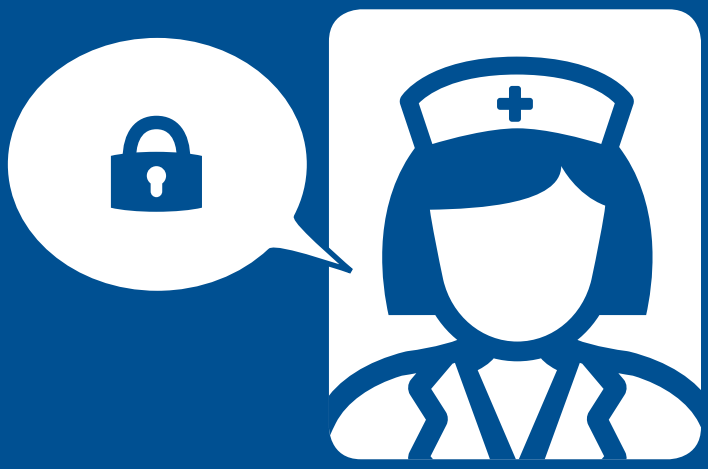
#ditisprivé



Whitepaper

Veiligheid patiëntgegevens in de praktijk

Cijfers, valkuilen en tips

#ditisprivé

Veiligheid patiëntgegevens in de praktijk

Tijdens de koffie patiëntinformatie delen met collega's die niet bij de behandeling betrokken zijn, wel heel voor de hand liggende wachtwoorden gebruiken, privacygevoelige gegevens met de privémail versturen... Bij de melding van datalekken blijkt vaak dat mensen de zwakke schakel zijn. Hoe veilig gaan Nederlandse zorgorganisaties om met patiëntgegevens? En wat zijn daarbij nog aandachtspunten? **Je leest het in deze whitepaper.**

Cijfers, valkuilen en tips

#ditisprivé

De cijfers

5.500 meldingen

van datalekken ontving de Autoriteit Persoonsgegevens in 2016. Daarvan waren 1.594 meldingen afkomstig uit de sector Gezondheid en Welzijn, oftewel 29% van het totaal.

Bronnen: Autoriteit Persoons-gegevens, computable.nl

666 datalekken

werden er in het eerste kwartaal van 2017 door de sector Gezondheid en Welzijn aan de Autoriteit Persoons-gegevens gemeld.

Dat zijn gemiddeld ruim 7 meldingen per dag. Van de 666 meldingen ging meer dan de helft, 55%, over het versturen van persoonsgegevens aan de verkeerde ontvanger. Dat is binnen de zorg dan ook met stip de grootste veroorzaker van datalekken.

Bronnen: Autoriteit Persoons-gegevens, computable.nl

60% lekt onbewust data

Top 5 van meest gemelde datalekken:

1. Persoonsgegevens aan de verkeerde ontvanger verstuurd of afgegeven
2. Overig (dat dit punt op twee staat, zegt wel iets over de verschillende oorzaken van datalekken)
3. Apparaat, gegevensdrager en/of papier kwijtgeraakt of gestolen
4. Brief of postpakket kwijtgeraakt of geopend retour ontvangen
5. Hacking, malware en/of phishing

Bronnen: Autoriteit Persoons-gegevens, computable.nl

#ditisprivé

Zeker **15** Nederlandse ziekenhuizen hebben de afgelopen drie jaar te maken gehad met ransomware-aanvallen

Dat bleek afgelopen juni na een rondgang van de NOS onder 25 ziekenhuizen. Doordat ziekenhuizen bijna dagelijks back-ups maken, ging er maar weinig informatie verloren. Geen van de getroffen ziekenhuizen heeft dan ook losgeld betaald om de 'gegijzelde' bestanden te kunnen ontsleutelen. Wel meldde een van de ziekenhuizen dat ze vanwege een ransomware-aanval een vertraging op een polikliniek hadden.

Bron: NOS

9% van de ziekenhuizen biedt patiënten de mogelijkheid om hun medische dossier in digitale vorm te ontvangen

Opvallend daarbij is dat 4% van de ziekenhuizen daarbij geen methode aanbiedt om die dossiers beveiligd aan te leveren.

Bron: Ulivio

Meer dan de helft van de ziekenhuizen maakt gebruik van standaard wachtwoorden (fabrieksinstellingen) om apparatuur te beveiligen

Dat bleek vorig jaar uit een onderzoek van Deloitte onder 24 ziekenhuizen uit 9 verschillende landen.

