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 7513:2010;
NEN 7513:2017 Ontw.

ICS 35.240.80

mei 2018

Normcommissie 303006 'Informatievoorziening in de zorg'

©2018 Koninklijk Nederlands Normalisatie-instituut
Postbus 5059, 2600 GB Delft
Telefoon (015) 2 690 390, Fax (015) 2 690 190

Inhoud

Voorwoord

Deze norm is de herziening van NEN 7513:2010.

NEN 7513 vervangt NEN 7513:2010. De belangrijkste wijzigingen ten opzichte van de vorige editie zijn:

— De norm schrijft niet alleen voor welke gegevens moeten worden gelogd, maar ook hoe deze gegevens op een begrijpelijke wijze kunnen worden verwerkt. *Patiënt*en of *cliënten* moeten hun persoonsgegevens namelijk ook kunnen inzien.

— Bij de herziening van hoofdstuk 7 is met extra zorg gekeken naar de compatibiliteit met andere standaarden over auditlog-berichten en -berichtenverkeer.

— Ook is rekening gehouden met recente ontwikkelingen in *persoonlijke gezondheidsomgeving*en, zoals het Medmij-programma. Privacyregelgeving is vooral gericht op de gegevens die *zorginstellingen* bijhouden over hun *cliënten*, maar afspraken over toegangsbeheersing kunnen net zo goed worden toegepast op gegevens die *cliënten* zelf over hun gezondheid verzamelen en bijhouden.

Deze norm is opgesteld door de normcommissie 303 006 ‘Informatievoorziening in de zorg’ na voorbereiding door de werkgroep 3030060012 ‘Werkgroep Revisie NEN 7513’.

0 Inleiding

0.1 Algemeen

Actuele ontwikkelingen in Nederland en Europa op het gebied van de privacy maken het meer dan ooit noodzakelijk om heldere afspraken te maken over de bescherming van medische gegevens tegen onbevoegde inzage en onbevoegd gebruik. Patiëntdossiers behoren zodanig te worden beveiligd dat *zorgverleners*, medewerkers of derden geen toegang hebben tot dossiers waarin zij niets te zoeken hebben.

De in NEN 7513 voorgeschreven wijze van *logging* heeft als doel een betrouwbaar overzicht te kunnen leveren van de *gebeurtenissen* waarbij *persoonlijke gezondheidsinformatie* is verwerkt [1)]. Wanneer voldaan is aan de norm is het mogelijk achteraf een overzicht te geven van de *gebeurtenissen* waarbij *persoonlijke gezondheidsinformatie* is vastgelegd, ingezien of anderszins verwerkt.

Dat overzicht maakt controle achteraf door *cliënten* mogelijk. En maakt het voor *zorginstellingen* mogelijk zich tegenover hun *cliënten*, collega's, *toezichthouders* en anderen, te verantwoorden over de zorgvuldigheid waarmee zij met de persoonsgegevens omgaan.

Analyse van de *logging* vormt voor een *zorginstelling* een aanvulling op de controle op bevoegdheden die door de *informatiesystemen* wordt uitgevoerd en faciliteert zo de op basis van NEN 7510-1:2017 voorgeschreven Plan Do Check ACT-cirkel m.b.t. de beveiliging van persoonsgegevens die door *zorginstellingen* worden gebruikt om hun *informatiesystemen* te verbeteren.

0.2 Leeswijzer

Hoofdstuk 1 beschrijft het toepassingsgebied of de 'scope' van deze norm. Waar gaat de norm precies over en waarover niet? Daarna volgen drie hoofdstukken waarin achtereenvolgens een opsomming met normen waarnaar in deze norm wordt verwezen, een opsomming van de gebruikte definities en een opsomming van gebruikte afkortingen te vinden zijn.

Om te bepalen welke items in de *logging* behoren te worden opgenomen, staat in hoofdstuk 5 welke informatie aan de *logging* moet kunnen worden ontleend. Daaruit volgen de te *loggen gebeurtenissen* in hoofdstuk 6 en de specificatie van de te *loggen* gegevens per *gebeurtenis* in hoofdstuk 7.

Hoofdstuk 8 benoemt de eisen die moeten waarborgen dat de *logging* betrouwbaar is en zorgvuldig wordt beheerd met een passende *toegangsregeling*. Hoofdstuk 9 gaat in op de eisen ten aanzien van weergave van de *logging*.

