Raad voor Accreditatie (RvA)

Specifiek Accreditatie-Protocol (SAP) voor certificatie van managementsystemen voor informatiebeveiliging in de zorg volgens NEN 7510-1

Documentcode:	**RvA-SAP-C025-NL**
	Versie 2.2, 14-04-2021

Een Specifiek Accreditatieprotocol (SAP) omschrijft het beoordelingsproces voor een specifieke accreditatie. De algemene RvA-reglementen, beleidsdocumenten en toelichtingen zijn van toepassing op dit SAP. De actuele versie van dit SAP en andere genoemde RvA documenten is te vinden op de website van de RvA. (www.rva.nl).

Inhoud

Inleiding 4

1 Relevante documenten 4

1.1 Norm die voor accreditatie wordt gebruikt 4
1.2 Aanvullende normen 4
1.5 Documenten met betrekking tot de uit te voeren conformiteitsbeoordelingen 4

2 Scope van accreditatie 4

2.1 Zorginstellingen en beheerders van persoonlijke gezondheidsinformatie 5
2.2 Afspraak met schemabeheerder NEN 5

3 Accreditatiebeoordelingen 6

3.1 Te verstrekken documenten 6
3.2 Aard en inhoud van de beoordelingen 6
3.3 Scope van certificatie 7

4 Specifieke aandachtspunten voor de RvA-beoordeling 9

5 Wijzigingen ten opzichte van de voorgaande versie 9

Inleiding

Dit SAP dient in samenhang met SAP-C000 te worden gelezen. In dit SAP worden enkel de ten opzichte van SAP-C000 aanvullende of afwijkende aspecten opgenomen. Dit betekent dat delen van de nummering ontbreken (informatie is dan al te vinden in SAP-C000).

Aangezien NCS 7510 is gebaseerd op ISO/IEC 27006:2015 en de norm NEN 7510-1:2017 is gebaseerd op EN ISO/IEC 27001:2013, kan certificatie voor NEN 7510-1 ook worden beschouwd als certificatie voor EN ISO/IEC 27001:2013 met "Gezondheidszorg in Nederland" als werkgebied en NCS 7510 als schema.

1 Relevante documenten

1.1 Norm die voor accreditatie wordt gebruikt

- EN ISO/IEC 17021-1; Conformiteitsbeoordeling - Eisen voor instellingen die audits en certificatie van managementsystemen uitvoeren.

1.2 Aanvullende normen

Nederlands certificatieschema NCS 7510; Conformiteitsbeoordeling – Eisen aan instellingen die audits ten behoeve van certificatie van informatiebeveiligingsmanagementsystemen in de zorg uitvoeren.

1.5 Documenten met betrekking tot de uit te voeren conformiteitsbeoordelingen

NEN 7510-1; Medische informatica – Informatiebeveiliging in de zorg – Deel 1: Managementsysteem.
Certificatie-instellingen kunnen de volgende NEN-documenten bij certificatie gebruiken:

- NEN 7510-2; Medische informatica - Informatiebeveiliging in de zorg - Deel 2: Beheersmaatregelen;
- NEN 7512; Medische informatica - Informatiebeveiliging in de zorg - Vertrouwensbasis voor gegevensuitwisseling;
- NEN 7513; Medische informatica – Logging – Vastleggen van acties op elektronische patiëntdossiers

2 Scope van accreditatie

Accreditatie van certificatie gebaseerd op NEN 7510-1 moet als volgt in de EN ISO/IEC 17021-1-scope van accreditatie worden opgenomen:

- Norm / normatief document: NEN 7510-1;
- Certificatieschema: NCS 7510: Conformiteitsbeoordeling – Eisen aan instellingen die audits ten behoeve van certificatie van informatiebeveiligingsmanagementsystemen in de zorg uitvoeren.

