Checklist NEN7510

Eén van de eerste stappen van het gestructureerd verbeteren van informatiebeveiliging en het implementeren van de NEN7510 omvat het bepalen van de status van de naleving van de NEN7510. Dit kan worden gedaan met behulp van onderstaande checklist.

Bij iedere vraag kan met 'ja', 'nee' of 'gedeeltelijk' worden geantwoord. 'Ja' betekent dat de maatregel volledig volgens de norm aanwezig is, is ingevoerd en wordt nageleefd. 'Nee' betekent dat dit (nog) niet het geval is. 'Gedeeltelijk' kan inhouden dat de maatregel wellicht in opzet wel aanwezig is, maar nog niet wordt nageleefd of dat delen van de instelling zich wel houden aan deze norm, maar andere delen nog niet. In het veld van de opmerkingen kan een toelichting op het gegeven antwoord worden opgenomen. Op deze manier ontstaat een checklist van mogelijke verbetermaatregelen op de plaatsen waar geen antwoord 'ja' kan worden gegeven.

Checklist NEN7510, Informatiebeveiliging in de mondzorgpraktijk		
Vraag	**Ja / Nee / Gedeeltelijk**	**Opmerking**
Beveiligingsbeleid		
1. Beschikt de praktijk over een beleidsdocument voor informatiebeveiliging?		
2. Vindt periodiek een beoordeling en evaluatie plaats van het informatiebeveiligingsbeleid?		
Organiseren van informatiebeveiliging		
3. Zijn de verantwoordelijkheden voor informatiebeveiliging toegewezen binnen de praktijk?		
4. Beschikt de praktijk over een bron voor specialistisch advies op het gebied van informatiebeveiliging?		
5. Zijn de verantwoordelijkheden voor de bescherming van individuele gegevens en voor het uitvoeren van bepaalde beveiligingsprocedures duidelijk gedefinieerd en belegd?		
6. Worden de juiste contacten onderhouden met communicatiepartners (zoals leveranciers van informatiediensten, telecommunicatiebedrijven en andere zorginstellingen) om ervoor te zorgen dat in geval van een incident snel de benodigde actie kan worden ondernomen en advies kan worden ingewonnen?		
7. Wordt de implementatie van informatiebeveiliging periodiek, en bij belangrijke wijzigingen, door de praktijkeigenaar beoordeeld?		
8. Worden de risico's bepaald die ontstaan doordat externe gebruikers toegang hebben tot informatieverwerkende voorzieningen en worden hiertegen de juiste maatregelen genomen?		
9. Zijn beveiligingsvoorwaarden en bijbehorende sancties gespecificeerd in contracten met derden die betrekking hebben op de toegang tot de informatieverwerkende voorzieningen van de instelling?		

Checklist NEN7510, Informatiebeveiliging in de mondzorgpraktijk		
Vraag	**Ja / Nee / Gedeeltelijk**	**Opmerking**
Beheer van middelen voor de informatievoorziening		
10. Is er een overzicht van de middelen die worden gebruikt voor de informatie-voorziening?		
11. Zijn voor alle gegevens en overige middelen de verantwoordelijken bepaald en vastgelegd?		
12. Maakt de praktijk gebruik van classificatie van gegevens, teneinde het vereiste beveiligingsniveau te kunnen aangeven?		
13. Zijn passende procedures opgesteld voor het classificeren en verwerken van gegevens, overeenkomstig het classificatiesysteem?		
Beveiligingseisen t.a.v. personeel		
14. Zijn de verantwoordelijkheden voor informatiebeveiliging opgenomen in de functieomschrijving?		
15. Heeft de praktijkeigenaar bepaald welk toezicht nodig is voor nieuw en onervaren personeel dat geautoriseerd is voor toegang tot gevoelige systemen?		
16. Worden werkzaamheden van medewerkers periodiek onderworpen aan een beoordelings- en goedkeuringsprocedure?		
17. Worden sollicitanten “gescreend” alvorens zij worden aangenomen?		
18. Is in het arbeidscontract opgenomen dat de medewerker een verantwoordelijkheid heeft betreffende informatiebeveiliging?		
19. Is vastgesteld en gewaarborgd dat personen die onder de wettelijke zwijgplicht vallen daarvan op de hoogte zijn?		