0.3 Voor wie is deze norm bedoeld?

Deze norm is bedoeld voor:

— *zorginstellingen*;

— andere beheerders van *persoonlijke gezondheidsinformatie*;

— *toezichthouders*;

1) 'Verwerken' is hier bedoeld zoals gedefinieerd in de AVG (zie hoofdstuk 3, termen en definities).

— ontwikkelaars van (zorg)*informatiesystemen*;

— *patiënt*en, *cliënten* en alle andere personen van wie *persoonlijke gezondheidsinformatie* wordt verwerkt.

Het toepassen van deze norm is niet vrijblijvend, immers wetgeving verwijst naar deze norm.

NEN 7513 bevat verplichtingen voor *zorginstellingen* en andere beheerders van *persoonlijke gezondheidsinformatie*, bijvoorbeeld gemeenten en ICT-toeleveranciers van *zorginstellingen*, zoals hosting providers en Zorg Service Providers. Degenen die binnen deze organisaties verantwoordelijk zijn voor (het toezicht op) de beveiliging van gezondheidsinformatie, evenals hun beveiligingsadviseurs, -consultants, -auditoren, -aanbieders en externe dienstverleners, vinden in deze norm eisen en richtlijnen m.b.t. de registratie van gegevens rond de toegang tot het *elektronisch patiëntdossier*.

Deze norm maakt aan ontwikkelaars van *informatiesystemen* duidelijk welke gegevens er in de *logging* aanwezig moeten zijn en wat de cardinaliteit en optionaliteit van die gegevens is. Bij de aanschaf of bouw van nieuwe applicaties moet rekening worden gehouden met deze norm. Het gebruik van het in hoofdstuk 7 beschreven datamodel voor *logging* kan de uitwisseling van *loggegevens* tussen *zorginstellingen* faciliteren. Met het oog op de hiervoor noodzakelijke systeemontwikkeling is in deze norm aansluiting gezocht bij de specificaties van IETF/RFC-3881 [1], NEN-EN-ISO 12052:2006 en het IHE IT Framework [2], [3].

Voor alle personen van wie *persoonlijke gezondheidsinformatie* wordt verwerkt, biedt NEN 7513 een duidelijk houvast over wat van een *zorginstelling* of andere beheerder van *persoonlijke gezondheidsinformatie* mag worden verwacht als het gaat om het verstrekken van informatie en over wie toegang heeft gehad tot haar of zijn elektronisch patiëntdossier.

Ook externe *toezichthouders* zijn belanghebbenden bij de *logging*. Interne *toezichthouders* behoren tot de *zorgaanbieder* zelf.

0.4 NEN 7513 in relatie tot NEN 7510

NEN 7510-2:2017 schrijft voor dat logbestanden van *gebeurtenissen* die gebruikersactiviteiten, uitzonderingen en informatiebeveiligings*gebeurtenissen* registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld. Logbestanden moeten zijn beveiligd en mogen niet kunnen worden gemanipuleerd. De toegang tot instrumenten voor audits van systemen en audittrajecten moet worden beveiligd om misbruik of compromittering te voorkomen.

Ook vermeldt NEN 7510-2:2017 dat activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en dat de logbestanden behoren te worden beschermd en regelmatig behoren te worden beoordeeld. Daarnaast staat in NEN 7510-2:2017 dat gezondheids*informatiesystemen* die tijdkritische activiteiten voor gedeelde zorg ondersteunen, in tijdssynchronisatiediensten moeten voorzien om het traceren en reconstrueren van de tijdpaden voor activiteiten waar vereist te ondersteunen.

NEN 7510-2:2017schrijft niet precies voor welke *gebeurtenissen* moeten worden gelogd, welke gegevens van die *gebeurtenissen* moeten worden vastgelegd, aan welke kwaliteitseisen het *loggen* en de logbestanden moeten voldoen en hoe lang de logbestanden moeten worden bewaard. NEN 7513 vult daarin NEN 7510-2:2017 nader aan en in.

