en het is mooi dat hierbij ook wordt gekeken naar standaarden uit andere sectoren dan enkel de zorg. De HTI-standaard (zorg-variant) is ontworpen om als eindgebruiker (burger) vanuit een (private) webomgeving zoals bijvoorbeeld een PGO een bepaalde taken/programma's van een "module" zoals een digitale zorg(preventie)-applicatie te kunnen openen/activeren zonder dat hierbij (persoons)gegevens beschikbaar worden gesteld aan de betreffende applicatie. Dit laatste is essentieel, want voor het gericht lanceren van taken binnen eHealth-applicaties waarvoor ook gevoelige gegevens uitgewisseld worden bestaan reeds internationale beproefde zorgstandaarden zoals (HL7 FHIR) Smart Application Launch framework. Om een innovatief, duurzaam en veilig landschap te creëren en behouden voor eHealth-applicaties in Nederland, heeft dan ook absoluut de voorkeur om voor dergelijke usecases altijd aan te sluiten bij internationale zorg-standaarden.

De HTI standaard gaat er dus in de basis vanuit dat de applicatie welke gelanceerd wordt geen persoonsgegevens of andere gevoelige data nodig heeft. Indien noodzakelijk zal de gelanceerde applicatie zelf de mogelijkheid voor invoer van (persoons)gegevens moeten verzorgen. Ditzelfde geldt ook voor authenticatie-voorziening indien een eindgebruiker later weer toegang wil krijgen tot dezelfde taak/programma binnen de betreffende gelanceerde applicatie via een andere route dan waaruit deze via HTI is gelanceerd. Wel kan er bijvoorbeeld een vorm van (consistent pseudo) user-ID worden meegegeven en een vorm van context-kenmerk om door te geven wat voor soort taak/programma gelanceerd moet worden, maar deze zou niet herleidbaar mogen zijn tot de persoon. Omdat beide voorbeelden (zowel user als module-context) uiteindelijk gekoppelde pseudoniemen zijn, kan ook deze informatie uiteindelijk herleidbaar en daarmee potentieel gevoelig zijn. Bijvoorbeeld User "PAT6463" heeft programma "LON25" gestart. ID's die "nietszeggend" zijn kunnen (zeker indien zij consistent zijn) door aanvallers misbruikt worden via bijvoorbeeld raden van hun betekenis. De standaard voorziet wel in de optie om eventueel ook (JWE) versleuteld informatie mee te kunnen geven via de browser, maar een backchannel ontbreekt echter. Communicatie via backchannel is vanuit beheer (afstemming verbindingen) een zwaarder middel, maar een gebruikelijker alternatief. Er moet dus enorm gewaakt worden voor (her)gebruik van HTI voor toepassingen waarvoor het niet geschikt is en hiermee dus een glijdende schaal van toepassing voor gevoelige informatie verzenden tussen applicaties via de browser te voorkomen. Indien de HTI standaard breder zou worden ingezet (scope creep), bijvoorbeeld voor het op voorschrift van zorgverleners gericht allerlei informatie verzenden voor het lanceren van eHealth-programma's aan patiënten vanuit een patiëntportaal zien we direct diverse risico's.

Risico's en kwetsbaarheden:
Door bovenstaande gedachte (geen persoonsgegevens delen) achter HTI is het ontwerp eenvoudig en verloopt alle verkeer via de (als onveilig te beschouwen) browser van de eindgebruiker. Het risico is dus dat de standaard ingezet wordt voor usecases waarbij (afgeleide) gevoelige informatie tussen

applicaties via de browser verloopt. Dit is dus het geval indien de standaard bijvoorbeeld zou worden gebruikt voor het openen van zorg-applicaties vanuit bijvoorbeeld een patiëntenportaal van een zorginstelling waarbij dan gevoelige gegevens via de browser van de eindgebruiker naar een andere applicaties wordt verzonden. Hiermee kent inzet van deze standaard tevens een kwetsbaarheid op bijvoorbeeld replay attacks naar de module doordat een kwaadwillende het request uit de browser kan uitlezen en hergebruiken. Hiernaast zijn door gebrek aan backchannel-verkeer maatregelen zoals certificate pinning noodzakelijk om man in the middle aanval te voorkomen, waarmee een kwaadwillende zich kan voordoen als module/applicatie die de eindgebruiker wil starten (spoofing). We adviseren dan ook om vooral om zeer zorgvuldig te zijn in de toepassingsmogelijkheden voor deze standaard.

Standaardisatie:
In het algemeen staan we dus positief ten opzichte van nieuwe innovatieve standaarden die bijvoorbeeld volgens het privacy-by-design principe minimale gegevens nodig hebben. Echter zien we een risico aan deze wijze van standaardisatie via het informatieberaad als Nederlandse bouwsteen. Een goede waarborg voor de geschikte toepassingsmogelijkheden van deze standaard lijkt te ontbreken, met risico op foutieve (te brede) toepassing in de praktijk. Tevens dient er bij voorkeur een controle ingebouwd te worden voor juiste implementatie, zeker omdat deze standaard een nieuwe aanvulling is naast breder gebruikte internationale standaarden in de zorg.

We hopen hiermee een zinvolle en constructieve bijdrage te hebben geleverd, mochten er vragen zijn, dan horen we het graag.