Nederlandse norm

NEN 7513

(nl)

Medische informatica - Logging - Vastleggen van acties op elektronische patiëntdossiers

Health informatics - Recording actions on electronic patient health records

Vervangt NEN 7513:2009 Ontw.

ICS 35.240.80

juli 2010

Normcommissie 303 006 "Informatievoorziening in de zorg"

NEN

Postbus 5059, 2600 GB Delft
Telefoon (015) 2 690 390, Fax (015) 2 690 190

Inhoud

Inleiding en context

Verschillende actuele ontwikkelingen maken het meer dan ooit noodzakelijk om heldere afspraken te maken over de beheersing van de elektronische toegang tot patiëntgegevens. Ontwikkelingen in infrastructuur en wetgeving zijn vooral gericht op verbetering van beschikbaarheid van informatie en doelmatige toepassing van elektronische communicatie daarbij.

De regelgeving op dit terrein is gericht op de gegevens die zorgaanbieders bijhouden over hun patiënten, maar afspraken over toegangsbeheersing kunnen evenzo worden toegepast op gegevens die patiënten zelf over hun gezondheid verzamelen en bijhouden, persoonlijke zorgdossiers genoemd.

De NEN normcommissie 'Informatiebeveiliging in de zorg' heeft begin 2006 de notitie "Beheersing van de elektronische toegang tot patiëntgegevens" opgesteld. Dit is een uitwerking van het hoofdstuk over Toegangsbeveiliging uit de Nederlandse norm NEN 7510. In de notitie zijn de contouren geschetst voor een samenhangend stelsel van normen om de elektronische verwerking en uitwisseling van patiëntgegevens verantwoord te laten plaatsvinden.

In die notitie was gesteld dat informatie- en communicatiesystemen die worden gebruikt voor vastlegging, opslag en verstrekking van patiëntgegevens moeten voorzien in mogelijkheden om:

a) de identiteit van een gebruiker eenduidig vast te stellen (*identificatie*) en te verifiëren (*authenticatie*);

b) bij een gebruiker één of meer rollen vast te leggen en te verwijderen (*roltoekenning*);

c) regels vast te leggen waarin de toegang tot bepaalde gegevens wordt gebonden aan bepaalde rollen (*autorisatieprotocollen*);

d) door de patiënt zelf aan te geven toegangsaanwijzingen (*toestemmingsprofielen*) vast te leggen en te wijzigen;

e) de toegang tot gegevens te beperken tot hetgeen overeenkomstig de regels (c) en de beperkingen (d) is geoorloofd (*toegangscontrole*);

f) gegevens over verleende toegang te registreren (*loggen*) waarmee de rechtmatigheid van de toegang achteraf kan worden gevalideerd.

Vanwege de noodzakelijke interactie tussen verschillende toepassingen en de infrastructurele voorzieningen is standaardisatie op de hier genoemde punten een vereiste. In dit kader is de eerste prioriteit toegekend aan het ontwikkelen van een norm voor het vastleggen van (meta)gegevens en kenmerken van de acties die feitelijk hebben plaatsgevonden op een patiëntdossier, een norm voor logging. Aan de hand van de gelogde acties wordt het mogelijk te controleren of de toegangsverlening en het gebruik van het dossier volgens de regels zijn verlopen. Tevens biedt dat mogelijkheden om verbeteringen te ontwerpen in bestaande toegangscontroles.

In het NEN-rapport "Uitgangspunten voor autorisatieprotocollen en toestemmingsprofielen" [11] is als voorbereiding op de ontwikkeling van een norm voor logging de samenhang weergegeven tussen de elementen die bij toegangsverlening een rol spelen. Het voorliggende document is een ontwerp van de logging-norm.

Doel van het loggen

Loggen van acties op elektronische patiëntdossiers heeft als doel een betrouwbaar overzicht te kunnen leveren van de gebeurtenissen waarbij zorggegevens over een persoon zijn verwerkt. "Verwerken" is hier bedoeld zoals gedefinieerd in de Wet bescherming persoonsgegevens: *"elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens"*.

Zorgaanbieders hebben de logging nodig om zich te kunnen verantwoorden tegenover hun patiënten, collega's en anderen, over de zorgvuldigheid waarmee zij met de zorggegevens omgaan.

Bij de beheersing van toegang tot zorggegevens vormt de logging, als vastlegging van feitelijke gebeurtenissen, een belangrijke schakel. Het loggen moet verantwoording en controle achteraf mogelijk maken. Analyse van de logging vormt een aanvulling op de controle op bevoegdheden die door de informatiesystemen wordt uitgevoerd, maar vervangt die niet.