Checklist NEN7510, Informatiebeveiliging in de mondzorgpraktijk		
Vraag	**Ja / Nee / Gedeeltelijk**	**Opmerking**
20. Moeten eigen en externe medewerkers die gebruik maken van middelen voor de informatievoorziening bij het begin van hun dienstverband een geheimhoudingsverklaring ondertekenen als onderdeel van het arbeidscontract?		
21. Stimuleert de praktijkeigenaar medewerkers, contractanten en externe gebruikers om de vastgestelde beveiligingsmaatregelen en procedures in acht te nemen?		
22. Worden inbreuken op de beveiliging disciplinair afgehandeld?		
23. Zijn de verantwoordelijkheden om het proces van vertrek van medewerkers te begeleiden duidelijk gedefinieerd en belegd?		
24. Wordt met medewerkers die de praktijk verlaten een afsluitingsgesprek gehouden?		
25. Is gewaarborgd dat alle medewerkers en externe partijen bij het beëindigen van hun contract alle nog in hun bezit zijnde eigendommen van de instelling teruggeven en dat toegangsrechten tot informatiesystemen worden ingetrokken?		
Fysieke beveiliging en beveiliging van de omgeving		
26. Worden beveiligde zones en ruimten beschermd door een adequate toegangscontrole, zodat alleen geautoriseerd personeel toegang kan krijgen?		
27. Is bij de keuze en het ontwerp van beveiligde zones en ruimten rekening gehouden met de mogelijkheid van schade door brand, wateroverlast, en andere natuurlijke of door mensen veroorzaakte calamiteiten?		
28. Zijn aanvullende maatregelen en richtlijnen aanwezig om de beveiliging van beveiligde ruimten te kunnen waarborgen?		

Checklist NEN7510, Informatiebeveiliging in de mondzorgpraktijk		
Vraag	**Ja / Nee / Gedeeltelijk**	**Opmerking**
29. Wordt apparatuur zodanig geplaatst en beveiligd dat de risico's van schade en storing van buitenaf en de kansen op ongeautoriseerd toegang of gebruik beperkt zijn?		
30. Is apparatuur beveiligd tegen stroomstoringen en andere elektrische storingen?		
31. Is de voedings- en telecommunicatiebekabeling voor gegevensverkeer en/of voor ondersteunende informatiediensten beschermd tegen interceptie en beschadiging?		
32. Gelden beveiligingsprocedures en beveiligingsmaatregelen ook voor apparatuur die buiten de praktijk wordt gebruikt?		
33. Is er een “clear desk” en “clear screen” beleid ingesteld?		
34. Zijn maatregelen getroffen om te voorkomen dat het personeel zonder toestemming eigendommen van de instelling meeneemt?		
Operationeel beheer van informatie – en communicatievoorzieningen		
35. Zijn schriftelijke procedures opgesteld voor de bediening van alle computersystemen?		
36. Zijn in het geval van het uitbesteden van het beheer van middelen passende beveiligingsmaatregelen met de contractant overeen gekomen en zijn deze opgenomen in het contract?		
37. Worden computer- en netwerkcapaciteitseisen in de gaten gehouden teneinde storingen ten gevolge van een gebrek aan capaciteit te voorkomen?		
38. Zijn er maatregelen ingevoerd voor de preventie en detectie van kwaadaardige programmatuur en zijn er adequate procedures om het bewustzijn van gebruikers te vergroten?		

Checklist NEN7510, Informatiebeveiliging in de mondzorgpraktijk		
Vraag	**Ja / Nee / Gedeeltelijk**	**Opmerking**
39. Worden regelmatig reservekopieën gemaakt van essentiële gegevens en programmatuur?		
40. Zijn adequate maatregelen getroffen voor de beveiliging van gegevens in netwerken en de bescherming van de aangesloten diensten tegen ongeautoriseerde toegang?		
41. Zijn er procedures voor het beheer van verwijderbare media zoals externe schijven, diskettes, usb sticks en (medische) dossiers?		
42. Worden media op een veilige en beveiligde manier afgevoerd wanneer zij niet langer nodig zijn?		
43. Zijn procedures opgesteld voor de behandeling en opslag van media om de erop opgeslagen gegevens te beschermen tegen ongeoorloofde openbaarmaking of misbruik?		
44. Zijn in overeenkomsten met andere partijen beveiligingsmaatregelen met betrekking tot het uitwisselen van gegevens opgenomen?		
45. Zijn er maatregelen getroffen om gegevens tijdens geautomatiseerde gegevensuitwisseling te beveiligen tegen beschadiging, verlies, ongeautoriseerde toegang, misbruik en manipulatie?		
46. Zijn gegevens die in on-line transacties zijn betrokken, beschermd tegen onvolledige overdracht, verkeerd terecht komen, ongeautoriseerde wijziging, ongeautoriseerde openbaarmaking en multiplicatie?		
47. Is aandacht besteed aan de bescherming van de integriteit van programmatuur, gegevens en andere informatie die beschikbaar wordt gesteld via een publiek toegankelijk systeem?		

