Waarborging patiëntgegevens

Welke persoon kan welke gegevens inzien?

- Huisarts / POH / assistente waarvoor op aanvraag van de zorggroep of praktijk een login is verstrekt:
    - De in het KIS ingeladen dossiers van de patiënten die tot de praktijk behoren.
    - Een deel van de meetwaarden die ingevoerd zijn door de ketenpartners, en de rapportage die teruggekoppeld is door de ketenpartners. Er is geen inzage in de overige gegevens die door de ketenpartners zijn vastgelegd (bijv. eetverslag).
- Ketenpartner waarvoor op aanvraag van de zorggroep een login is verstrekt:
    - Een, op basis van de betreffende discipline/rol, beperkt gedeelte van het patiëntdossier wat relevant is voor die rol en dan alleen voor die patiënten die daadwerkelijk door de huisartsenpraktijk verwezen zijn.
- Zorggroep:
    - Alle vastgelegde meetwaarden, incl. de daarop gebaseerde indicatoren- en declaratiegegevens.
- VitalHealth:
    - De personen die configuratie en support uitvoeren, kunnen toegang hebben tot de gegevens in het KIS.

Beveiliging van geautoriseerd gebruik

Bovenstaand gebruik is als volgt beveiligd:

- De autorisatie van gebruikers:
    - Alle gebruikers krijgen persoonsgebonden inloggegevens.
    - Het advies is om het wachtwoord direct te wijzigen na uitgifte van de inloggegevens. In het KIS is hierin voorzien door bij de eerste keer inloggen de gebruiker te vragen een eigen wachtwoord in te geven. Hierbij wordt dringend geadviseerd om geen wachtwoorden als welkom01 en 1234567 te gebruiken.
    - Het tweede advies is om de inloggegevens strikt persoonlijk te houden en nergens te noteren.
    - Om het risico op uitlekken van logingegevens te verkleinen, vraagt het KIS iedere 90 dagen om een nieuw wachtwoord in te geven.
    - Er wordt geregistreerd welke gebruiker op welk tijdstip is ingelogd geweest in het KIS.
    - Het KIS kan door de gebruikers alleen benaderd worden via een beveiligde internetverbinding, te herkennen aan “https” in de URL.
- Specifiek voor VitalHealth is de integriteit van het omgaan met data als volgt gewaarborgd:
    - Tussen de zorggroep en VitalHealth is contractueel vastgelegd hoe er omgegaan wordt met de gegevens.

- De medewerkers die toegang hebben tot vertrouwelijke gegevens, benutten deze toegang strikt alleen wanneer dit noodzakelijk is t.b.v. het uitvoeren van configuratie of support of op uitdrukkelijk verzoek van de klant. Deze toegang wordt uitgevoerd onder een geheimhoudingsplicht, wat contractueel met iedere medewerker is vastgelegd.

Beveiliging tegen ongeautoriseerd gebruik

- De gegevens zijn opgeslagen op beveiligde servers in beveiligde datacentra, die alleen gekoppeld zijn via een beveiligde netwerkverbinding (bijv. Ezorg).
- De gebruiker wordt automatisch uitgelogd wanneer deze 15 minuten niet actief geweest is in het KIS. Dit om toegang door onbevoegden te voorkomen.

Uitwisseling van gegevens tussen HIS en KIS

- Deze uitwisseling vindt plaats volgens de landelijke OZIS-ketenzorg-standaard. Deze standaard beschrijft welke gegevens volgens welke procedures worden uitgewisseld.
- De gegevens worden binnen een beveiligd netwerk uitgewisseld (bijv. Ezorg).
- De patiëntgegevens kunnen door de gebruiker worden uitgewisseld tussen HIS en KIS, wanneer hiervoor in het KIS de toestemming van de patiënt is geregistreerd. De zorggroep bepaalt op welke manier de toestemming aan de patiënt wordt gevraagd en hoe dit wordt vastgelegd.
- De huisartsenpraktijk kan deze toestemmingsregistratie gebruiken als voorwaarde voor verwijzing naar ketenpartners.
- Wanneer het HIS vanuit het KIS bevraagd is, wordt er een melding vanuit het KIS verzonden naar het HIS. Dit wordt door het HIS verwerkt in het patiëntdossier.
- In overleg met de zorggroep zijn c.q. worden, als onderdeel van de inrichting van het KIS, de patiëntdossiers vanuit het HIS collectief ingeladen in het KIS. De notificatie hiervan naar het HIS is uitgezet, om vervuiling te voorkomen. Wanneer gewenst is het mogelijk dit aan te zetten.