

De standaard Logging Dataverwerkingen versus de standaard NEN 7513: Vastleggen van acties op persoonlijke gezondheidsinformatie

Inleiding

De logging van Dataverwerking in de Nederlandse gezondheidszorg gebaseerd op de NEN7513 norm. De NEN7513 biedt een standaard ten aanzien van de te loggen gegevens, de standaard geeft echter geen inzicht in de manier waarop de deze gegevens gelogd moeten worden, de standaard Logging Gegevensverwerkingen biedt wel een concreet antwoord op de vraag HOE er gelogd moet worden. Dit document geeft de grootste verschillen weer tussen de standaard Logboek Dataverwerkingen en de standaard NEN7513 en hoe deze verschillen in de te loggen gegevens overbrugd kunnen worden. Daarnaast biedt dit document een voorbeeldarchitectuur aan voor de implementatie van de NEN7513 gebaseerd op de standaard Logging Dataverwerkingen. Dit document is niet-normatief.

NEN 7513: de standaard voor logging in de Nederlandse gezondheidszorg

Medische persoonsdata behoren tot de meest privacygevoelige categorie van data. Medische dossiers worden ingezien, bijgewerkt en verzonden naar andere instanties. Het is daarom van groot belang dat er vooraf door beveiliging van data en achteraf door controle kan worden nagegaan of de data-integriteit is gewaarborgd. In [extensie](#) van de Core standaard Logboek Dataverwerkingen worden de specificaties voor de NEN7513 gespecificeerd.

Verschillen in standaarden

Diverse velden van beide standaarden komen niet overeen, dit is globaal als volgt te verklaren:

- 1. Audit/systeemgebeurtenissen niet in scope:** De standaard Logging Dataverwerkingen laat audit- en systeemloggingen buiten beschouwing. Dit betekent dat de NEN7513 Categorieën Gebruiker, Bronsysteem, 'Nederlandse Velden', Vraager, Vraag en Alternatieve Deelnemer niet gemapt kunnen worden.
- 2. Objectregistratie:** De NEN7513 standaard heeft een uitgebreide Objectregistratie uitgewerkt. In de standaard Logging Dataverwerkingen wordt de Objectregistratie verder gedetailleerd in onder andere de extensie Betrokkene.
- 3. Tracering:** De kernwaarde van de standaard Logging Dataverwerkingen is het gebruik van tracering (interoperabiliteit). Dit betekent dat tracering moet worden toegepast bij elke Logregel (tracingId en spanId). De standaard NEN7513 gebruikt (optioneel) tracering in Uitwisselingsgebeurtenissen.

Twée standaarden komen bij elkaar

Ondanks de verschillen in visie en data is een gezamenlijk datamodel goed mogelijk. De standaard NEN7513 zal wel een aantal wijzigingen moeten ondergaan.

Data vergeleken

De datavelden van de NEN7513 en de standaard Logboek Dataverwerkingen vergeleken, levert het volgende overzicht op:

NEN-veldnaam	NEN-betekenis	Standaard LDV
EventID	Identificatie van gebeurtenis	dplCoreProcessingActivityId
EventActionCode	De in de gebeurtenis uitgevoerde actie waardoor de logging werd gegenereerd	name
EventDateTime	De datum/tijd waarop de gebeurtenis zich heeft voorgedaan	startTime en endTime
EventOutcomeIndicator	Code voor het al dan niet slagen van de gebeurtenis	statusCode
EventTypeCode	Het type gebeurtenis	Niet Aanwezig
UserID	Identificatie van de persoon die of het proces dat zich van de gegevens bedient	Niet Aanwezig
AlternateUserID	Lokale identificatie van de persoon die of het proces dat zich van de gegevens bedient	Niet Aanwezig
UserName	De naam van de persoon die of het proces dat zich van de gegevens bedient	Niet Aanwezig
UserIsRequestor	Of de persoon die of het proces dat zich van de gegevens bedient al dan niet de initiator van deze gebeurtenis is	Niet Aanwezig
RoleIDCode	De rol van de persoon die of het proces dat zich van de gegevens bedient bij het uitvoeren van de gebeurtenis	Niet Aanwezig
PurposeOfUse	Het doel van het gebruik van de gegevens waartoe toegang wordt gemaakt	Niet Aanwezig (onderdeel van Register van Verwerkingsactiviteiten)
NetworkAccessPointTypeCode	Typecode van het toegangspunt tot het netwerk	Niet Aanwezig
NetworkAccessPointID	Identificatie van het toegangspunt tot het netwerk	Niet Aanwezig
AuditEnterpriseSiteID	De logische locatie van het bronsysteem	Niet Aanwezig