Bevoegdheden en toegangsregels

De bevoegdheden die aan gebruikers van informatiesystemen worden toegekend moeten het hun mogelijk maken het systeem voor hun taken te gebruiken. Niet alle taken zullen echter tijdig vooraf te voorzien zijn en detaillering van bevoegdheden is ook maar beperkt mogelijk. In de praktijk bieden de toegekende bevoegdheden daardoor een zekere ruimte ten opzichte van de formele toegangsregels.

Ten aanzien van zorggegevens zijn verschillende wetten, regels en richtlijnen van toepassing die in een bepaalde situatie bepalen hoe met de gegevens moet worden omgegaan. De Wet op de geneeskundige behandelingsovereenkomst en de Wet bescherming persoonsgegevens leggen de zorgaanbieders verplichtingen op en geven de patiënten bepaalde rechten. Doelbinding vormt voor het omgaan met persoonsgegevens een sleutelbegrip.

Autorisatieprotocollen en toestemmingsprofielen

Als uitwerking van de wetgeving worden door zorgverleners en daartoe aangewezen instanties autorisatieprotocollen opgesteld waarin de reguliere toegang tot bepaalde zorggegevens wordt gebonden aan een rol in het zorgproces en kunnen patiënten specifiek gewenste verruimingen of beperkingen op de algemene regels kenbaar maken in toestemmingsprofielen. Meer hierover is beschreven in het NEN-rapport "Uitgangspunten voor autorisatieprotocollen en toestemmingsprofielen" [11].

Om te kunnen dienen voor verantwoording van een bepaalde actie op een elektronisch patiëntdossier moeten in de logging verwijzingen worden opgenomen naar het autorisatieprotocol en naar het toestemmingsprofiel dat bij die gebeurtenis van toepassing was. Is er (nog) geen autorisatieprotocol of toestemmingsprofiel van kracht, dan wordt het ontbreken ervan vermeld. Dit maakt geleidelijke ontwikkeling en invoering mogelijk.

Gestandaardiseerde logging

Bij het specificeren van de logging is toekomstvastheid nagestreefd. Het inpassen van logging in informatiesystemen gaat inspanning en tijd vergen en het is niet gewenst dat de systemen opnieuw moeten worden aangepast bij elke ontwikkeling in de toegangsbeheersing. In de specificaties komt daarom nog een aantal open einden voor, zoals verwijzingen naar codestelsels die nodig zijn, maar nog niet bestaan en aanduiding van delen van het patiëntdossier, terwijl over compartimentering nog afspraken moeten worden gemaakt. Verder is gestreefd naar flexibiliteit en compatibiliteit met internationale ontwikkelingen. Dat heeft op een aantal plaatsen geleid tot optionele velden.

Met de logging wordt beoogd een betrouwbaar overzicht te kunnen leveren van de gebeurtenissen waarbij zorggegevens over een persoon zijn verwerkt. Die gebeurtenissen kunnen zich over verschillende plaatsen en tijden uitstrekken. Het beoogde overzicht is dus alleen mogelijk als de loggegevens uit verschillende bronnen kunnen worden gecombineerd. Ook zonder direct een virtueel wereldwijd en levenslang patiëntdossier als doel te stellen is duidelijk dat gestandaardiseerde logging een voorwaarde is om het overzicht voor de betreffende persoon mogelijk te maken.

Informatiedomeinen

Delen van het totaal aan zorginformatie over een persoon kunnen zich in verschillende informatiesystemen bevinden en onder verschillende verantwoordelijkheidsgebieden vallen.

Een gebied waarbinnen het beleid en de verantwoordelijkheden ten aanzien van de informatievoorziening gemeenschappelijk zijn en de naamgeving van personen, systemen en andere objecten uniek is, wordt hier informatiedomein genoemd. In een informatiedomein bevinden zich één of vele informatiesystemen onder

hetzelfde regime. Evenzo kunnen zich één of meer bronnen van loggegevens in een informatiedomein bevinden.

Informatiedomeinen kunnen geheel of gedeeltelijk met andere informatiedomeinen worden gecombineerd tot samengestelde informatiedomeinen. Het beleid, de verantwoordelijkheden en de systematiek voor naamgeving moeten dan voor het geheel van de samenstellende informatiedomeinen gemeenschappelijk gaan gelden.

In de eenvoudigste vorm omvat een informatiedomein een enkel informatiesysteem en is dat ook de bron van de loggegevens. Dat kan bijvoorbeeld het geval zijn in een individuele zorgpraktijk of in een zelfstandig laboratorium. In samenwerkingsverbanden en complexere organisaties zijn veel informatiesystemen aanwezig. Dan kan een enkel informatiedomein worden gevormd wanneer voor een gemeenschappelijk regime wordt gekozen. Een bijzonder informatiedomein vormt het landelijk (virtueel) EPD van AORTA met het landelijk schakelpunt als centraal systeem. Beleid, verantwoordelijkheden en naamgeving zijn hiervoor op nationaal niveau bepaald. Aan het andere eind van het spectrum vormt het persoonlijk zorgdossier van een patiënt een privé informatiedomein.

