Inspectie Gezondheidszorg en Jeugd
Ministerie van Volksgezondheid, Welzijn en Sport

> Retouradres Postbus 2115 3500 GC Utrecht

Clinical Diagnostics NMDL B.V. en LCPL B.V.
[redacted]

Bezoekadres
Stadsplateau 1
3521 AZ Utrecht
Postbus 2115
3500 GC Utrecht
T 088 120 5000
www.igj.nl

Inlichtingen bij
[redacted]

Ons kenmerk
[redacted]

Datum 8 april 2026
Betreft Definitief briefrapport Inspectie Gezondheidszorg en Jeugd

Geachte [redacted]

Op 16 december 2025 bracht de Inspectie Gezondheidszorg en Jeugd (IGJ), als onderdeel van ons onderzoek, een aangekondigd bezoek aan Clinical Diagnostics LCPL B.V. en Clinical Diagnostics NMDL B.V. op het Kesslerpark te Rijswijk.
De aanleiding van dit bezoek was het informatiebeveiligingsincident dat begin juli 2025 in uw organisatie plaatsvond. Voorafgaand aan en na afloop van het bezoek leverde u ons, op ons verzoek, ook schriftelijk informatie aan. In dit briefrapport beschrijven wij onze bevindingen op basis van alle door u verstrekte informatie.

Aanleiding onderzoek
Begin augustus 2025 heeft de IGJ kennis genomen van een informatiebeveiligingsincident bij Clinical Diagnostics LCPL B.V. en Clinical Diagnostics NMDL B.V. te Rijswijk. Dit incident vond begin juli 2025 plaats en heeft een datalek tot gevolg gehad. Bij dit incident was een grote hoeveelheid zeer gevoelige persoonsgegevens betrokken. Deze gegevens waren onder meer afkomstig van deelnemers aan het bevolkingsonderzoek naar baarmoederhalskanker, dat wordt uitgevoerd door Bevolkingsonderzoek Nederland (BVO NL). Naast de gegevens van BVO NL waren ook gegevens van andere zorgaanbieders betrokken. De IGJ heeft naar aanleiding van deze gebeurtenis een onderzoek gestart.

Doel en aanpak onderzoek
Doel van het onderzoek was inzicht te krijgen in de status van informatiebeveiliging van de getroffen bedrijfsonderdelen van Clinical Diagnostics, zowel op het moment van het informatiebeveiligingsincident als ten tijde van het inspectiebezoek. De IGJ onderzocht of Clinical Diagnostics voldeed aan de norm voor informatiebeveiliging in de zorg, NEN 7510. Tijdens het bezoek wilde de inspectie ook een beeld krijgen van de samenwerking van Clinical Diagnostics met andere partijen in het kader van diagnostiek en het leveren van zorg.

Het onderzoek van de IGJ vond plaats in de periode september 2025 tot maart 2026. In dit onderzoek stelden we schriftelijk vragen en brachten we een aangekondigd inspectiebezoek. Nadat het informatiebeveiligingsincident bij ons bekend werd, stelden we u hierover op 11 september, 29 september en 17 oktober 2025 schriftelijk vragen. Deze beantwoordde u respectievelijk op 3, 13

en 24 oktober 2025. Tijdens het inspectiebezoek van 16 december 2025 vroegen we u onder meer een aantal van deze antwoorden verder toe te lichten. Omdat u tijdens het bezoek niet alle informatie voorhanden had, hebben we u de gelegenheid gegeven om aanvullende informatie toe te sturen. Op 5 februari 2026 leverde u deze informatie schriftelijk aan. Dit rapport is gebaseerd op alle door de inspectie verzamelde informatie.

Juridisch kader Inspectie Gezondheidszorg en Jeugd
De inspectie is belast met het toezicht op de artikelen 4 tot en met 12, 15d, 15e en 15j van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz)[1]. De verplichting te voldoen aan de NEN 7510 blijkt daarnaast uit de Regeling Gebruik Burgerservicenummer in de zorg en het Besluit elektronische gegevensverwerking door zorgaanbieders.

