Gedragscode Elektronische Gegevensuitwisseling in de Zorg (EGiZ)

Samenvatting, september 2019

De Gedragscode Elektronische Gegevensuitwisseling in de Zorg (EGiZ) bundelt de bestaande privacyregels voor uitwisseling van patiëntgegevens en helpt zorgverleners zo bij de naleving daarvan. Doel: een veilige gegevensuitwisseling. De koepels van zorgverleners hebben deze regels op een rij gezet om in elke (praktijk)situatie aan de wettelijke regels rond privacy en beroepsgeheim te kunnen voldoen. De gedragscode bevat dus geen nieuwe regels. De opstellers gaan er van uit dat alle zorgaanbieders inmiddels ook voldoen aan de wettelijke voorschriften met betrekking tot autorisatie en beveiliging.

De gedragscode gaat uit van het volgende samenspel:

- Wanneer een patiënt bij een *zorgaanbieder* in behandeling is, legt deze zorgaanbieder gezondheidsgegevens van de patiënt vast. Deze gegevens kunnen van belang zijn voor andere *zorgverleners* die een *behandelrelatie* met de patiënt hebben.
- Zodra sprake is (of wordt) van daadwerkelijke gegevensuitwisseling, noemen we de eerstgenoemde zorgaanbieder de *brondossierhouder*. Deze aanbieder houdt immers het patiëntendossier bij dat als brondossier dient voor de als tweede genoemde zorgverlener, die we dan de *dossierraadpleger* noemen.
- Naast de patiënt, de brondossierhouder en de dossierraadpleger is nog een 4e partij van belang, nl. de *verwerkingsverantwoordelijke* voor (het systeem van) de gegevensuitwisseling.
- Bij gegevensuitwisseling wordt onderscheid gemaakt tussen 'push-' en 'pull-verkeer'.
    - Bij 'push-verkeer' ligt het initiatief voor gegevensuitwisseling bij de verzender, de brondossierhouder dus. Die verstuurt gericht bepaalde gegevens naar één of enkele ontvangers waarvan de behandelrelatie met de betrokken patiënt vaststaat.
    - Bij 'pull-verkeer' stelt de brondossierhouder gegevens beschikbaar voor raadpleging door andere zorgverleners (dossierraadplegers). Op voorhand staat niet vast wie uiteindelijk de gegevens zullen raadplegen. Het initiatief voor de daadwerkelijke gegevensuitwisseling ligt dus bij de dossierraadpleger.

De gedragscode stelt dan het volgende:

- De technieken van gegevensuitwisseling en de organisatie eromheen, moeten voldoende beveiliging bieden tegen onrechtmatige kennisneming. Daarvoor gelden als normen:
    - Veilige en betrouwbare aanmeldprocedures voor gebruikers (inloggen, identificatie en authenticatie). Zorgverleners gebruiken daarvoor de UZI-pas of vergelijkbaar.
    - Gebruik van BSN om patiënt aan te duiden.
    - Logging van acties en controle op de logging.
    - Registratie en opvolging van patiënttoestemming (bij 'pull') dan wel -bezwaar (bij 'push')
    - Bij 'pull': controle op behandelrelatie bij raadpleging en waarborgen van autorisatieregels.
- De verwerkingsverantwoordelijke zorgt voor:
    - gezamenlijk autorisatiebeleid, met zeggenschap voor patiëntenvertegenwoordiging;
    - (toezicht op) bovengenoemde technische en organisatorische maatregelen;
    - heldere en actuele publieksinformatie over gegevensuitwisseling;
    - inrichting van een klantloket voor uitoefening van patiëntrechten m.b.t. de specifieke gegevensuitwisseling(en) waarvoor de verantwoordelijke verantwoordelijk is (indien patiënt hiervoor niet rechtstreeks naar brondossierhouder gaat).
- De brondossierhouder zorgt voor:
    - persoonlijke informatie over gegevensuitwisseling(en), met verwijzing naar verantwoordelijke(n), diens publieksinformatie en diens klantloket;

    - desgewenst: persoonlijke informatie over raadpleging van het dossier (uit de logging);
    - bij 'pull': expliciete toestemming van de patiënt (opt-in) om zijn/haar gegevens beschikbaar te stellen;
    - bij 'push': opvolging van eventueel gemaakt bezwaar tegen verzending van gegevens.
- De toestemming die een patiënt geeft aan een brondossierhouder is generiek, d.w.z. ongeacht de techniek en geldend voor alle uitwisselingssystemen, mits voor al die systemen aan de overige voorwaarden in de code is voldaan.

