Katern PURA over privacy en informatieveiligheid

Opstellers: Architectuurboard GGD GHOR NL (Anja Teeuwen en Sergio Richardson).

Uitgangspunten:

PURA erft de principes en richtlijnen van de NORA over; daarmee zijn de thema's beveiliging en privacy van de NORA richtinggevend. In deze PURA katern privacy en informatieveiligheid worden daarom enkel die zaken opgenomen die nog niet of nog onvolledig in de NORA beschreven zijn.

Inhoud van de katern PURA privacy en informatieveiligheid

Aanvullende onderwerpen op het gebied van privacy en informatieveiligheid die voor de publieke gezondheidszorg relevant zijn en daarom aanvullend op de NORA katern beschreven worden.

1. Aanvullende wet- en regelgeving gezondheidszorg
2. Gevolgen AVG voor publieke gezondheidszorg.
3. Geconcretiseerde richtlijnen voor leveranciers.

Aanvullende wet- en regelgeving gezondheidszorg

In de gezondheidszorg zijn aanvullend aan de andere e-overheidsprincipes ook de volgende wet- en regelgevingskaders aanwezig:

A. Wet op de geneeskundige behandelingsovereenkomst. De Wet op de geneeskundige behandelingsovereenkomst (WGBO) regelt de rechten en plichten van de patiënt. Zo staat in deze wet dat patiënten recht hebben op informatie en dat zij toestemming moeten geven voor een behandeling. Ook regelt de WGBO de privacy van de patiënt, het recht op een *second opinion,* het inzagerecht van patiënten in hun eigen medisch dossier en de vertegenwoordiging van patiënten als zij niet zelf kunnen beslissen. Daarnaast verplicht de WGBO zorgverleners om een medisch dossier bij te houden.
B. Wet cliëntenrechten bij elektronische verwerking van gegevens in de zorg en de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg. De wet cliëntenrechten heeft ertoe geleid, dat een aantal andere wetten is gewijzigd (aangescherpt), waaronder de Wet gebruik burgerservicenummer in de zorg (Wet BSN-z). De Wet BSN-z heet sinds de wetswijziging "Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg" (Wabvpz). Concreet zijn de aanscherpingen:
    - De plicht voor de zorgaanbieder om uitdrukkelijke toestemming van de patiënt te verkrijgen voor het uitwisselen van gegevens. Per 1-7-2020 dient de patiënt bovendien in staat te kunnen zijn om aan te geven welke gegevens wel of niet door welke (categorieën van) zorgverleners mogen worden ingezien (gespecificeerde toestemming).
    - De plicht van de zorgaanbieder om de patiënt informatie te verstrekken over zijn rechten bij elektronische gegevensuitwisseling, de wijze waarop hij zijn rechten kan

uitoefenen en over de werking van het elektronisch uitwisselingssysteem (in werking per 1-7-2017).

- De plicht van de zorgaanbieder om ervoor te zorgen dat het elektronisch uitwisselingssysteem dat hij gebruikt, vastlegt wie gegevens beschikbaar heeft gesteld en wie ze heeft ingezien (logging) (treedt in werking per 1-72020).
- Het recht van de patiënt op een afschrift van zijn dossier, of van de gegevens betreffende deze patiënt die de zorgaanbieder via een elektronisch uitwisselingssysteem beschikbaar stelt. En de plicht van de zorgaanbieder om deze gegevens elektronisch beschikbaar te stellen (het tweede deel van deze bepaling treedt per 1-7-2020 in werking).

Gevolgen AVG voor de publieke gezondheidszorg:

- Recht op data portabiliteit → elektronische overdracht wordt ondersteund. Het recht op data portabiliteit houdt in dat de betrokkene in bepaalde gevallen (namelijk wanneer er sprake is van elektronische gegevensverwerking) het recht heeft om zijn gegevens in een gestructureerde, gangbaar en machine-leesbare vorm te verkrijgen. En dat hij deze mag overdragen aan een andere verantwoordelijke.
- Recht op vergetelheid → een persoon heeft het recht om zijn gegevens te laten wissen, tenzij het om medische dossiers gaat, daar geldt een bewaarplicht van 15 jaar. Een persoon kan wel vragen om bepaalde gegevens uit het medisch dossier te wissen.

Geconcretiseerde richtlijnen voor leveranciers voor implementeren wet- en regelgeving in het kader van privacy

1. Leverancier hanteert het principe 'Privacy by design '
   Zowel voor nieuwe ontwikkelingen als bij onderhoud .
2. Leverancier bouwt applicatie conform het principe van 'privacy by default'':
   Technische maatregelen die ervoor zorgen dat standaard alléén persoonsgegevens verwerkt kunnen worden die noodzakelijk zijn voor het specifieke doel waarvoor de applicatie dient.
3. Applicaties dienen het afschermen van gegevens conform wet- en regelgeving maximaal te ondersteunen. Daarbij dient de WGBO ondersteund te worden zodat alleen degene die een behandelrelatie heeft met een cliënt diens gegevens mag zien.
4. Gegevens dienen onweerlegbaar te zijn, de herkomst/bron van registratie dient vastgelegd te zijn.
5. Ondersteunen van logging: Een cliënt dient te allen tijde inzage te hebben in de raadplegingen en bewerkingen die op zijn gegevens hebben plaatsgevonden.
6. Ondersteunen van het recht om gegevens te wissen. Een cliënt mag vragen om medische gegevens te laten vernietigen.

Geraadpleegde bronnen:

VZVZ Factsheet LSP – en privacywetgeving: https://www.vzvz.nl/media/downloads/factsheet-lsp-en-privacywetgeving/download