Gesprekspartners
Tijdens het bezoek op 16 december 2025 heeft de inspectie met verschillende betrokkenen gesproken. Dit zijn personen in de volgende rollen:
- Directeur-bestuurder;
- Functionaris Gegevensbescherming;
- IT-infrastructuur specialist;
- IT-architect;
- Leden van het externe advocatenteam.

Bevindingen toezicht
De inspectie heeft onder meer gekeken naar:
1. Organisatorische aspecten van Clinical Diagnostics;
2. Het informatiebeveiligingsincident;
3. Informatiebeveiliging ten tijde van het incident;
4. Informatiebeveiliging in de toekomst.

Hieronder beschrijven wij per onderwerp onze bevindingen.

1 Organisatorische aspecten
Clinical Diagnostics Netherlands Holding B.V. (Clinical Diagnostics Nederland) is onderdeel van Eurofins.

Clinical Diagnostics NMDL BV. (NMDL) en LCPL BV. (LCPL) zijn twee van de zes werkmaatschappijen die onderdeel zijn van Clinical Diagnostics Nederland. In de functie van directeur-bestuurder bestuurt u vijf van de zes werkmaatschappijen, waaronder NMDL en LCPL. Op het moment van het inspectiebezoek, op 16 december 2025, bekleedde u deze functie ongeveer een jaar. U stuurt de activiteiten van Clinical Diagnostics Nederland samen met een managementteam aan. In dit team is één IT-directeur. Deze is verantwoordelijk voor alle IT-gerelateerde zaken. De IT-medewerkers, waaronder een IT-architect, 3 IT-infrastructuur specialisten, service, solutions en functioneel beheerders zijn werkzaam voor alle Nederlandse entiteiten van Clinical Diagnostics Nederland. Clinical Diagnostics maakt voor monitoring en analyse gebruik van het *Security Operations Center (SOC)* van de internationale Eurofins-organisatie.

[1] wetten.nl - Regeling - Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg - BWBR0023864

Voorafgaand en tijdens het informatiebeveiligingsincident had de organisatie een *Regional Information Security Officer (RISO)*. Tijdens het gesprek van 16 december 2025 vertelde u dat de organisatie na het incident een *Chief Information Security Officer (CISO)* heeft aangesteld. De CISO en de IT-directeur leggen samen aan u verantwoording af over de informatiebeveiliging van alle entiteiten van Clinical Diagnostics. De CISO en de IT-directeur hebben periodiek overleg over rapportages vanuit het SOC met Eurofins. Bij de inrichting van de IT-omgeving en bijbehorende processen wordt gebruik gemaakt van 'key guidance documents'. Dit zijn richtlijnen vanuit de Eurofins moederorganisatie. De lokale IT-afdeling is eindverantwoordelijk en neemt de finale beslissingen. Voor intern toezicht op naleving van de privacywetgeving heeft uw organisatie een externe functionaris gegevensbescherming ingehuurd.

2 Het informatiebeveiligingsincident

Clinical Diagnostics NMDL B.V. en LCPL B.V waren betrokken bij het informatiebeveiligingsincident. Het informatiebeveiligingsincident is door Clinical Diagnostics ontdekt op 6 juli 2025. U vertelde tijdens het inspectiebezoek op 16 december 2025 dat het incident heeft plaatsgevonden in een IT-omgeving die werd overgezet naar een andere omgeving. Het incident vond plaats in een legacy-omgeving die op de planning stond om te worden overgezet naar een centrale omgeving (CTNL). De data in de betreffende omgeving was nog niet overgezet naar de centrale omgeving.