Wat betekent de code ....

...voor de zorgaanbieder die gegevens van een patiënt bijhoudt en deze wil delen met anderen?

- Bij push:
    - Vergewis je ervan dat het systeem waarmee je de gegevens verzendt vertrouwd is en voldoende beveiligd.
    - Zorg ervoor dat je alleen gegevens verzendt aan zorgverleners die een behandelrelatie met de patiënt hebben (of krijgen).
    - Informeer de patiënt over de gegevensuitwisseling(en), eventueel via (permanente) verwijzing naar publieksinformatie, bijvoorbeeld via de privacyverklaring van de verwerkingsverantwoordelijke.
    - Bied patiënt de mogelijkheid tot bezwaar tegen verzending.
- Bij pull:
    - Vergewis je ervan dat alle pull-systemen waarop je bent aangesloten een duidelijke verwerkingsverantwoordelijke hebben die de waarborgen conform de code regelt (als dit niet zo is, kun je de vertrouwensrelatie die een patiënt met je is aangegaan onvoldoende waarmaken en zou je je moeten afsluiten van het betreffende systeem).
    - Informeer de patiënt over de gegevensuitwisseling(en), eventueel via (permanente) verwijzing naar publieksinformatie van de verwerkingsverantwoordelijke en ook via eigen informatiemateriaal en website van de zorgaanbieder.
    - Zorg voor toestemming van de patiënt, vóórdat je diens gegevens beschikbaar stelt (of laat stellen) voor raadpleging.
    - (Zorg voor vertegenwoordiging bij de verwerkingsverantwoordelijke i.v.m. opstellen en onderhouden van autorisatiebeleid).

...voor de zorgaanbieder die gegevens van een patiënt krijgt (push) of wil raadplegen (pull)?

- Bij push:
    - Vergewis je ervan dat de gegevens inderdaad voor jou bedoeld zijn.
- Bij pull:
    - Bied patiënt mogelijkheid tot bezwaar tegen raadpleging.
    - (Zorg voor vertegenwoordiging bij verwerkingsverantwoordelijke i.v.m. opstellen en onderhouden van autorisatiebeleid).

...voor de verwerkingsverantwoordelijke (bij pull)

- Zorg voor gezamenlijk autorisatiebeleid, met zeggenschap voor patiëntenvertegenwoordiging.
- Zorg voor passende technische en organisatorische maatregelen. Neem daarbij de verantwoordelijkheid voor de hele keten (niet alleen het centrale uitwisselingssysteem, maar ook de aansluiting van zorgverleners en hun systemen).
- Zorg voor heldere en actuele publieksinformatie over de gegevensuitwisseling.
- Richt een klantloket in voor vraagstukken van patiënten m.b.t. de gegevensuitwisseling.

...voor ICT-leveranciers

- Richt de systemen in op basis van beveiligingsnormen in de code, uiteraard in opdracht van je klant: verwerkingsverantwoordelijke(n) dan wel zorgaanbieders.

- Zorg ervoor dat de systemen ook voldoen aan de overige wettelijke eisen.

...voor de patiënt

- Geef toestemming aan je zorgverlener om jouw informatie raadpleegbaar te maken (tenzij je dit niet wilt natuurlijk).
- Maak, indien je bezwaar hebt tegen verzending of raadplegen van gegevens door zorgverleners, dat bezwaar tijdig aan die zorgverlener kenbaar.
- Zorg dat je, indien je dit wilt, geïnformeerd bent over de gegevensuitwisseling waarop jouw zorgaanbieder is aangesloten (of wil aansluiten). Vraag ernaar bij je zorgaanbieder of lees de informatie waarnaar hij of zij je verwijst. Zorg ook dat je weet waar en hoe je eerder gegeven toestemming dan wel gemaakt bezwaar kunt intrekken.
- Kijk of vraag af en toe eens naar de logging t.a.v. jouw gegevens: wie heeft jouw gegevens geraadpleegd?