Doel van de logging-norm

De logging-norm specificeert de gebeurtenissen die in aanmerking komen om te loggen en de loggegevens die dan bij een gebeurtenis in een logregel moeten worden vastgelegd. De gebeurtenissen betreffen toegang tot patiëntgegevens, toegang tot de logging en gebeurtenissen die invloed kunnen hebben op de betekenis of de betrouwbaarheid van de logging.

De norm moet toepasbaar zijn op elk informatiedomein in de gezondheidszorg. Verwijzingen in de logging naar codestelsels, naamconventies en beleid dat van toepassing is in het desbetreffende informatiedomein, moeten zorgen voor de flexibiliteit om dat mogelijk te maken. Het beleid dat voor een informatiedomein geldt kan een veld in de logregel dat in de norm optioneel is, binnen het informatiedomein verplicht stellen. Omgekeerd kan dat niet.

De norm specificeert het niveau van detail waarmee de acties worden gelogd die bij een gebeurtenis plaatsvinden. Als er bijvoorbeeld gegevens zijn toegevoegd in een patiëntdossier zal dat als feit worden gelogd. De toegevoegde gegevens staan dan in het dossier, niet in de logging. Voor een aanduiding op welk deel van het patiëntdossier de actie heeft plaatsgehad is ruimte gereserveerd.

Beveiliging van de logging

Conceptueel vormt de logging een tweede-orde informatiesysteem dat informatie bevat over systemen die de zorg ondersteunen. En net als voor elk ander informatiesysteem moet voor de logging aandacht worden besteed aan integriteit, vertrouwelijkheid en beschikbaarheid. De wijze waarop dit wordt geregeld is sterk afhankelijk van de technische opzet die voor de logging wordt gekozen. Daarvoor zijn diverse modellen denkbaar, maar in alle gevallen moet de toegang tot de logging worden gereguleerd en gecontroleerd met geschikte programmatuur. Rechtstreeks lezen van de logging is dus geen optie.

Verantwoordelijkheid en toezicht

Iedere deelnemer aan het zorgproces die behoefte heeft zich te kunnen verantwoorden, of daartoe wordt genoodzaakt, is gebaat bij de aanwezigheid van een betrouwbare logging. Het is dan ook een collectieve verantwoordelijkheid daarvoor te zorgen. De norm voor logging moet het loggen op gestandaardiseerde wijze mogelijk maken. Wanneer hierbij wordt gedacht aan toezicht, zal het niet zozeer gaan over toezicht op het toepassen van deze norm, als wel over het toezicht op het zorgvuldig omgaan met zorginformatie.

Groeiproces

Het toepassen van deze norm is geen doel op zichzelf, maar een stap in de ontwikkeling van systematische beheersing van de toegang tot zorginformatie. Volledige implementatie van de systematiek zal nog geruime tijd vergen en mogelijk op onderdelen niet volledig haalbaar zijn.

OPMERKING Er zijn systemen die per definitie niet kunnen voldoen aan deze norm – voorbeeld is een PDMS (*Patient Data Management System*) op de IC, dat vanwege zijn functie altijd aan staat met cruciale gegevens. Registratie van degenen die gegevens hebben gezien (ook voorbijgangers) is per definitie niet mogelijk en daarmee is voor dit specifieke systeem volledige implementatie van de norm niet mogelijk.

Implementatie van de norm in een organisatie begint met het uitvoeren van een risicoanalyse, met het oog op de in deze norm gestelde eisen. Op basis van deze risicoanalyse moet men bepalen voor welke terreinen binnen de organisatie (bijvoorbeeld organisatorische deelterreinen en/of informatiesystemen), in welke mate en op welke termijn deze norm zal worden gevolgd.

Daar de normtoepassing mede afhankelijk is van de geschiktheid van informatiesystemen, is overleg met de leveranciers van deze systemen essentieel. Bij de aanschaf of bouw van nieuwe applicaties moet rekening worden gehouden met deze norm. Met het oog op de hiervoor noodzakelijke systeemontwikkeling is in deze norm aansluiting gezocht bij de specificaties van IETF/RFC-3881 [1], DICOM [3] en het IHE IT Framework [4], [5].

Medische informatica – Logging – Vastleggen van acties op elektronische patiëntdossiers

1 Onderwerp en toepassingsgebied

Het patiëntdossier vormt een wezenlijk onderdeel van de veilige zorg aan de patiënt. Voor veilige zorg is het essentieel dat gegevens in het dossier integer zijn. Daarbij bevat het dossier in de aard van de registratie zeer privacygevoelige gegevens. Om deze twee redenen, vastgelegd in wettelijke bepalingen, is het van belang te allen tijde te kunnen achterhalen wie toegang heeft gehad tot het dossier, volgens welke regels hij die toegang heeft gekregen en welke acties hij daarop heeft uitgevoerd.