Tijdens het informatiebeveiligingsincident kregen onbevoegden toegang tot gegevens in de legacy-omgeving. Volgens uw eerdere schriftelijke antwoorden van 13 oktober 2025 heeft forensisch onderzoek uitgewezen dat op 3 juli 2025 voor het eerst ongeautoriseerde toegang had plaatsgevonden. De werkzaamheden van NMDL en LCPL konden na een onderbreking op 8 juli 2025 worden hervat. Dit was mogelijk doordat er op korte termijn nieuwe fileservers zijn ingericht waarop op 6 en 7 juli 2025 gescreende back-ups zijn geplaatst. De gevolgen voor de beschikbaarheid van de gegevens zijn volgens u dan ook zeer beperkt geweest. U geeft tevens aan dat niet is gebleken dat de integriteit van de gegevens is beïnvloed. Zoals eerder aangegeven heeft het incident geleid tot een groot datalek.

Oorzaak incident

U vertelde de inspectie tijdens het gesprek van 16 december 2025 dat Clinical Diagnostics door een externe partij onderzoek heeft laten uitvoeren naar de oorzaak van het informatiebeveiligingsincident. Hieruit is gebleken dat een gebruikersaccount is gecompromitteerd. Met dit gebruikersaccount was via een remote desktopconnectie toegang verkregen tot de legacy-omgeving. Er is uitgebreid onderzoek gedaan naar de wijze waarop toegang verkregen zou kunnen zijn tot het account en de betreffende inloggegevens. Het bleek volgens u niet mogelijk om vast te stellen hoe de ongeautoriseerde toegang was verkregen.

De gehele omgeving van Clinical Diagnostics werd gemonitord door het *Security Operations Center (SOC)* van de internationale Eurofins-organisatie. Dit betrof volgens u ook de legacy-omgevingen die nog niet waren overgezet naar de centrale omgeving. De legacy-omgevingen zouden echter door een menselijke fout buiten de scope van de monitoring gekomen zijn. Het SOC verkeerde op basis van onjuiste informatie in de veronderstelling dat de betreffende legacy-omgeving niet langer actief was en heeft de monitoring hiervan uitgeschakeld. Hierdoor werden afwijkende patronen in de logging niet opgemerkt.

U vertelde dat de toegang tot het gecompromitteerde account, toen het informatiebeveiligingsincident plaatsvond, was beveiligd met een wachtwoord van 16 karakters. Op het getroffen account was op dat moment geen Multi Factor Authenticatie (MFA) actief. Op de omgeving waarbinnen het account zich begaf, zou volgens u wel MFA actief zijn geweest. In het verleden zou op het betreffende account volgens u wel MFA actief zijn geweest.

3 Status van informatiebeveiliging
U antwoordde ons op 13 oktober 2025 op schriftelijke vragen dat uw organisatie op dat moment gedeeltelijk aan de NEN 7510 norm voldeed. Eén van de andere Nederlandse Clinical Diagnostics entiteiten (niet zijnde NMDL of LCPL) is NEN 7510-gecertificeerd. In het gesprek van 16 december 2025 vertelde u dat dit het bedrijfsonderdeel SCAL betreft. Dit heeft de inspectie in het landelijk register NEN 7510 geverifieerd.

Tijdens het inspectiebezoek vroegen we u of de entiteiten die getroffen zijn door het informatiebeveiligingsincident, namelijk NMDL en LCPL, ten tijde van het informatiebeveiligingsincident of daarna, aantoonbaar voldeden aan de norm NEN 7510. U gaf aan dat u niet wist of hier in het verleden een audit op had plaatsgevonden. De inspectie gaf u de mogelijkheid om na het inspectiebezoek na te gaan of er eerder een audit was uitgevoerd waarmee u zou kunnen aantonen volgens de norm NEN 7510 te werken. In de op 5 februari 2026 ontvangen stukken gaf u aan dat in de periode 3 jaar voorafgaand aan het informatiebeveiligingsincident geen audit was uitgevoerd op het onderwerp informatiebeveiliging/NEN 7510.

