Beste patïent,

Wij informeren u over een situatie die mogelijk uw medische en persoonsgegevens raakt. We begrijpen dat dit vragen of zorgen kan oproepen. Daarom leggen we u zo duidelijk mogelijk uit wat er is gebeurd, wat dit voor u betekent en wat u zelf kunt doen.

Wat is er gebeurd?

Onze praktijk werkt met een computersysteem van ChipSoft voor het bijhouden van patiëntendossiers. Dit systeem is getroffen door een cyberaanval (ransomware).

De aanval is ontdekt op 7 april 2026. Daarbij hebben onbevoegden toegang gekregen tot gegevens uit patiëntdossiers en mogelijk gegevens in kunnen zien en kunnen kopiëren.

Het is op dit moment nog niet met zekerheid vast te stellen of *uw* gegevens daadwerkelijk zijn ingezien. Wel is het zeer waarschijnlijk dat uw gegevens betrokken zijn. Het kan daarbij gaan om contactgegevens en medische gegevens. Zodra hierover duidelijkheid is informeren we u verder.

Wat betekent dit voor u?

We begrijpen dat dit vervelend en onrustig kan zijn. Uw vertrouwen is voor ons van groot belang. Uw zorg en behandeling gaan gewoon door zoals u gewend bent. In sommige gevallen proberen criminelen misbruik te maken van gegevens, bijvoorbeeld door:

- *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 zelf doen?

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. We adviseren u om de komende tijd extra alert te zijn:

- *Wees voorzichtig met onverwachte berichten of telefoontjes*
- *Klik niet zomaar op links en open geen bijlagen die u niet vertrouwt*
- *Deel geen persoonlijke of medische gegevens als u twijfelt*
- *Neem bij twijfel contact op met onze praktijk*
- *Controleer regelmatig uw bankafschriften en meld verdachte transacties direct bij uw bank.*

Twijfelt u? Neem gerust contact met ons op. We kijken met u mee.

Wat doen wij?

Wij hebben direct maatregelen genomen en werken samen met ChipSoft, cybersecurity-experts en andere betrokken partijen om:

- *de impact van het incident te onderzoeken*

- *de veiligheid van onze systemen te waarborgen*
- *vast te stellen welke gegevens mogelijk zijn geraakt*

Daarnaast hebben wij het datalek gemeld bij de Autoriteit Persoonsgegevens. Zodra er nieuwe informatie beschikbaar is die voor u relevant is, informeren wij u opnieuw.

Uw privacyrechten

U heeft op grond van de privacywetgeving (AVG) verschillende rechten, zoals het recht op inzage en correctie van uw persoonsgegevens. U kunt ook een klacht indienen bij de Autoriteit Persoonsgegevens.

Uw huisarts blijft uw aanspreekpunt

Als uw huisartsen kennen we u en uw situatie. Dat verandert niet. Juist in dit soort situaties vinden wij het belangrijk dat u weet dat u bij ons terechtkunt met vragen of zorgen.

Meer informatie of vragen?

Heeft u vragen of maakt u zich zorgen? Voor algemene vragen over de ransomware-aanval is door onze leverancier ChipSoft een servicelijn ingericht. Op werkdagen van 09:00 tot 17:00 uur kunt u bellen naar telefoonnummer 088-1236122.

Of neem contact op met de praktijk:
· e-mail: info.praktijkspencer@ezorg.nl
· telefoon: 072-5091288
· website van de praktijk: https://huisartsenpraktijkspencer.nl/. Voor het laatste nieuws klikt u op de zin "**Klik hier voor meer informatie**" in de paarse balk op de voorpagina van de website.

Meer algemene informatie over veilig omgaan met gegevens vindt u op:

- www.politie.nl (identiteitsfraude)
- www.rijksoverheid.nl

Wij betreuren dit incident zeer en doen ons uiterste best om u zo goed en zorgvuldig mogelijk te informeren via de bovengenoemde kanalen. Om u in de toekomst sneller te kunnen informeren, willen wij graag nagaan of uw juiste e-mailadres bij ons bekend is. Daarom verzoeken wij u vriendelijk om uw e-mailadres aan ons door te geven. U kunt dit doen door een e-mail te sturen naar info.praktijkspencer@ezorg.nl.

Met vriendelijke groet,

Caroline Spencer, huisarts