0.5 Bevoegdheden en toegangsregels

De bevoegdheden die aan *gebruikers* van *informatiesystemen* worden toegekend maken het hun mogelijk het systeem voor hun taken te gebruiken. Niet alle taken zijn tijdig vooraf te voorzien en detaillering van bevoegdheden is beperkt mogelijk. In de praktijk bieden de toegekende bevoegdheden daardoor een zekere speling ten opzichte van de formele toegangsregels. Met formele toegangsregels wordt bijvoorbeeld vigerende wet- en regelgeving bedoeld, en de door de *zorginstelling* opgestelde beleidsregels als onderdeel van de in 5.3 van NEN 7510-1:2017 bedoelde verplichting van een *directie* van een *zorginstelling* om te 'bewerkstelligen dat de verantwoordelijkheden en bevoegdheden voor rollen die relevant zijn voor informatiebeveiliging worden toegekend en gecommuniceerd.'

Ten aanzien van *persoonlijke gezondheidsinformatie* 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 (WGBO) is daarvan een goed voorbeeld.

Medische informatica – Logging – Vastleggen van acties op elektronische patiëntdossiers

1 Onderwerp en toepassingsgebied

NEN 7513 stelt eisen aan de registratie van gegevens rond de toegang tot de totale verzameling van alle elektronisch vastgelegde *persoonlijke gezondheidsinformatie* bij een *zorginstelling* of een andere organisatie die *persoonlijke gezondheidsinformatie* verwerkt. In het kader van deze norm noemen we deze totale verzameling 'het *elektronisch patiëntdossier*'.

NEN 7513 beschrijft de stelselmatige geautomatiseerde registratie van gegevens rond de toegang tot het elektronisch patiëntdossier die controle van de rechtmatigheid ervan mogelijk maakt. NEN 7513 is daarmee ook een uitwerking van hetgeen NEN 7510-2:2017 in 12.4 voorschrijft voor zover het gaat om de verplichting *gebeurtenissen* in *elektronische patiëntdossiers* te *loggen* [2)] en deze te beheren en te beveiligen.

NEN 7513 specificeert de *gebeurtenissen* die worden gelogd en de *loggegevens* die bij een *gebeurtenis* in een *logregel* worden vastgelegd. De *gebeurtenissen* betreffen toegang tot *patiënt*gegevens, toegang tot de *logging* en *gebeurtenissen* die invloed kunnen hebben op de betekenis of de betrouwbaarheid van de *logging*.

De norm specificeert ook het detailniveau 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 zelf staan dan in het patiëntdossier, niet in de *logging*. Voor een aanduiding op welk deel van het *patiëntdossier* de actie heeft plaatsgehad is ruimte in de *logregel* gereserveerd.

NEN 7513 schrijft voor hoe lang logbestanden minimaal en maximaal moeten worden bewaard. NEN 7513 geeft aanwijzingen over de te gebruiken templates van de *logging* voor *cliënten* en *zorginstellingen*, conform wettelijke kaders [3)].

NEN 7513 gaat niet over de *logging* van *gebeurtenissen* in papieren dossiers.

NEN 7513 gaat niet in op de wijze waarop het instrument *logging* wordt ingezet door de belanghebbenden. Ongeautoriseerde toegang tot de *logging* of ongeautoriseerde toegang tot een *elektronisch patiëntdossier* dat met de *logging* is aangetoond, kan en zal mogelijk aanleiding zijn sancties op te leggen aan een overtreder. Deze sancties vallen buiten het toepassingsgebied van deze norm.

NEN 7513 gaat niet in op het gebruik van de *logging* door het toezicht.

Buiten het toepassingsgebied van deze norm valt het *loggen* op technisch systeemniveau bedoeld om de werking en beveiliging van een *informatiesysteem* te volgen, misbruik van het systeem te detecteren en systeemherstel mogelijk te maken na eventuele storingen [4)].

2) Loggen dient niet te worden verward met **in**loggen. NEN 7513 gaat niet over inloggen: De wijze waarop toegang wordt verkregen tot het elektronisch *patiënt*dossier.
3) Die kaders zijn onder meer te vinden in de WBP en in de AVG en in de wet Cliëntenrechten bij elektronische verwerking van gegevens.
4) De specificaties en het gebruik van logbestanden voor deze soorten toepassingen wordt onder meer geregeld in NEN-ISO/IEC 15408-2.