Beschrijving van de cluster:

- Z: Zorginstellingen
- B: Beheerders van persoonlijke gezondheidsinformatie, anders dan zorginstellingen

Een volledige accreditatiescope betekent accreditatie voor cluster Z en cluster B.

2.1 Zorginstellingen en beheerders van persoonlijke gezondheidsinformatie

Uitleg over ‘zorginstellingen’ en ‘beheerders van persoonlijke gezondheidsinformatie, anders dan zorginstellingen’, (citaat uit NEN 7510-1):

Een instelling wordt volgens artikel 1 van de Wet kwaliteit, klachten en geschillen zorg (Wkkgz) gedefinieerd als een rechtspersoon die bedrijfsmatig zorg verleent, een organisatorisch verband van natuurlijke personen die bedrijfsmatig zorg verlenen of doen verlenen, alsmede een natuurlijke persoon die bedrijfsmatig zorg doet verlenen. In dit verband wordt ook genoemd de Wet toelating zorginstellingen, die in artikel 5 aangeeft welke organisaties zorg mogen verlenen. Ten derde wordt ook het Interimbesluit forensische zorg genoemd, dat in artikel 1 aangeeft welke zorginstellingen forensische zorg mogen verlenen.
NEN 7510-1 en NEN 7510-2 zijn in ieder geval van toepassing op de zorginstellingen zoals gedefinieerd in bovengenoemde wet- en regelgeving.
Naast de zorginstellingen zelf bestaat de doelgroep van NEN 7510-1 en NEN 7510-2 ook uit andere beheerders van persoonlijke gezondheidsinformatie. Naast de ‘instellingen die zorg verlenen’, zijn er namelijk ook andere organisaties die ten aanzien van persoonlijke gezondheidsinformatie als beheerder optreden. Voorbeelden hiervan zijn zorgserviceproviders, gemeenten en toeleveranciers van zorginstellingen, zoals hostingproviders.

2.2 Afspraak met schemabeheerder NEN

De norm NEN 7510-1:2017 richt zich op de doelgroep van zorginstellingen én andere beheerders van persoonlijke gezondheidsinformatie (zie NEN 7510-1 paragraaf 0.5). Idealiter vormen beide doelgroepen onderdeel van de accreditatieaanvraag door de CBI en rekent de CBI beide doelgroepen tot haar klantenkring. Voor beide doelgroepen zijn echter significant verschillende competenties bij de CBI nodig. Naar analogie met de vaststelling van de scope voor de NEN-HKZ accreditaties van de CBI, en in overleg met de schemabeheerder NEN, wordt een clustering in de scope van accreditatie gehanteerd. In de praktijk heeft dit de consequentie dat een CBI die eerst een accreditatie-aanvraag heeft gedaan voor bijvoorbeeld de doelgroep 'andere beheerders van persoonlijke gezondheidsinformatie', een nieuwe accreditatie (scope-uitbreiding) moet aanvragen indien zij haar scope voor NEN 7510-1 wil uitbreiden naar de andere doelgroep, bijvoorbeeld 'zorginstellingen'. Bovenstaande geeft CBI’s die alleen ‘Beheerders van persoonlijke gezondheidsinformatie” in hun klantenkring hebben de mogelijkheid hun scope van accreditatie te beperken.

Voorbeeld van een beperkte scope.

Norm / Normatief document	**Certificatieschema**
NEN 7510-1 Medische informatica – Informatiebeveiliging in de zorg	NCS 7510: Conformiteitsbeoordeling – Eisen aan instellingen die audits ten behoeve van certificatie van informatiebeveiligings-managementsystemen in de zorg uitvoeren voor cluster B: - Beheerders van persoonlijke gezondheidsinformatie, anders dan zorginstellingen. NCS 7510 is gebaseerd op de ISO 27006.

