met spoed beschikbaar

Hoe beperk je de risico's van verwisseling van medische gegevens in de acute zorg?

Digitale gegevensuitwisseling is cruciaal in de spoedzorg. Het ondersteunt zorgverleners beter in hun werk, zodat de patiënt sneller de juiste zorg op de juiste plaats krijgt. De wet verplicht het gebruik van het BSN wanneer zorgverleners onderling patiëntgegevens uitwisselen. Daarbij is de voorwaarde dat de patiënt geïdentificeerd wordt met een wettelijk identiteitsdocument (WID).
Maar wat doe je als dat in de spoedsituatie niet lukt? Als je de identiteit van een patiënt niet kent of als je geen tijd hebt voor de persoonsidentificatie?

Zorgverleners wisselen in een spoedsituatie, waarbij de persoonsidentificatie niet mogelijk is, dan ook gegevens uit:

- Zonder BSN Deze gegevens leveren immers een belangrijke bijdrage voor de juiste zorg verderop in de keten.
- Met een BSN zonder persoonsidentificatie: Bijvoorbeeld door de identiteit van de patiënt op basis van (controle)vragen vast te stellen. Opvolgende zorgverleners gebruiken dit BSN immers om medische gegevens van de patiënt te raadplegen.

Met een WID kun je de patiënt identificeren en met zekerheid vaststellen dat het BSN van de patiënt is. Zonder persoonsidentificatie is dit niet mogelijk en kunnen er risico's verderop in de acute zorgketen ontstaan.

Wat zijn de risico's van een BSN zonder persoonsidentificatie?

Verkeerde voorbereiding: Als achteraf blijkt dat het BSN niet van de patiënt was, dan kunnen medische gegevens van een andere patiënt worden geraadpleegd. Hierdoor kunnen zorgverleners verkeerde voorbereidingen treffen. Het gevolg kan zeer schadelijk zijn voor de patiënt, omdat essentiële medische gegevens worden gemist of onjuist zijn.

Dossiervervuiling: Als achteraf blijkt dat het BSN niet van de patiënt was, dan worden de bij de behandeling vastgelegde en/of ontvangen gegevens aan het verkeerde dossier gekoppeld. Hierdoor ontstaat dossiervervuiling. Daarnaast ontstaat een dossiertekort voor zorgverleners die de patiënt verder behandelen in het ziekenhuis. Het gevolg kan zeer schadelijk zijn voor de patiënt, omdat essentiële medische gegevens worden gemist of onjuist zijn.

Privacyschending: Als achteraf blijkt dat het BSN niet van de patiënt was, dan kunnen medische gegevens van een andere patiënt worden geraadpleegd. Hierdoor wordt de privacy van een andere patiënt geschonden, namelijk van degene van wie het BSN is.

Welke maatregelen kun je treffen om de risico's te beperken?

Om de risico's te verkleinen is het goed om onderling afspraken te maken over de uitvoering van persoonsidentificatie. Het is goed om met elkaar de verwachtingen ten aanzien van persoonsidentificatie en de impact hiervan op het zorgproces uit te spreken.

Wat kan de verzender doen?

Het beste is natuurlijk om een persoonsidentificatie uit te voeren, zodat verwisseling van medische gegevens in de acute zorg niet kan gebeuren. Deze persoonsidentificatie bestaat uit het vaststellen van de identiteit aan de hand van het WID en het controleren van de geldigheid van het WID.

Helaas is dit in een spoedsituatie niet altijd uit te voeren.

Alternatief is om het BSN op te vragen en het BSN te controleren door de patiënt daarbij zoveel mogelijk controlevragen te stellen. Als hiervoor gekozen wordt, is het van belang om in de uitwisseling mee te geven dat er geen persoonsidentificatie heeft plaatsgevonden.

Zodra de gelegenheid zich voordoet, voer je de persoonsidentificatie alsnog uit om de administratie eventueel hierop te corrigeren. Tot die tijd is het van belang om te onthouden dat:

- als de ontvangen gegevens worden toegevoegd aan een bestaand dossier, dat dit mogelijk niet het correcte dossier is ('dossiervervuiling').
- als er gegevens opgevraagd worden, deze mogelijk niet bij de patiënt horen ('treffen van verkeerde voorbereiding').

Als je na persoonsidentificatie constateert dat je het verkeerde BSN meegestuurd hebt, licht je de zorgaanbieder waarmee je hebt uitgewisseld hierover in ('dossiervervuiling').

Bij onterechte opvraging van medische gegevens geef je een melding door aan de zorgaanbieder bij wie de gegevens zijn opgevraagd, zodat deze van het misverstand op de hoogte is. Ook moet overwogen worden om de patiënt wiens gegevens onterecht zijn opgevraagd, te informeren. Onterecht opgevraagde gegevens worden direct weer verwijderd ('privacyschending').

Wat kan de ontvanger doen?

Als ontvangende zorgaanbieder moet je de persoonsidentificatie altijd zelf doen zodra de gelegenheid zich voordoet. Om de risico's tot die tijd te beperken is het van belang dat je:

- onthoudt dat de informatie die op basis van het ontvangen BSN is opgezocht, mogelijk niet bij de betreffende patiënt hoort ('treffen van verkeerde voorbereiding').
- de ontvangen informatie niet direct aan een dossier in het eigen EPD koppelt. De gegevens worden zolang aangemerkt als 'van buiten ontvangen gegevens' of nog apart van het eigen dossier bewaard ('dossiervervuiling').

Als je na persoonsidentificatie constateert dat de verzender het verkeerde BSN meegestuurd heeft, licht je de verzender direct hierover in. Ook in hun EPD is dan immers een verkeerd BSN vermeld ('dossiervervuiling').

Bij onterechte opvraging van medische gegevens geef je een melding door aan de zorgaanbieder bij wie de gegevens zijn opgevraagd, zodat deze van het misverstand op de hoogte is. Ook moet overwogen worden om de patiënt wiens gegevens onterecht zijn opgevraagd, te informeren. Onterecht opgevraagde gegevens worden direct weer verwijderd ('privacyschending').

Doel van digitale gegevensuitwisseling

Het doel van digitale gegevensuitwisseling is om zorgverleners adequaat te ondersteunen. Zij kunnen niet blind vertrouwen op de informatie die ze op deze manier ontvangen. De zorgverlener houdt zijn eigen onderzoeksplicht om de ontvangen gegevens te toetsen, bijvoorbeeld door contact met de patiënt, familie of naasten.