17 april 2026

Onderwerp: belangrijke informatie over ransomware-aanval: uw gegevens zijn ontvreemd.

Geachte heer/ mevrouw,

Wij hebben een belangrijke mededeling over een cyberaanval door criminelen bij Chipsoft, de leverancier van ons patiëntregistratiesysteem HIX.

Uw gegevens zijn ontvreemd door cybercriminelen

Op 7 april 2026 heeft de leverancier van ons EPD-systeem ChipSoft ontdekt dat er afwijkingen waren in het online patiëntregistratiesysteem dat ook onze zorginstelling gebruikt. Na onderzoek stelden zij vast dat dit ging om een ransomeware-aanval.

Samen met ChipSoft hebben wij direct maatregelen getroffen en zijn de verbindingen met ChipSoft verbroken om de impact van het incident te beperken en de veiligheid van patiënt- en medewerkersgegevens zo goed mogelijk te waarborgen. Helaas hebben de cybercriminelen toegang gekregen tot uw gegevens in het patiëntdossier. Vervolgens hebben zij gegevens ontvreemd. Het is op dit moment nog onduidelijk om welke persoonsgegevens het gaat.

Wat betekent dit voor u?

Criminelen kunnen misbruik proberen te maken van deze gegevens. Bijvoorbeeld door oplichting. Mogelijke risico's voor u zijn onder meer:

• Phishing: u ontvangt e-mails, sms-berichten of telefoontjes die betrouwbaar lijken (bijv. van onze instelling of uw behandelend arts). Omdat de criminelen uw gegevens hebben, kunnen zij de e-mail heel persoonlijk maken. Daardoor lijkt de e-mail betrouwbaar. U krijgt bijvoorbeeld de vraag om op een link te klikken. Als u dit doet, kunt u opgelicht worden.

• Criminelen kunnen u ook bellen. De crimineel doet zich dan bijvoorbeeld voor als een medewerker van onze instelling of als een familielid. Krijgt u de vraag om wachtwoorden te noemen of iets te downloaden op uw computer? Doe dat niet. U kunt worden opgelicht. Check daarom eerst bij onze instelling of uw familielid, of die u écht heeft gebeld.

• Identiteitsfraude: een crimineel kan misbruik van uw persoonsgegevens maken door zich voor te doen als u.

• Gerichte fraude: berichten die inspelen op uw medische situatie.

• Openbaarmaking van uw medische informatie, wat kan leiden tot discriminatie of reputatieschade.

• Social engineering: pogingen om extra informatie van u te verkrijgen door vertrouwen op te wekken. Dat doet de crimineel door gebruik te maken van de gelekte informatie.

Wat kunt u doen om risico's te voorkomen?

Let de komende tijd goed op en klik niet zomaar op links in e-mails, sms'jes en appjes. U kunt een verdachte e-mail, sms of app soms herkennen aan typfouten en onbekende afzenders. Controleer het telefoonnummer. Of wat er na het '@'-teken van een e-mailadres staat. Als het bericht een link naar een website betreft, kunt u beter zelf naar de website surfen in plaats van op de link te klikken. Krijgt u een telefoontje? Het kan zijn dat er echt een medewerker van onze instelling of een ander bedrijf belt. Geef nooit iemand uw wachtwoord of pincode.

Wij geven u de volgende adviezen mee:

• Wees extra alert op onverwachte e-mails, sms-berichten of telefoontjes.

• Klik niet op links en open geen bijlagen als u de afzender niet volledig vertrouwt.

• Deel geen persoonlijke of medische gegevens via e-mail of telefoon zonder dat u nagaat of u te maken hebt met een betrouwbare partij.

• Neem bij twijfel rechtstreeks contact op met onze organisatie via 0495-593386

• Controleer regelmatig uw bankafschriften en meld verdachte transacties direct bij uw bank.

Meer informatie

Zie voor meer informatie over identiteitsfraude en hoe dat tegen te gaan, de onderstaande twee websites. Hiernaar verwijzen wij op advies van de Autoriteit Persoonsgegevens:

• https://www.politie.nl/onderwerpen/identiteitsfraude.html

• https://www.rijksoverheid.nl/onderwerpen/identiteitsfraude

Onze rol als uw zorginstelling

Wij zijn ook erg geschrokken en vinden het vreselijk dat dit gebeurd is. Wij werken nauw samen met alle betrokken partijen zoals ChipSoft om de impact te beperken. Uit voorzorg blijven ons Zorgportaal, HIX uitgeschakeld, totdat we weten dat we deze weer veilig kunnen activeren. De patiëntenzorg loopt wel door en zorgverleners kunnen met HIX werken. Als patiënt kunt u alleen tijdelijk niet in uw zorgportaal. Gespecialiseerde externe cybersecurity-experts en onze leverancier

Chipsoft zijn als vanzelfsprekend ook hard bezig met deskundig (forensisch) onderzoek. Deze experts blijven ook nauwlettend monitoren hoe de situatie zich verder ontwikkelt. Ook hebben wij als zorginstelling het datalek gemeld bij de Autoriteit Persoonsgegevens (AP).

Uw rechten

Als patiënt heeft u privacyrechten, zoals inzage en correctie van persoonsgegevens die wij voor u verwerken. Ook kunt u zelf een klacht indienen bij de AP. Voor meer informatie verwijzen wij naar de website van de AP: https://www.autoriteitpersoonsgegevens.nl/.

Meer informatie

Heeft u vragen of zorgen? Neem gerust contact met ons op via:

• telefoon: 0495-593386

• e-mail: mcsoerendonk@ezorg.nl

Met vriendelijke groet,

L. Klinkers en A. Govaert

Huisartsen Medisch Centrum Soerendonk