AuditSourceID	Unieke identificatie van het bronsysteem	Niet Aanwezig
AuditSourceTypeCode	De typecode van het bronsysteem	Niet Aanwezig
ParticipantObjectTypeCode	De klasse van het betrokken object	Niet Aanwezig
ParticipantObjectTypeCodeRole	De categorie van het betrokken object	Niet Aanwezig
ParticipantObjectDataLifeCycle	Identificatie van het stadium in de levenscyclus van het betrokken object	Niet Aanwezig
ParticipantObjectIDTypeCode	Het in het veld [ParticipantObjectID] opgenomen type	dplCoreDataSubjectIdType
ParticipantObjectPermissionPolicySet	Het actieve toestemmings-beleid voor de identificatie [ParticipantObjectID], bijvoorbeeld informatie over het geven van toestemming door de cliënt	Niet Aanwezig
ParticipantObjectSensitivity	De in het kader van het beleid gedefinieerde gevoeligheid voor de identificatie [ParticipantObjectID]	Niet Aanwezig
ParticipantObjectID	De instantie-identificatie van het betrokken object	dplCoreDataSubjectId
ParticipantObjectName	De naam van de instantie van het betrokken object	Niet Aanwezig
ParticipantObjectDetail	De details van de instantie van het betrokken object	Niet Aanwezig
ParticipantObjectDescription	De beschrijving van de instantie van het betrokken object	Niet Aanwezig
ParticipantObjectQuery	De inhoud van de zoekvraag	Niet Aanwezig
Autorisatie protocol	Identificatie van het autorisatieprotocol dat bij de gebeurtenis is gehanteerd	Niet Aanwezig
Behandelrelatie protocol	Identificatie van het protocol dat beschrijft hoe wordt vastgesteld dat er sprake is van een behandelrelatie	Niet Aanwezig
Toestemmingsprofiel	Identificatie van het toestemmingsprofiel dat bij de gebeurtenis is gehanteerd	Niet Aanwezig
Controles	De resultaten van de uitgevoerde controles op autorisatie, behandelrelatie, toestemming cliënt en gebruik noodprocedure	Niet Aanwezig

W3c-Trace-Context-Traceparent	Unieke samengestelde identificatie voor individuele traceerverzoeken	traceld/spanId/parentSpanId
W3c-Trace-Context-Traceresponse	Identificatie van een voltooid traceerverzoek	traceld/spanId/parentSpanId

Verdere detaillering data

Metadata

Voor het metadatagedeelte van de logging is er speciale aandacht nodig voor de volgende data:

EventID: De NEN7315 spreekt niet expliciet over de koppeling met een Register van Verwerkingen. Het gaat hier om een unieke identifier om bepaald type Gebeurtenis aan te geven. Daarmee rechtvaardigt het in dit geval om dit veld te koppelen aan het Register van Verwerkingen.

EventTypeCode: Dit veld komt niet voor in de standaard Logboek Dataverwerkingen. Het veld wordt opgenomen als 'Key Value' pair in de Attributes-lijst.

NEN7513	Standaard LDV
EventID	dplCoreProcessingActivityId
EventActionCode	name
EventDateTime	startTime/endTime
EventOutcomeIndicator	statusCode
EventTypeCode	Niet aanwezig

Vertalingen van de NEN7513-benamingen naar de Logboek Dataverwerkingenbenamingen worden in het Profiel van het logboek geregeld.

Objectdata

De standaard Logboek Dataverwerkingen schrijft op een summiere wijze richtlijnen voor ten aanzien van de registratie van objecten om zo ruimte te bieden voor verschillende manieren waarop een object gelogd kan worden.

In de standaard Logboek Dataverwerkingen wordt een Betrokkene geregistreerd door middel van dpl.core.data_subject_id (unieke identifier van de Betrokkene) en dpl.core.data_subject_id_type (type van subjectId, bijvoorbeeld BSN). In de NEN7513 wordt een Betrokkene als volgt geregistreerd (in dit voorbeeld een Cliënt):

-) ParticipantObjectID: <unieke Id>
-) ParticipantObjectIDTypeCode: 1 (Persoon)
-) ParticipantObjectTypeCodeRole: 1 (Cliënt)

De NEN-methodiek kan worden toegepast op voorwaarde dat er een vertaling aanwezig is naar de standaard Logboek Dataverwerkingen.

Objectdata wordt geregistreerd als key-value pair en als lijst in 'Attributes'.

Audit/systeemdata

De standaard Logboek Dataverwerkingen beschouwt audit/systeemdata als niet in scope. Voor de standaard NEN7513 is deze data van wezenlijk belang. In de ideale situatie wordt audit/systeem weggeschreven in een apart Logboek Audit/systeem. Hierbij wordt tracing bijgevoegd zodat er eenvoudig een relatie kan worden gelegd met de data die is geregistreerd in het Logboek Dataverwerkingen.

Indien het Logboek Audit/systeem niet aanwezig is en/of niet mogelijk is, dan kan ook een aparte logregel worden toegevoegd aan het Logboek Dataverwerkingen met alleen de audit/systeemdata. Ook hier moet tracing worden toegevoegd worden om de relatie tussen de logregels te waarborgen.

In het geval er geen apart logboek Audit/systeem aanwezig is, dan moet de audit/systeemdata geregistreerd worden als key-value pair en als lijst in 'Attributes'.