Bron: Deloitte

Zo'n **8%** van de zorgprofessionals geeft aan over genoeg digitale vaardigheden te beschikken om over de technologie mee te kunnen denken

Aan de andere kant van het spectrum is er een kleine groep (bijna 4%) die nog moeite heeft met digitale basisvaardigheden.

Bron: Zelftest digitale vaardigheden voor zorgprofessionals

#ditisprivé

Het sterkste wapen tegen datalekken: bewustwording!

Natuurlijk: goede IT-beveiliging is cruciaal. Daar is dan ook veel aandacht voor. Ondertussen blijft een ander risico vaak nog onderbelicht. Namelijk het risico dat zorgorganisaties lopen als niet iedereen zich netjes aan de privacy-regels houdt.

Risico's

Medewerkers weten vaak wel hoe belangrijk het is om zorgvuldig om te gaan met privacygevoelige informatie, maar vervallen in de waan van de dag toch vaak in oude gedragspatronen. Dan delen ze persoonsgegevens met een voor hen vertrouwde organisatie die de patiënt verder kan helpen, maar vergeten ze te checken of de patiënt wel formeel toestemming heeft gegeven voor het delen van die informatie. In de wandelgangen en bij de koffieautomaat zorgt loslippigheid er ook nog regelmatig voor dat patiëntgegevens worden gedeeld met collega's die niet betrokken zijn bij de behandeling. En soms is het een kwestie van verstrooidheid. Dan stuurt een zorgmedewerker bijvoorbeeld tussen de bedrijven door snel een mailtje, om er vervolgens achter te komen dat hij het bericht met patiëntgegevens per ongeluk naar de verkeerde ontvanger heeft verstuurd. Bij de Autoriteit Persoonsgegevens komen dit soort meldingen opvallend vaak binnen.

Cybersecurity was lange tijd voornamelijk het domein van IT'ers. Maar nu de digitalisering steeds dieper in de werkprocessen van zorgprofessionals doordringt, moeten ook zij voortdurend alert zijn op cyberrisico's en voorkomen dat patiëntgegevens in verkeerde handen vallen. Vooral nu blijkt dat de digitale weerbaarheid van Nederland achterblijft bij de groei van de dreigingen. Die waarschuwing is in ieder geval te lezen in het Cybersecuritybeeld Nederland 2017. Overheid, bedrijfsleven en burgers nemen weliswaar veel stappen om hun digitale weerbaarheid te vergroten, maar niet snel genoeg. Aldus het Nationaal Cyber Security Centrum (NCSC).

Hackers worden steeds professioneler en ze breiden hun digitale werkgebied steeds verder uit. Sommigen hebben zich zelfs gespecialiseerd in het beïnvloeden van democratische processen. Daarnaast kunnen ze op het Dark Web voor een prikkie kant-en-klare hackpakketten kopen. Of huren, want die optie is er tegenwoordig ook. Een aanval met ransomware wordt daardoor steeds makkelijker. En die gijzelsoftware wordt ook steeds grootschaliger ingezet. Afgelopen mei was er nog een wereldwijde aanval waarbij onder andere zeven Britse ziekenhuizen werden getroffen. WannaCry zorgde er toen voor dat er volledige afdelingen van die ziekenhuizen stil kwamen te liggen. Zeer verontrustend, vooral omdat het volgens experts niet eens om een gerichte aanval ging, maar eerder om 'een schot hagel'.

Cybercriminelen richten zich in het algemeen juist wel steeds vaker op ziekenhuizen en andere zorginstellingen. De zorgwereld heeft hun speciale interesse omdat de veiligheidsmaatregelen daar nog niet zo geavanceerd zijn als bij de financiële wereld. Bovendien levert de informatie van medische dossiers op het Dark Web beduidend meer op dan creditcardinformatie.

Valkuilen

Informatiebeveiliging is in de eerste plaats de verantwoordelijkheid van zorginstellingen en zorgverleners zelf. Daarbij moeten ze aan Europese en nationale wettelijke voorschriften voldoen. Ondertussen zijn zij wel afhankelijk van derden, zoals leveranciers van medische apparatuur. Hebben die de informatiebeveiliging niet goed op orde? Dan kan dat alsnog tot datalekken leiden. En dat is zeker geen denkbeeldig probleem. Zo verschijnen er regelmatig berichten over medische apparatuur die nog met verouderde Microsoft-software wordt aangestuurd.

