Geachte patiënt,

Wij vinden het zeer vervelend u te moeten melden dat het huisartseninformatiesysteem (HiX voor huisartsen), dat wij in 2021 zorgvuldig hebben gekozen vanwege de hoge veiligheidseisen, betrokken is geraakt bij een cyberaanval door criminelen.

Ondanks de uitgebreide en gecertificeerde beveiliging van het Electronisch-Patienten-Dossier-systeem (EPD-systeem) moeten we er, op basis van het nog lopende onderzoek bij ChipSoft, van uit gaan dat toegang is verkregen tot gegevens uit het patiënt-registratiesysteem en uw gegevens mogelijk zijn ontvreemd.

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.

Wat weten we nu?
Op 7 april 2026 heeft de leverancier van ons EPD-systeem ChipSoft ontdekt dat er afwijkingen waren in het online patiënt-registratiesysteem dat ook onze praktijk gebruikt. Na onderzoek stelden zij vast dat dit ging om een ransomeware-aanval. Ransomware (gijzelsoftware) is een vorm van kwaadaardige software (malware) die bestanden, apparaten of complete computernetwerken versleutelt of blokkeert. De aanvallers eisen vervolgens losgeld (ransom) om de toegang tot de gegevens te herstellen. Bij moderne aanvallen dreigen criminelen niet alleen de bestanden versleuteld te houden, maar ook gestolen vertrouwelijke gegevens te publiceren als er niet wordt betaald (dubbele afpersing).

Omdat het onderzoek nog steeds lopende is kunnen de betrokken instanties geen preciezere mededeling doen over wat er in handen van de criminelen is gevallen. Om die reden informeren wij u over de mogelijke risico's, maar kunnen we op dit moment niet aangeven hoe groot deze risico's zijn.

Wat betekent dit voor u?
Criminelen kunnen misbruik proberen te maken van de gegevens die zij in handen hebben gekregen, bijvoorbeeld door oplichting. Hieronder beschrijven wij een aantal voorbeelden van manieren van oplichting. U zult ze herkennen van informatie die ook door overheidsinstellingen en banken regelmatig wordt gegeven over oplichting.

Mogelijke risico's voor u zijn onder meer:
• **Phishing:** u ontvangt e-mails, sms-berichten of telefoontjes die betrouwbaar lijken (bijv. alsof ze van de praktijk afkomstig zijn). 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.** Een persoon doet zich bijvoorbeeld voor als een medewerker van onze praktijk 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 wordt gedaan 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. Twijfelt u, hang dan op, en bel zelf de praktijk op het reguliere nummer terug.
Geef nooit iemand uw wachtwoord of pincode.

De adviezen samengevat:
• Wees extra alert op verdachte 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 uw praktijk.
• 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 huisartsenpraktijk
Wij werken nauw samen met alle betrokken partijen zoals ChipSoft om de impact te beperken. Uit voorzorg blijft het patiëntenportaal 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, en dus online geen afspraken maken, uw dossier niet inzien, en geen herhaalrecepten aanvragen. Voor al deze zaken zult u de praktijk moeten bellen, en eventueel via een terugbelverzoek een aanvraag moeten doen.
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/.

Met vriendelijke groet,

Caroline Spencer, huisarts