Voorbeeld van een volledige scope:

Norm / Normatief document	Certification scheme
NEN 7510-1 Medische informatica – Informatiebeveiliging in de zorg	NCS 7510:2018 Conformiteitsbeoordeling – Eisen aan instellingen die audits ten behoeve van certificatie van informatiebeveiligingsmanagementsystemen in de zorg uitvoeren. Voor de clusters Z en B: - Zorginstellingen - Beheerders van persoonlijke gezondheidsinformatie, anders dan zorginstellingen. NCS 7510 is gebaseerd op de ISO 27006.

3 Accreditatiebeoordelingen

3.1 Te verstrekken documenten

Vereisten aanvullend op SAP-C000:

Voor bijwoningen:

- de 'verklaring van toepasselijkheid' van de auditee (SoA; Statement of Applicability);
- referentie naar van toepassing zijnde wettelijke regels en verordeningen (per cluster).

3.2 Aard en inhoud van de beoordelingen

In aanvulling op de algemene regels voor de aard en omvang van de RvA-beoordelingen, zoals vastgelegd in RvA-BR002 en RvA-BR005, gelden voor deze specifieke accreditatie de regels uit onderstaande tabel. De aard en omvang van de beoordelingen hangen af van de aangevraagde scope van accreditatie, een mogelijk reeds bestaande accreditatie en het functioneren van de instelling in het verleden (waar van toepassing).

Methode van beoordelen	Initiële beoordeling	Beoordelingen gedurende de accreditatiecyclus (controles + herbeoordeling)	Scope-uitbreiding(1)
Bijwoning	√ Een initiële audit	√ Minimum: Per cyclus: 1 + 0,2√c (3) per cluster	√ Een initiële of hercertificatie-audit (1)(2) (zie 3.2.1)

(1) Als de certificatie-instelling de fase 1- / fase 2-methode niet heeft toegepast bij andere geaccrediteerde schema's dan is het bijwonen van een volledige fase 1- / fase 2-audit vereist.

(2) Als geen volledige fase 1- / fase 2-audit beschikbaar is zal een herbeoordelingsaudit worden bijgewoond en moet de certificatie-instelling de eerstvolgende volledige fase 1- / fase 2-audit aanmelden als mogelijkheid voor bijwoning.

(3) √c: vierkantswortel van het totale aantal certificaten voor dat cluster, waarbij de uitkomst van de formule in de tabel naar boven afgerond wordt. Dit aantal kan worden verhoogd op basis van factoren genoemd in document IAF MD17, artikel 2.3.3.

3.2.1 Initiële beoordelingen en scope-uitbreidingen

Bij een scope-uitbreiding voor een andere cluster moet de initiële of herbeoordelingsaudit plaatsvinden bij een organisatie die representatief is voor dat cluster.

Opmerking: Zorginstellingen zijn altijd betrokken bij het beheer van persoonsgebonden informatie over gezondheid, maar dit beheer is meestal (gedeeltelijk) uitbesteed. Maar er zijn ook zorginstellingen die persoonlijke gezondheidsinformatie zelf beheren zonder uitbesteding.

Indien een certificatie-instelling een aanvraag indient voor accreditatie voor de volledige scope op basis van een initiële beoordeling dan moet een certificatieaudit worden bijgewoond bij een zorginstelling die haar eigen persoonlijke gezondheidsinformatie beheert (zonder uitbesteding) of moeten twee certificatie-audits worden bijgewoond; één bij een zorginstelling die het beheer van persoonlijke gezondheidsinformatie (deels) heeft uitbesteed. Een tweede audit moet worden bijgewoond bij een organisatie die persoonsgebonden informatie over gezondheid beheert voor zorginstellingen.

Voor een aanvraag voor accreditatie voor cluster B is een bijwoning vereist bij een organisatie die persoonlijke gezondheidsinformatie beheert voor zorginstellingen.
Voor een aanvraag voor accreditatie voor cluster Z is een bijwoning vereist bij een zorginstelling.

