OLVG krijgt forse boete AP na privacy-overtreding

11 februari 2021

In 2018 bleek dat werkstudenten van het OLVG heel eenvoudig toegang hadden tot elektronische patiëntgegevens in het EPD van het ziekenhuis. Verkeerd afgestelde software was er volgens het OLVG de oorzaak van dat werkstudenten alle medische dossiers konden inzien. Het profiel van deze werkstudenten, die snel moesten kunnen schakelen tussen afdelingen, stond onbedoeld zo ingesteld dat zij patiënten van álle specialismen konden opzoeken. Het OLVG heeft in 2018 en 2019 een reeks maatregelen ingevoerd om de privacy van patiënten beter te beschermen.

OLVG teleurgesteld over privacy-boete

OLVG-bestuursvoorzitter Maurice van den Bosch reageert teleurgesteld op het boetebesluit. “Het is goed dat we in Nederland een toezichthouder hebben voor privacy en gegevensbescherming. Gegevens in een ziekenhuis moeten veilig en beschermd zijn. We hadden niet alles goed op orde. We zijn echter teleurgesteld dat we niet de kans hebben gekregen om eerst de geconstateerde tekortkomingen op te lossen, alvorens een boete opgelegd te krijgen.”

Ook vindt Van den Bosch de boete voor een maatschappelijke instelling zoals een ziekenhuis wel erg hoog. “Dat is geld dat we nu niet kunnen besteden aan datgene waar ons geld het

hardste nodig is: voor de zorg voor onze patiënten.” Het ziekenhuis gaat volgens de AP echter niet in bezwaar of beroep tegen de boete van de toezichthouder.

AP: ernstige fout

AP-vicevoorzitter Monique Verdier vindt de boete terecht. Ze benadrukt dat mensen erop moeten kunnen vertrouwen dat hun medische gegevens veilig zijn. “Je moet er toch niet aan denken dat mensen, die daar helemaal niets te zoeken hebben, zomaar in de aantekeningen van de dokter over jou en jouw ziekte kunnen rondneuzen. Patiënten moeten ervan uit kunnen gaan dat medewerkers alleen medische dossiers inzien als dat nodig is voor hun behandeling. Het OLVG nam te weinig beveiligingsmaatregelen om dit te waarborgen. Dat is ernstig en daarom legt de AP het OLVG nu deze boete op.”

Naast medische gegevens bevatten de dossiers informatie als burgerservicenummers, adressen en telefoonnummers. Ook die gegevens moeten goed beschermd zijn, vanwege de risico’s op bijvoorbeeld identiteitsfraude en phishing.

Twee privacy-overtredingen

De AP begon in 2018 met een onderzoek na een tip van een bezorgde burger, signalen uit de media en twee datalekmeldingen van het OLVG, over werkstudenten en andere medewerkers die medische dossiers inzagen zonder dat dit nodig was voor hun werk. De AP concludeerde na haar onderzoek dat het OLVG structureel niet goed omging met de toegang tot medische dossiers. Er waren twee overtredingen:

1. Het ziekenhuis moet bijhouden en regelmatig controleren wie welk dossier raadpleegt. Zo kan het ziekenhuis tijdig signaleren wanneer iemand een dossier raadpleegt terwijl dat niet mag en daartegen maatregelen nemen. Het OLVG hield wel automatisch bij welke medewerker wanneer welk medisch dossier inzag (logging), maar controleerde die logging niet vaak genoeg op onbevoegde toegang.
2. Bij een goede beveiliging hoort authenticatie met ten minste twee factoren. De identiteit van een gebruiker om toegang te krijgen tot een patiëntendossier wordt dan bijvoorbeeld vastgesteld met een code of een wachtwoord in combinatie met een personeelspas. Het OLVG maakte in het ziekenhuis geen gebruik van deze tweefactor-authenticatie. Inloggen buiten het ziekenhuis ging wel via tweefactor-authenticatie.

Juist in de zorg, waar de gevoeligste persoonsgegevens in de systemen staan, ziet de AP veel datalekken: de afgelopen jaren staat de zorg altijd in de top 3 van sectoren met de meeste datalekken.

AP-vicevoorzitter Verdier hierover: “Terwijl de bescherming van patiëntgegevens cruciaal is. Patiënten delen veel gegevens met zorginstellingen en dat is ook nodig, de laatste tijd door de coronacrisis misschien wel meer dan ooit. Mensen moeten er dan wel op kunnen vertrouwen dat hun gegevens veilig zijn. Wij roepen ziekenhuizen en andere zorginstellingen dan ook op heel goed na te gaan hoe zij de bescherming van de gegevens van patiënten geregeld hebben en deze te verbeteren waar nodig.’

Verbeteringen doorgevoerd

Tijdens het onderzoek van de AP heeft het OLVG verbeteringen doorgevoerd:

- Het OLVG controleert met grotere regelmaat wie welk dossier raadpleegt. Daarbij ziet het ziekenhuis er strikter op toe of inzage ook wordt gedaan door een medewerker die hier bevoegd voor is. In de meeste gevallen is een logische, legitieme reden voor inzage door de zorgverlener. In een enkel geval is een inzage onbevoegd. Wanneer hier sprake van is, leidt dit tot arbeidsrechtelijke sancties.
- Er is extra beveiliging om in te kunnen loggen, de zogenaamde tweefactor-authenticatie. Dit betekent dat toegang tot een dossier via een wachtwoord gaat en daarnaast met een scan van de personeelspas of met behulp van een identificatietoken. NB. Inloggen buiten OLVG ging al wel op deze manier.
- Naast deze technische maatregelen geeft OLVG extra aandacht voor privacy en het omgaan met gevoelige informatie. Zo is er voor alle medewerkers een verplichte e-learning en wijst de instelling nieuwe medewerkers actief op privacybescherming in het introductieprogramma.

Haga en Barbie

Begin 2018 was er een vergelijkbare geruchtmakende privacy-zaak in de zorgsector, in het Haagse Haga Ziekenhuis. De AP stelde toen onderzoek in naar of er ongeoorloofd door medewerkers van het ziekenhuis is gekeken in het medisch dossier van reality-ster Samantha de Jong (Barbie). Zij werd in januari in het ziekenhuis opgenomen. Ook het HagaZiekenhuis voerde daarna een reeks (deels technische) maatregelen door om herhaling te voorkomen. De AP legde het Haagse ziekenhuis voor de onvoldoende beveiliging in juli 2019 een boete op van 460.000 euro.