#ditisprivé

Zorgprofessionals zijn geen ICT-experts. Hoewel hun digitale vaardigheden snel verbeteren en die vaardigheden ook steeds vaker als eis in vacatures wordt genoemd, is er op dat vlak absoluut nog een grote slag te maken.

De opslag van patiëntgegevens gebeurt nog op diverse manieren. Er was weliswaar een voorstel om een elektronisch patiëntendossier (EPD) in te voeren, maar dat initiatief is in 2011 vanwege privacyredenen stopgezet. Sindsdien wordt er wel aan regionale EPD's gewerkt. Ook is er het Landelijk Schakel Punt (LSP) dat huisartsen, apotheken en medisch specialisten in staat stelt om medische gegevens met andere zorgverleners te delen zodat zij een patiënt snel, goed en veilig kunnen helpen. Maar dat delen mag alleen als de patiënt daar toestemming voor heeft gegeven. Er is momenteel dus nog geen centrale database waar alle patiëntgegevens in zijn opgeslagen. Daardoor is het ook niet mogelijk om al die gegevens op een eenduidige manier te beveiligen.

Door de inzet van sensoren worden er steeds meer gezondheidsdata verzameld en gebruikt, maar voor die ontwikkeling is er nog geen gezamenlijke strategie. Ook is nog onduidelijk waar de verantwoordelijkheid ligt en welke rol patiënten, artsen, verzekeraars, overheid en ICT-partijen hebben. Dat is in ieder geval de conclusie die ECP (platform voor de informatiesamenleving) eind vorig jaar trok in het visiedocument 'De zorgzame informatiesamenleving'.

Tips

De coalitie 'Digivaardig in de zorg'* heeft enkele initiatieven gelanceerd:

- **Zelftest digitale vaardigheden:** een gratis online test die zorgprofessionals inzicht geeft in hun digitale vaardigheden. Na het invullen van de test verschijnt de feedback meteen op het scherm. De zelftest is een gevalideerd en genormeerd wetenschappelijk meetinstrument. Met andere woorden: het gaat hier om een test die op een betrouwbare manier aangeeft in hoeverre iemand zich in de digitale wereld weet te redden.
- **Emailcursus 'slimmerwerkenindezorgin1minuut':** na aanmelding ontvangt de zorgprofessional vijf cases in zijn mailbox. In een minuut tijd wordt een onderwerp behandeld, waaronder internetveiligheid. Aanmelden kan via www.slimmerwerkenindezorgin1minuut.nl.

* *'Digivaardig in de zorg' heeft als doel om de digitale competenties te vergroten van mensen die in de zorg werken. Bij dit initiatief van ECP (platform voor de informatiesamenleving) zijn inmiddels al flink wat partners aangehaakt, zoals V&VN (verpleegkundigen), Actiz (koepel zorginstellingen), Nictiz (expertise e-health en standaardisatie), ZiN (ZorginstituutNederland), OIZ (ICT-ers in de zorg) en hogescholen HAN (Arnhem Nijmegen) en HH (Den Haag).*

Z-CERT is een eerder dit jaar opgerichte sectorale CERT voor de zorg. CERT staat voor Computer Emergency Response Team, en de Z geeft aan dat dit team zich specifiek op zorginstellingen richt. Het is een stichting die aangesloten zorginstellingen helpt met het vergroten van de cybersecurity en die ondersteuning biedt als er incidenten zijn. Kennisdeling is daarbij ook een belangrijk aandachtspunt. Z-CERT werkt nauw samen met andere CERT's, waaronder het Nationaal Cyber Security Centrum (NCSC). Op dit moment kunnen ziekenhuizen en GGZ-instellingen zich als deelnemer aanmelden. In de toekomst zal Z-CERT ook diensten aan andere zorgverleners aanbieden. Zie ook: www.z-cert.nl.

De nieuwe privacywetgeving die vanaf 25 mei 2018 wordt ingevoerd, zet iedereen ook op scherp. In de aanloop naar die Algemene verordening gegevensbescherming (AVG) hebben veel bedrijven en organisaties al duidelijk in beeld welke risico's ze lopen en welke maatregelen ze nog moeten nemen om aan de nieuwe wet te kunnen voldoen. Het onderwerp staat dus al hoog op de agenda, maar voor veel partijen zal het nog wel een uitdaging worden om op tijd de juiste acties te nemen. Voor meer verdieping kunnen zij terecht op de website van Autoriteit Persoonsgegevens.

