Onderwerp: Belangrijke mededeling in verband met uw persoonsgegevens

Enschede, 17 april 2026

Geachte patiënt,

U ontvangt deze mail omdat wij u uit voorzorg willen waarschuwen voor mogelijke risico's op misbruik van uw persoonsgegevens.

Afgelopen periode is er berichtgeving geweest over de cyberaanval bij Chipsoft van 7 april 2026. Daarbij hebben cybercriminelen ransomware (gijzelsoftware) ingezet, waarmee systemen van ChipSoft zijn versleuteld. ChipSoft geeft aan direct maatregelen te hebben genomen om de gevolgen van dit incident zoveel mogelijk te beperken.

Roessingh maakt gebruik van de dienstverlening van ChipSoft voor ons elektronisch patiëntendossier en wij hebben alle door ChipSoft aangegeven maatregelen opgevolgd.

Op 16 april heeft ChipSoft ons geïnformeerd dat de cybercriminelen mogelijk toegang hebben gehad tot patiëntgegevens van Roessingh. Op dit moment zijn wij de gevolgen van deze informatie voor u en voor Roessingh aan het onderzoeken. Zodra wij meer informatie hebben over de mate waarin uw persoonsgegevens betrokken zijn, informeren we u hier waar mogelijk persoonlijk over.

In de tussentijd vragen we u uit voorzorg op te letten voor het volgende:

- Zoals u wellicht al weet, kunnen derden persoonsgegevens proberen te misbruiken. Bijvoorbeeld door zich via de telefoon of via e-mail voor te doen als iemand van uw bank. Blijf daarom altijd alert op dit soort telefoontjes, sms'jes, appjes of e-mails.

- Let goed op bij het openen van links in e-mails, sms'jes en appjes. U kunt een verdachte e-mail, sms of app vaak herkennen aan typfouten en onbekende afzenders. Controleer het telefoonnummer. Of wat er na het '@'-teken van een e-mailadres staat.

- Krijgt u een onverwacht telefoontje van een nummer dat u niet kent? Het kan zijn dat er echt een medewerker van uw bank of een ander bedrijf belt. U kunt dit controleren door de beller te vragen naar zijn/haar voor- en achternaam en hem/haar te vragen naar het algemene telefoonnummer is van het bedrijf. Zeg dat u graag eerst wil controleren of de persoon een echte medewerker is en hang op. Controleer vervolgens op de website van het bedrijf of het nummer inderdaad klopt. Klopt het nummer? Bel dan zelf en vraag naar de medewerker die u heeft gebeld.

- Geef nooit iemand uw wachtwoord of pincode.

- Criminelen proberen soms de gegevens van een geldig identiteitsdocument te gebruiken om namens iemand anders spullen te kopen, een lening aan te vragen of een contract te ondertekenen. Wilt u meer informatie over identiteitsfraude? Of denkt u het slachtoffer te zijn van identiteitsfraude? Dan kunt u ook terecht bij het Centraal Meldpunt Identiteitsfraude (CMI) van de Rijksoverheid.

- Wees alert op het ontvangen van valse facturen. Cybercriminelen kunnen misbruik maken van de situatie door valse facturen te sturen die van ons lijken te komen. Controleer daarom altijd zorgvuldig de herkomst en juistheid van ontvangen facturen voordat u overgaat tot betaling. Neem bij twijfel altijd contact met ons op.

Meer informatie

Wij betreuren dit incident zeer en doen ons uiterste best om u zo goed en zorgvuldig mogelijk te informeren. Daarbij zijn wij afhankelijk van de informatie die wij ontvangen van ChipSoft, omdat het incident zich bij hen heeft voorgedaan.

Op onze website vindt u de actuele informatie over dit onderwerp. Hier vindt u ook de antwoorden op een aantal veelgestelde vragen.

Heeft u vragen of zorgen? Neem gerust contact met ons op per mail via patient@roessingh.nl.

Met vriendelijke groet,
Roessingh, Centrum voor Revalidatie