De in deze norm beschreven logging voorziet in de stelselmatige geautomatiseerde registratie van gegevens rond de toegang tot het patiëntdossier, die controle van de rechtmatigheid ervan mogelijk maakt.

Deze norm biedt zorgaanbieders aanwijzingen voor het loggen en gebruik van de logging om te voldoen aan wettelijke verplichtingen en levert ontwikkelaars van informatiesystemen een aantal eisen waaraan hun systemen zullen moeten voldoen.

Op zorgverleners rust een dossierplicht. Patiënten[1)] moeten worden geïnformeerd en hebben recht op inzage in het dossier waarin de gegevens over hun behandeling zijn gedocumenteerd. Wanneer, zoals meestal het geval is, verschillende zorgverleners op verschillende momenten bij de zorg aan een patiënt worden betrokken, vormt het dossier een van de schakels in de communicatie.

In het kader van deze norm wordt onder een elektronisch patiëntdossier de totale verzameling verstaan van alle elektronisch vastgelegde gegevens die de diagnostiek en medische en paramedische behandeling en verzorging van een bepaalde persoon documenteren. Een elektronisch patiëntdossier in deze zin zal dus meestal delen omvatten die op verschillende tijdstippen, in verschillende informatiedomeinen, door verschillende personen zijn vastgelegd. Het beleid voor het informatiedomein bepaalt welke gegevens voor het documenteren van zorg en behandeling nodig zijn.

Raadplegen van relevante gegevens uit het patiëntdossier en daarin vastleggen van bevindingen en uitgevoerde behandelingen zijn onverbrekelijk verbonden aan het zorgproces. Voor het vastleggen van die acties op het patiëntdossier wordt in deze norm de term 'loggen' gehanteerd. Het resultaat van het loggen wordt hier aangeduid met de term 'logging'. Dit is een verzamelbegrip voor de gegevens die betreffende een bepaalde actie worden gelogd, de 'loggegevens', en de 'logbestanden' waarin deze worden bewaard.

Belanghebbenden van de logging zijn allereerst de patiënten zelf of diegenen die namens hen optreden. Zorgaanbieders vormen een tweede categorie belanghebbenden. Daarnaast zijn ook toezichthouders belanghebbenden bij de logging. Dat kunnen externe toezichthouders zijn, maar ook toezichthouders binnen een zorginstelling of binnen een kring van zorgverleners. Op de wijze waarop de logging door de belanghebbenden zal worden gebruikt en invulling van het toezicht gaat deze norm niet in.

De logging moet kunnen voorzien in informatie waaraan de genoemde belanghebbenden behoefte hebben. Een belangrijk aspect daarbij is de controle op gerechtigdheid van de raadpleging. Daarnaast kan analyse van de logging ondersteuning bieden voor het verbeteren van het proces van de toegangscontrole tot patiëntgegevens. De bewaartermijn voor de logging moet in overeenstemming zijn met het beoogde gebruik van de logging.

Deze norm specificeert de gegevens die nodig zijn met het oog op de vastgestelde informatiebehoefte van de belanghebbenden en de aanleidingen voor het vastleggen ervan. Geen uitspraak wordt gedaan over de plaats waar de loggegevens moeten worden opgeslagen. Dit kan bijvoorbeeld bij het deeldossier waarop de logging betrekking heeft, in een centrale databank of op een andere plaats zijn. In alle gevallen moet echter worden voldaan aan dezelfde eisen van volledigheid, betrouwbaarheid, toegangsbeheersing en interoperabiliteit.

1) Overwogen is de term 'patiënt' in deze normtekst te vervangen door 'zorgconsument'. Met het oog op het bewaren van de aansluiting bij gebruikelijke termen als 'patiëntdossier' is daartoe echter niet overgegaan.

NEN
CONNECT

ALTIJD DE ACTUELE NORM IN UW BEZIT HEBBEN?

Nooit meer zoeken in de systemen en uzelf de vraag stellen: ‘Is NEN 7513:2010 nl de laatste versie?’

Via het digitale platform NEN Connect heeft u altijd toegang tot de meest actuele versie van deze norm. Vervallen versies blijven ook beschikbaar. **U en uw collega’s** kunnen de norm via NEN Connect makkelijk raadplagen, online en offline.

Kies voor slimmer werken en bekijk onze mogelijkheden op **www.nenconnect.nl**.

Heeft u vragen?

Onze Klantenservice is bereikbaar maandag tot en met vrijdag, van 8.30 tot 17.00 uur.

Telefoon: 015 2 690 391
E-mail: klantenservice@nen.nl