3.2.2 Controles en herbeoordelingen

De implementatie van het NEN 7510 certificatie systeem zal bij iedere RvA controle- en herbeoordeling worden geverifieerd. Tijdens de vierjarige cyclus zullen dossiers (dus certificatiedossiers en personele competentie-dossiers) uit alle clusters, waar de CI voor is geaccrediteerd, worden geverifieerd.

3.3 Scope van certificatie

Artikel 8.2.2 van EN ISO/IEC 17021-1: 2015 verklaart dat het toepassingsgebied van de certificatie met betrekking tot de soort activiteiten, producten en diensten (de scope) zoals van toepassing is op elke vestiging, niet misleidend of dubbelzinnig mag zijn.
Daarom moet de scope van certificatie duidelijk maken welke activiteiten, producten of diensten betrekking hebbende op het beheer van persoonlijke gezondheidsinformatie zijn uitbesteed, waarbij de van toepassing zijnde beheersmaatregelen uit de ‘verklaring van toepasselijkheid’ van de auditee worden gespecificeerd.

Beheerders van persoonlijke gezondheidsinformatie, anders dan zorginstellingen, komen in aanmerking voor een NEN 7510 certificaat, indien zij kunnen aantonen dat

1. ze persoonlijke gezondheidsinformatie verwerken, en
2. de Verklaring van Toepasselijkheid zorg-specifieke beheersmaatregelen bevat die relevant zijn voor de verwerking van de persoonlijke gezondheidsinformatie, en die voortvloeien uit de risicobeoordeling van informatiebeveiliging (cl 6.1 van NEN 7510-1:2017).

Indien zorginstellingen een aanvraag indienen voor certificatie voor NEN 7510-1 is het niet acceptabel dat hun scope van certificatie beperkt is tot die delen van de organisatie die niet betrokken zijn bij de primaire gezondheidszorgprocessen.

Dientengevolge zal de scope van certificatie altijd de primaire gezondheidszorgprocessen van de zorginstelling omvatten.

De certificatie-instelling moet tijdens de fase 1 beoordeling toetsen dat aan deze vereisten wordt voldaan.

4 Specifieke aandachtspunten voor de RvA-beoordeling

Wanneer een certificatie-instelling accreditatie aanvraagt voor NEN 7510-1-certificatie kunnen zich verschillende situaties voordoen:

1. De certificatie-instelling heeft al een RvA-accreditatie voor EN ISO/IEC 27001.
2. De certificatie-instelling heeft al een accreditatie van een andere accreditatie-instelling voor EN ISO/IEC 27001.
3. De certificatie instelling heeft geen accreditatie voor EN ISO/IEC 27001.

Situatie 1:
In deze situatie worden een documentenbeoordeling en een bijwoning van een certificatieaudit (zie boven) uitgevoerd;

Situatie 2:
In deze situatie worden een documentenbeoordeling, een kantooronderzoek en een bijwoning van een certificatieaudit (zie boven) uitgevoerd;

Situatie 3:
In deze situatie worden een vooronderzoek, een kantooronderzoek en een bijwoning van een certificatie-audit (zie boven) uitgevoerd;

Opmerking:
Paragraaf 9.1.4 van EN ISO/IEC 17021-1:2015 geeft duidelijk aan dat de CBI gedocumenteerde procedures moet hebben voor het bepalen van de audittijd, rekening houdend met de grootte en het aantal locaties, hun geografische locaties en overwegingen indien de audit meerdere vestigingen omvat.

Met betrekking tot multi-site moet deze gedocumenteerde procedure rekening houden met de vereisten van zowel NCS 7510 als IAF MD1 waarbij de vereisten van NCS 7510 prevaleren boven de vereisten van IAF MD1.

5 Wijzigingen ten opzichte van de voorgaande versie

Ten opzichte van versie 2.1 van 12 februari 2021 zijn de volgende wijzigingen opgenomen:

- 3.3 begrip interfaces met toelichting verwijderd,
- 3.3 beschrijving van beheerder verduidelijkt.