De volgende data wordt gelogd als Audit/systeemdata:

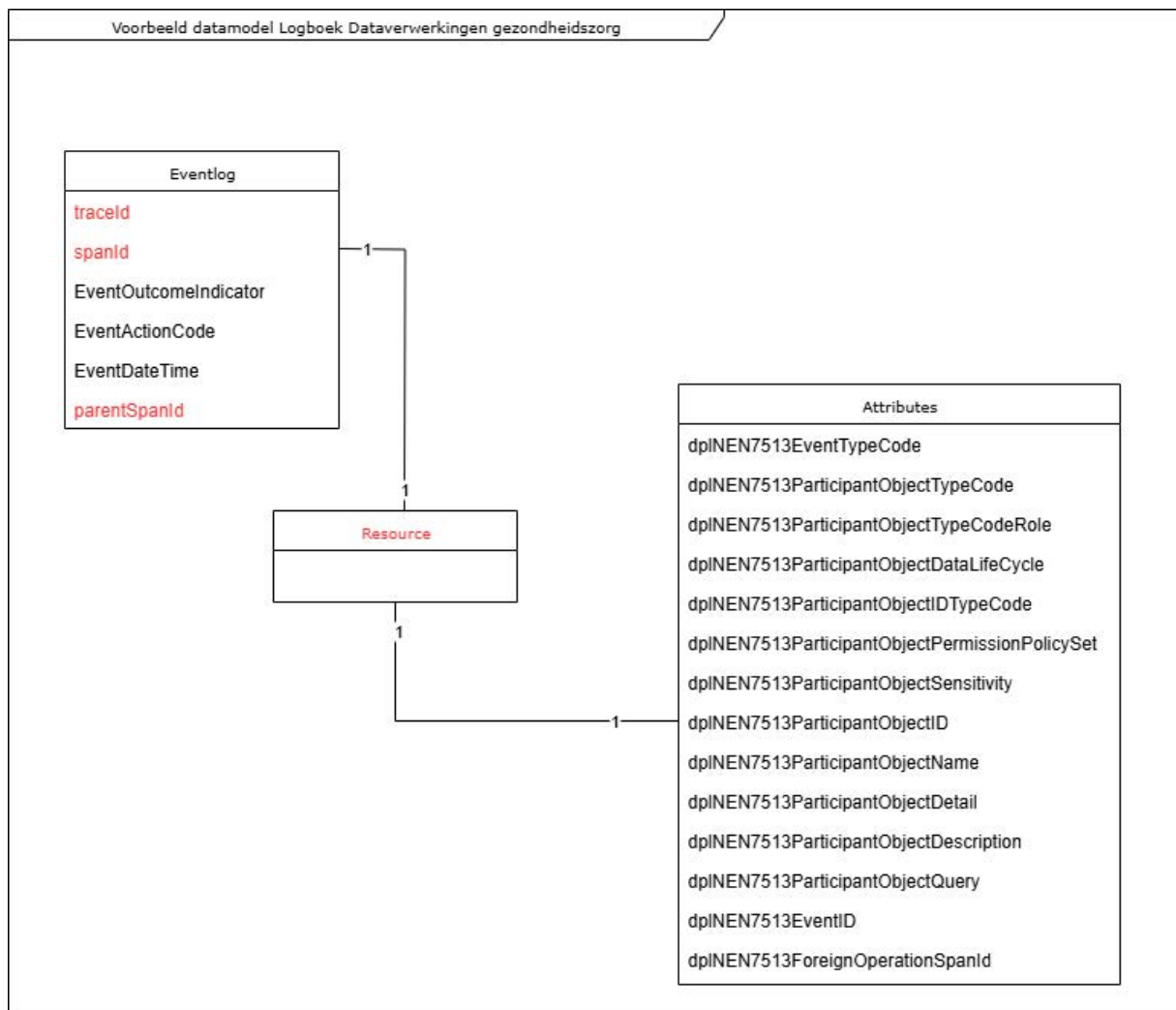
NEN-veldnaam
UserID
AlternateUserID
UserName
UserIsRequestor
RoleIDCode
PurposeOfUse
NetworkAccessPointTypeCode
NetworkAccessPointID
AuditEnterpriseSiteID
AuditSourceID
AuditSourceTypeCode
Autorisatie protocol
Behandelrelatie protocol
Toestemmingsprofiel
Controles

Namespace

De standaard Logboek Dataverwerkingen stelt dat elk data-element in 'Attributes' voorzien wordt van een namespace 'dpl.<domain>'. Dit betekent dat alle data-elementen voorzien worden van 'dpl.NEN7513' als prefix. Bijvoorbeeld: ParticipantObjectID wordt dplNEN7513ParticipantObjectID.

Datamodel NEN7513

Op basis van voorgestelde wijzigingen zou het datamodel van een logregel voor de NEN7513 er als volgt uitzien:



Idealiter worden de Audit/systeemdata opgeslagen in een Audit/systeemlog. Als dit niet het geval is, dan worden de Audit/systeemdata ook voorzien van de prefix 'dpINEN7513'.