Implementatie van deze 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 worden bepaald voor welke terreinen binnen de organisatie, bijvoorbeeld organisatorische deelterreinen en/of *informatiesystemen*, in welke mate en op welke termijn deze norm zal worden gevolgd.

2 Normatieve verwijzingen

Naar de volgende documenten wordt in de tekst zo verwezen dat de bepalingen ervan geheel of gedeeltelijk ook voor dit document gelden. Bij gedateerde verwijzingen is alleen de aangehaalde editie van toepassing. Bij ongedateerde verwijzingen is de laatste editie van het document (met inbegrip van eventuele wijzigingsbladen en correctiebladen) waarnaar is verwezen van toepassing.

NEN 7510-1:2017 en NEN 7510-2:2017, *Medische informatica – Informatiebeveiliging in de zorg*

NEN-ISO 8601:2005, *Data elements and interchange formats – Information interchange – Representation of dates and times*

NEN-EN-ISO 21298:2017, *Health informatics – Functional and structural roles*

3 Termen en definities

Voor de toepassing van deze norm gelden de volgende termen en definities.

3.1
actie
verwerking in een *informatiesysteem*, in het kader van een *gebeurtenis*

Opmerking 1 bij de term: In het kader van deze norm behoort van een *gebeurtenis* altijd een van de volgende *acties* te worden vastgelegd (zie 7.2.2):

C	Create: het creëren van nieuwe gegevens
R	Read: het lezen van gegevens door een gebruiker of proces
U	Update: het aanpassen van bestaande gegevens
D	Delete: het verwijderen of als verwijderd markeren van gegevens
E	Execute: het starten of stoppen van een proces. Bijvoorbeeld het starten van een proces of het beginnen van een data transfer.

3.2
authenticatie
het verschaffen van zekerheid met betrekking tot de juistheid van een geclaimde karakteristiek, zoals identiteit

[BRON: NEN 7510-1:2017]

3.3
autorisatie
het toekennen van bevoegdheden

[BRON: NEN 7510-1:2017]

Bestelformulier

Stuur naar:

NEN Standards Products & Services
t.a.v. afdeling Klantenservice
Antwoordnummer 10214
2600 WB Delft

NEN Standards Products & Services

Postbus 5059
2600 GB Delft

Vlinderweg 6
2623 AX Delft

T (015) 2 690 390
F (015) 2 690 271

www.nen.nl/normshop

Ja, ik bestel

__ ex. NEN 7513:2018 nl Medische informatica - Logging - Vastleggen van acties op elektronische patiëntdossiers € 0.00

Wilt u deze norm in PDF-formaat? Deze bestelt u eenvoudig via www.nen.nl/normshop

Gratis e-mailnieuwsbrieven

Wilt u op de hoogte blijven van de laatste ontwikkelingen op het gebied van normen, normalisatie en regelgeving? Neem dan een gratis abonnement op een van onze e-mailnieuwsbrieven. www.nen.nl/nieuwsbrieven

Gegevens

Bedrijf / Instelling

T.a.v. O M O V

E-mail

Klantnummer NEN

Uw ordernummer BTW nummer

Postbus / Adres

Postcode Plaats

Telefoon Fax

Factuuradres (indien dit afwijkt van bovenstaand adres)

Postbus / Adres

Postcode Plaats

Datum Handtekening

Retourneren

Fax: 015 2 690 271
E-mail: klantenservice@nen.nl
Post: NEN Standards Products & Services,
t.a.v. afdeling Klantenservice
Antwoordnummer 10214,
2600 WB Delft
(geen postzegel nodig).

Voorwaarden

- De prijzen zijn geldig tot 31 december 2018, tenzij anders aangegeven.
- Alle prijzen zijn excl. btw, verzend- en handelingskosten en onder voorbehoud bij o.m. ISO- en IEC-normen.
- Bestelt u via de normshop een pdf, dan betaalt u geen handeling en verzendkosten.
- Meer informatie: telefoon 015 2 690 391, dagelijks van 8.30 tot 17.00 uur.
- Wijzigingen en typefouten in teksten en prijsinformatie voorbehouden.
- U kunt onze algemene voorwaarden terugvinden op: www.nen.nl/leveringsvoorwaarden.