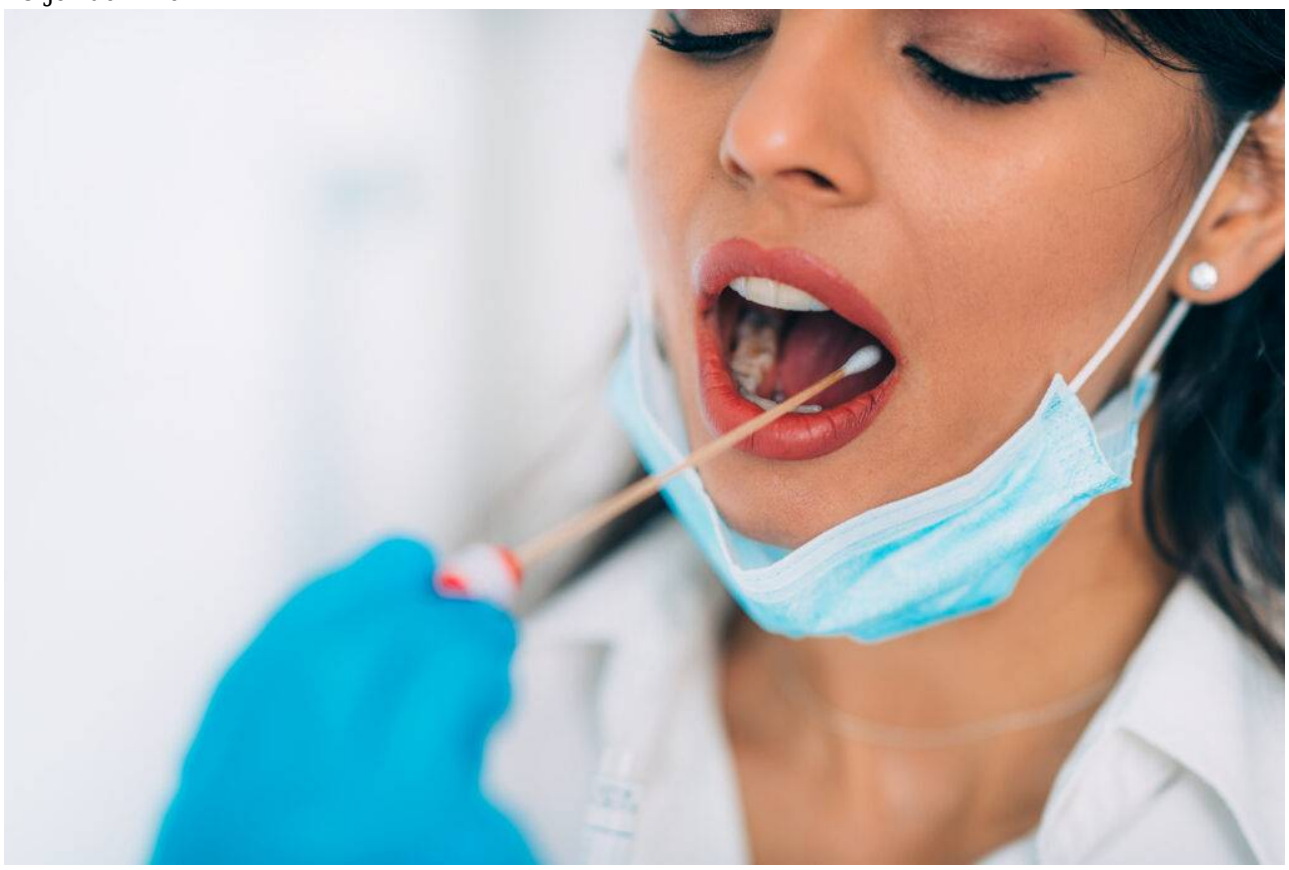
AP stelt GGD onder verscherpt toezicht na datalek

29 januari 2021



De AP stelde woensdag 27 januari dat het direct opheldering heeft geëist bij de GGD. De privacytoezichthouder liet ook weten dat de GGD burgers goed en snel moeten informeren over de diefstal, onder meer via de website en door een informatielijn open te stellen. De AP was op woensdag slecht bereikbaar door wat het 'vele telefoontjes' noemde van ongeruste mensen. Bij de gelekte gegevens gaat het om adressen, telefoonnummers, burgerservicenummers en testresultaten.