Daarnaast verzocht de inspectie tijdens het gesprek van 16 december 2025 om documentatie over risicoanalyse(s) op het gebied van informatiebeveiliging die voorafgaand aan het informatiebeveiligingsincident zouden zijn uitgevoerd en ook een risicoanalyse daterend van na het informatiebeveiligingsincident. In antwoord op dat verzoek stuurde u op 5 februari 2026 een tweetal documenten[2].
Deze documenten bevatten de uitkomsten van screening van de IT-omgevingen. Met deze screenings houdt Clinical Diagnostics toezicht op het verkeer en gedrag op de digitale omgeving. Hierbij maakt zij gebruik van dashboards en diensten van Eurofins. De toegestuurde dashboards in deze documenten bevatten de data van Clinical Diagnostics Benelux en betroffen de rapportages van juni 2025 en februari 2026.

Tot slot stelden we tijdens het gesprek van 16 december 2025 vragen over de gegevensuitwisseling. Hiermee wilde de inspectie een beeld krijgen van de wijze waarop uw organisatie daar uitvoering aan geeft. U gaf aan dat u gegevens uitwisselt op basis van de afspraken die gemaakt zijn met de samenwerkende partij. Deze afspraken staan volgens u beschreven in de contracten met deze partijen. U heeft aangegeven dat Clinical Diagnostics bepaalt welke gegevens noodzakelijk zijn om haar werkzaamheden op medisch verantwoorde wijze uit te kunnen voeren en daarom welke gegevens door de aanvrager van een onderzoek worden gedeeld. Een aanvrager heeft een bepaalde mate van vrijheid in het bepalen welke gegevens zij aan Clinical Diagnostics toestuurt[3].

[2] 'ITISC06 Information Security Dashboard June 2025.pdf' en 'ITISC06 Information Security Dashboard February 2026.pdf'
[3] Tekst op uw verzoek gewijzigd op 23 april 2026.

Voor de samenwerking met BVO NL is volgens u een uitvoeringskader opgesteld door het RIVM. U gaf aan dit uitvoeringskader te gebruiken en ook gebruik te maken van richtlijnen. Tijdens het inspectiebezoek was het niet duidelijk om welke richtlijnen het ging. Daarom vroeg de inspectie aan u om dit te verduidelijken. Op 5 februari 2026 liet u ons weten dat u gebruik maakt van technische standaarden. Het gebruik van deze standaarden komt volgens u voort uit de inrichting van de elektronische patiëntendossiers die de zorgaanbieders hanteren (zoals Edifact en Hl7v2).

4 Informatiebeveiliging in de toekomst

In de schriftelijke antwoorden van 13 oktober 2025 gaf u aan dat er een strategische planning is opgesteld om de certificering van SCAL gefaseerd uit te breiden naar andere entiteiten, waaronder NMDL en LCPL. U liet weten dat u hiervoor extra capaciteit heeft aangetrokken. U gaf als doelstelling om in 2026 de entiteiten NMDL en LCPL volledig gecertificeerd te hebben volgens NEN 7510.

In het gesprek van 16 december 2025 vertelde u dat u vóór september 2026 de entiteiten NMDL en LCPL zult laten certificeren voor de norm NEN 7510. Clinical Diagostics had destijds een partij op het oog om de certificering uit te voeren, maar daar was op dat moment nog geen formele opdracht voor gegeven. Tijdens het inspectiebezoek vertelde u de inspectie dat er inmiddels een interne GAP-analyse was gemaakt. Een concreet plan van aanpak waaruit bleek welke stappen u zou gaan zetten om aantoonbaar te gaan voldoen aan de norm was tijdens het gesprek niet beschikbaar. Daarom vroeg de inspectie een plan van aanpak te delen wanneer dit beschikbaar zou zijn.