#ditisprivé

10 TIPS Zo ga je in de dagelijkse praktijk veilig met patiëntgegevens om

1 Papieren of digitale post met privacygevoelige persoonsgegevens...

... altijd aangetekend of via je zakelijke emailadres versturen.
... alleen versturen naar partijen die officieel toestemming hebben om die gegevens in te zien.
... altijd even extra controleren voordat je het verstuurt. Check en dubbelcheck vooral het post- of emailadres van de ontvanger(s). Maak daar echt een gewoonte van. Want nogmaals: verkeerd geadresseerde post en e-mails zijn nog altijd de grootste veroorzakers van datalekken.

2 Wachtwoorden...

... op zo'n manier samenstellen dat het voor anderen onmogelijk is om ze te raden. Lijkt een inkoppertje, maar het gebeurt nog heel vaak dat wachtwoorden kinderlijk eenvoudig te kraken zijn.
... goed beschermen. Bijvoorbeeld met een wachtwoord-manager, zoals 1Password, True Key of Lastpass. Schrijf wachtwoorden niet op. Al helemaal niet op een Post-it die op het beeldscherm of in de buurt van de computer hangt.

3 Documentenbeheer...

... samen met IT optimaliseren en daarbij gebruikmaken van encryptiemethoden zodat documenten alleen via een wachtwoord toegankelijk zijn.
... onderling goed afstemmen, die afspraken vastleggen en binnen het team verspreiden
... regelmatig onder de aandacht brengen.
... bewaken, dus ook aan de bel trekken als een collega zich niet aan de afspraken houdt.
... gaat uiteraard ook over papieren documenten. Zorg dus voor afsluitbare archiefkasten en papiervernietiging.
... blijven monitoren, want er kunnen altijd nieuwe situaties ontstaan waarbij privacygevoelige informatie in verkeerde handen kan vallen.

4 Computers...

... op zo'n manier plaatsen dat mensen niet over je schouder of via het raam op jouw beeldscherm kunnen meekijken.
... altijd uitloggen en afschermen met een lastig te raden inlogcode. Als je van je plek bent, moet niet iedereen toegang tot je computer kunnen krijgen.
... moeten uiteraard up-do-date zijn. Installeer veiligheidsupdates dus zo snel mogelijk.
... kunnen ondanks allerlei voorzorgsmaatregelen toch geïnfecteerd worden met malware. Sla dan ook direct bij de IT-afdeling alarm als je iets verdachts ziet.

5 usb-sticks en laptops...

... kunnen in verkeerde handen vallen. Zet er dus nooit privacygevoelige gegevens en/of identiteitsinformatie op. Gebruik hiervoor altijd je zakelijke computer die op de juiste manier beveiligd is.

6 Openbare wi-fi-netwerken...

... vermijden! Er bestaat namelijk altijd een kans dat een hacker toegang tot je computer probeert te krijgen. Maak altijd gebruik van beveiligde netwerken die zijn voorzien van een beveiligingssleutel met inlogcode.

#ditisprivé

10 TIPS

7 Bsn-nummer nodig?...

... Schrijf dan alleen dat nummer op. Alleen in uitzonderlijke gevallen mag er een scan worden gemaakt van iemands identiteitsbewijs, bijvoorbeeld als dat expliciet in de wet staat.

8 Delen van informatie...

... mag alleen als het in lijn is met de professionele beroepscodes en de specifieke regels die gelden voor het delen van patiënt-specifieke informatie.

... kan pas als ook de patiënt daar expliciet toestemming voor geeft. Leg die toestemming schriftelijk vast en geef de patiënt daarbij de mogelijkheid om die toestemming desgewenst ook weer in te trekken.

... mag alleen via de officiële en goed beveiligde kanalen. Gebruik voor het werk dus geen social media of je privé-mail.

... doe je tijdens overleggen in een afgesloten ruimte. Deel informatie over cliënten niet tijdens een praatje met een collega in de wandelgang of een open kantoortuin.

9 Externe partijen...

... dienen zich uiteraard ook aan al jullie privacyregels te houden: zorg er bij het uitbesteden van werkzaamheden dus voor dat ze die regels goed kennen en naleven.

10 Checklist...

... Kijk zelf eens na werktijd wat je op de werkplekken aantreft. Zijn alle computers uit? Zijn computers die aanstaan nog ingelogd? Zijn de kasten op slot en zijn de sleutels niet op de werkplek aanwezig? Hanteer een checklist waar dergelijke vragen op staan en bespreek de resultaten in het werkoverleg.

Bron: Privacy8, Autoriteit Persoonsgegevens

#ditisprivé

Meer weten?
medireva.nl/ditisprive

MediReva