De AP heeft de GGD laten weten dat zij mensen goed moeten informeren over de diefstal. Onder meer via de website en door een informatielijn open te stellen. Mensen die de AP bellen voor informatie, zijn doorverwezen naar de GGD. De AP gaat pas met een klacht aan de slag als die eerst schriftelijk is ingediend bij de GGD zelf en het bewijs hiervan bij de AP is aangeleverd. Volgens de GGD-GHOR loopt er momenteel een politieonderzoek naar de datadiefstal.

Beveiliging gegevens topprioriteit

De AP heeft de overheid en de zorgsector, in de afgelopen jaren al regelmatig gewaarschuwd dat beveiliging van medische gegevens aan de hoogste eisen moet voldoen. Deze datadiefstal laat vlgens de AP weer zien hoe belangrijk gegevensbescherming is. 'Iedere organisatie – niet alleen de overheid – moet de beveiliging van persoonsgegevens als topprioriteit aanmerken', schrijft de toezichthouder. 'Hoe meer je doet met data, hoe groter de risico's zijn. En hoe hoger

het niveau van gegevensbescherming daarom moet zijn.’

Aleid Wolfsen, voorzitter van de AP, stelt dat medische gegevens, adres, telefoonnummer en BSN heel geschikt zijn voor bijvoorbeeld identiteitsfraude en phishing. “De beveiliging moet daarom aan de hoogste eisen voldoen. Doe je dat onvoldoende, dan ben je nalatig en kun je aansprakelijk gesteld worden. Je riskeert dan niet alleen een boete van de AP, maar mogelijk ook claims van slachtoffers.”

Bij het testen en bron- en contactonderzoek (BCO) zijn veel mensen betrokken. Dan juist moet je je gegevens extra goed beveiligen, stelt de AP. En checken of medewerkers niet meer gegevens opvragen dan noodzakelijk of complete datasets downloaden. Het is belangrijk om persoonsgegevens goed te beveiligen en ervoor te zorgen dat niet iedereen overal bij kan. Loggen en dit goed blijven monitoren zijn daarbij essentieel.

Steekproefsgewijze controle GGD

RTL Nieuws meldde echter dat het zeer eenvoudig was om gegevens via een pdf te downloaden en te delen. Ook werd er volgens de GGD in eerste slechts steekproefsgewijs gecontroleerd. Pas sinds eind maart gebeurt dit continu. Minister De Jonge had eerder aangegeven dat vanaf het begin van het testen door de GGD al continue gecontroleerd werd op het gebruik van de systemen.

In september berichtte Nieuwsuur dat de gegevens van geteste Nederlanders toegankelijk waren voor duizenden medewerkers van de coronatestlijn, ongeacht of ze daar wel of niet bij zouden mogen volgens de wet. Verder bleek dat medewerkers via WhatsApp privégegevens van geteste mensen, onder wie bekende Nederlanders, met elkaar deelden. Inmiddels is dit volgens de GGD vergaand beperkt, maar BCO-medewerkers zouden Nieuwsuur gemeld hebben dat zij nog altijd toegang hebben tot alle gegevens.

Stoppen met HPZone

GGD-GHOR, waar alle 23 regionale GGD’s onder vallen, zou inmiddels van plan zijn om te stoppen met een van de twee omstreden IT-systemen. Het gaat om HPZone, een elektronisch dossier dat de GGD’en gebruiken om het bron- en contactonderzoek uit te voeren. Als iemand een positieve testuitslag heeft en deze gemeld wordt bij de GGD, dan wordt een dossier van deze persoon in HPZone aangemaakt.

Het andere systeem is CoronIT. Dit is het administratiesysteem voor het test- en vaccinatieproces en de communicatie hierover. Van wie een afspraak maakt voor een coronatest via het callcenter, de coronatest website of een arts, komen persoonsgegevens terecht in CoronIT. Dat geldt ook voor een afspraak voor een vaccinatie.