Op 5 februari 2026 ontving de inspectie dit plan van aanpak met daarbij een presentatie waarin het plan werd toegelicht. Deze presentatie bevatte tevens een detailplanning. In dit plan is de eerder genoemde GAP-analyse verwerkt. De streefdatum voor certificering, die u in deze presentatie heeft opgenomen, is april 2026. Uit dit plan blijkt dat het contract met de certificerende instantie is getekend en dat audits zijn ingepland op 3 en 4 maart en op 13 en 14 april 2026.

Het viel de IGJ op dat de scope van dit plan alleen Clinical Diagnostics LCPL B.V. en niet Clinical Diagnostics NMDL B.V. betreft. Dit in tegenstelling tot uw eerdere antwoorden. Hierover gaf u desgevraagd op 17 februari 2026 schriftelijk de volgende uitleg: De laboratoriumactiviteiten van NMDL zijn geheel overgedragen aan LCPL. In november 2025 zou dit zijn geformaliseerd doordat de Raad van Accreditatie de accreditatie van NMDL heeft ingetrokken. Voor enige dossierbewaarplichten die nog op NMDL rusten maakt u volledig gebruik van de IT-omgeving van LCPL. Om deze reden bestaat er volgens u niet langer de noodzaak om NMDL te laten certificeren voor NEN 7510.

5 Conclusie inspectie

Het doel van het onderzoek was inzicht te krijgen in de status van informatiebeveiliging bij de getroffen bedrijfsonderdelen van Clinical Diagnostics, zowel op het moment van het informatiebeveiligingsincident als ten tijde van het inspectiebezoek. Concreet toetste de inspectie of u voldeed aan wettelijk verplichte norm NEN 7510.

Op basis van de informatie die tijdens het onderzoek ontvangen is, concludeert de IGJ dat u niet heeft kunnen aantonen dat beide bedrijfsonderdelen, zowel op het

moment van het informatiebeveiligingsincident als tijdens het inspectiebezoek, aan de norm voldeden. Daarnaast stelt de IGJ vast dat u op de getoetste onderwerpen van de norm, niet voldeed aan de eisen die de norm stelt. De IGJ concludeert daarom dat LCPL en NMDL niet voldeden aan de norm en daarmee niet aan de wettelijke vereisten die volgen uit de Wabvpz.
Gezien de grote omvang van de verwerking en de risico's voor de persoonlijke levenssfeer van betrokkenen door de gevoelige aard van de gegevens, hadden Clinical Diagnostics LCPL en NMDL zich hebben moeten vergewissen van hun verantwoordelijkheid. De wettelijke plicht om te werken volgens NEN 7510 bestaat juist om dit soort risico's te beperken. Clinical Diagnostics had de risico's van de verwerking van deze gegevens periodiek en bij grote veranderingen in kaart moeten brengen. Zonder deze risico's te kennen, zijn zij niet in staat geweest passende maatregelen te treffen. Deze maatregelen hadden het risico op het plaatsvinden van het informatiebeveiligingsincident kunnen verkleinen en de gevolgen daarvan kunnen beperken.

Onderbouwing conclusie
In de op 5 februari 2026 ontvangen stukken gaf u aan dat in de periode 3 jaar voorafgaand aan het incident geen audit was uitgevoerd op het onderwerp informatiebeveiliging/ NEN 7510. Dit betekent dat Clinical Diagnostics NMDL en Clinical Diagnostics LCPL niet hebben kunnen aantonen in die periode te voldoen aan de norm NEN 7510.

Naast de vaststelling dat LCPL en NMDL niet hebben kunnen aantonen aan de norm te voldoen, heeft de IGJ afwijkingen van de norm vastgesteld. De IGJ heeft in het onderzoek niet alle verplichtingen uit norm getoetst, maar heeft zich op een aantal, voor dit onderzoek, relevante onderdelen gericht:

- Een audit of beoordeling op de norm waarmee is vastgesteld dat er gewerkt wordt volgens de norm NEN 7510.
- Een risicoanalyse op het gebied van informatiebeveiliging.
- De samenwerking en gegevensuitwisseling met andere zorgaanbieders.

Aangezien de risicoanalyse vereist is om de juiste beheersmaatregelen voor informatiebeveiliging te kunnen inschatten en de audit vereist is om zo nodig bij te kunnen sturen, zijn dit essentiële vereisten uit de norm en kan het managementsysteem voor informatiebeveiliging niet als effectief worden beschouwd wanneer deze niet aanwezig zijn.

Deze verplichtingen staan in de volgende onderdelen van de norm:

- Hoofdstuk 8. De organisatie moet, met geplande tussenpozen of zodra belangrijke veranderingen worden voorgesteld of zich voordoen, risicobeoordelingen voor informatiebeveiliging uitvoeren (…)
  De organisatie moet gedocumenteerde informatie bewaren over de resultaten van de risicobeoordelingen voor informatiebeveiliging.
- Hoofdstuk 9.2.2: De organisatie moet (een) auditprogramma('s) plannen, vaststellen, implementeren en onderhouden, met inbegrip van de frequentie, methoden, verantwoordelijkheden, planningseisen en rapportage. (…) Gedocumenteerde informatie moet beschikbaar zijn als bewijs van de implementatie van het (de) audit programma('s) en de auditresultaten.
- A.5.35, Onafhankelijke beoordeling van informatiebeveiliging: De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan, met inbegrip van mensen, processen en

technologieën, moeten onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen, worden beoordeeld.
- Verder gaat het ten aanzien van gegevensuitwisseling om het volgende vereiste uit NEN 7512[4]:
  Hoofdstuk 5. Voordat het kader tot stand komt, behoort voor het geheel van de communicatiepartijen duidelijk te worden welke mate van risico acceptabel is. (NB: het 'kader' is de overeenkomst die bij de uitvoering van de uitwisseling betrokken communicatiepartijen bindt; zie voor verdere details hoofdstuk 5 van de NEN 7512).

Vervolgacties
In hoofdstuk 3b van de Wabvpz is bepaald dat de (ambtenaren van de) inspectie belast zijn met het toezicht op de naleving van de artikelen 4 tot en met 12, 15d, 15e, 15ea en 15j. In de Wabpvz is ook opgenomen welke maatregelen de inspectie kan nemen bij een overtreding van deze wettelijke bepalingen.
De handhavingsinstrumenten die de inspectie heeft, betreffen herstelmaatregelen. Een herstelmaatregel strekt tot het geheel dan wel gedeeltelijk ongedaan maken of beëindigen van een overtreding, tot het voorkomen van herhaling van een overtreding, dan wel tot het wegnemen of beperken van de gevolgen van een overtreding. Op grond van de Wabpvz is de inspectie, voor zover zij toeziet op deze wet, niet bevoegd bestraffende maatregelen in te zetten.

U heeft aangegeven NEN 7510 binnen LCPL in te voeren. Vervolgens laat u LCPL hierop halverwege april door een certificerende instantie beoordelen. De IGJ verwacht dat Clinical Diagnostics LPCL vanaf dat moment aantoonbaar zal voldoen aan de NEN 7510. Concreet verwacht de inspectie:

- De uitkomsten van de certificeringsaudit die zal plaatsvinden op 3 en 4 maart en 13 en 14 april 2026. Graag ontvangen we uiterlijk 30 april 2026 de eerste resultaten. Het rapport en certificaat ontvangen we vervolgens per omgaande zodra die in uw bezit zijn.
- Indien er verschuivingen in deze planning plaatsvinden verwachten we hiervan direct bericht.

Vragen
Heeft u vragen over deze brief? Dan kunt u contact met ons opnemen via [redacted]. Vermeldt daarbij het nummer [redacted] in uw mail of brief.
U kunt ook telefonisch contact met ons opnemen via het meldpunt IGJ.

[redacted]