Checklist NEN7510, Informatiebeveiliging in de mondzorgpraktijk		
Vraag	**Ja / Nee / Gedeeltelijk**	**Opmerking**
48. Is gegarandeerd dat gegevens alleen via elektronische publicatiesystemen worden verkregen in overeenstemming met de wetgeving op het gebied van privacybescherming?		
49. Wordt een goedkeuringsprocedure gevolgd voordat informatie op publiek toegankelijke systemen wordt gezet?		
Toegangsbeveiliging		
50. Zijn duidelijke regels opgesteld met betrekking tot toegangsbeveiliging voor elke gebruiker?		
51. Zijn er procedures opgesteld voor het registreren en afmelden van gebruikers?		
52. Hebben alle gebruikers een unieke gebruikersidentificatie voor persoonlijk gebruik?		
53. Zijn er procedures vastgesteld voor het toewijzen van gebruikersidentificaties?		
54. Beschikt de praktijk over een wachtwoordsysteem om de identiteit van een gebruiker te verifiëren?		
55. Zijn er procedures voor het instellen, wijzigen en intrekken van wachtwoorden?		
56. Verloopt de toegang tot informatiediensten via een veilige inlogprocedure?		
57. Is beeldschermapparatuur waarop gevoelige gegevens worden verwerkt, zodanig opgesteld dat er zo min mogelijk kans op toevallige waarneming is?		
58. Worden gebruikers verplicht om goede beveiligingsgewoontes in acht te nemen bij het kiezen en gebruiken van wachtwoorden?		
59. Zijn gebruikers verplicht ervoor te zorgen dat onbeheerde apparatuur voldoende is beveiligd?		

Checklist NEN7510, Informatiebeveiliging in de mondzorgpraktijk		
Vraag	**Ja / Nee / Gedeeltelijk**	**Opmerking**
60. Is voor inactieve werkstations op locaties met verhoogd risico een time-out voorziening ingesteld?		
61. Wordt de toegang tot gegevens en functies verleend overeenkomstig het toegangsbeleid van de praktijk?		
62. Heeft de praktijk procedures en regels vastgesteld voor de toekenning en intrekking van bevoegdheden?		
63. Wordt de toewijzing en het gebruik van bijzondere bevoegdheden voor noodprocedures, systeembeheer, onderhoud en dergelijke beperkt?		
64. Worden poorten die dienen voor systeemdiagnose ten behoeve van onderhoud op afstand door een beveiligingsmechanisme en een beveiligingsprocedure beveiligd?		
65. Is een beleid opgesteld voor de omgang met mobiele computers welke de risico's behandelt van het gebruik van mobiele computervoorzieningen?		
66. Is beleid geformuleerd voor telewerken en de risico's daarvan?		
Aanschaf, ontwikkeling en onderhoud van informatiesystemen		
67. Worden gegevens die worden ingevoerd in toepassingssystemen gevalideerd op juistheid, volledigheid en mate van actualiteit?		
68. Is een risicoanalyse uitgevoerd om te bepalen of authenticatie voor de verzending van gevoelige gegevens vereist is?		
69. Krijgen leveranciers van programmatuur alleen fysieke of logische toegang wanneer dit nodig is en dan alleen na toestemming van de leiding?		

Checklist NEN7510, Informatiebeveiliging in de mondzorgpraktijk		
Vraag	**Ja / Nee / Gedeeltelijk**	**Opmerking**
70. Worden ingeval van uitbesteding van de ontwikkeling van programmatuur schriftelijke afspraken gemaakt om de kwaliteit van de programmatuur te kunnen waarborgen?		
Continuïteitsbeheer		
71. Beschikt de instelling over een continuïteitsstrategie?		
72. Zijn er plannen ontwikkeld om de bedrijfsactiviteiten na een onderbreking of verstoring in stand te houden of tijdig te herstellen?		
73. Worden continuïteitsplannen regelmatig getest?		
Naleving		
74. Zijn alle specifieke maatregelen en individuele verantwoordelijkheden om aan de wettelijke en contractuele verplichtingen te voldoen gespecificeerd en gedocumenteerd?		
75. Zijn maatregelen geïmplementeerd om belangrijke documenten en informatie tegen verlies, vernietiging en vervalsing te beveiligen?		
76. Voldoen toepassingen waarin gegevens over personen worden verwerkt, aan de Wet Bescherming Persoonsgegevens?		
77. Zijn maatregelen genomen om ervoor te zorgen dat de informatievoorziening van de praktijk alleen voor geautoriseerde doeleinden worden gebruikt?		
78. Worden informatiesystemen regelmatig geaudit op de naleving van beveiligingsnormen?		
79. Worden audits van operationele systemen gepland en goedgekeurd?		
Beveiligingsincidenten		
80. Wordt eenlogboek van bijzondere gebeurtenissen bewaard?		

Checklist NEN7510, Informatiebeveiliging in de mondzorgpraktijk		
Vraag	**Ja / Nee / Gedeeltelijk**	**Opmerking**
81. Houden de systeembeheerders een logboek bij van hun werkzaamheden?		
82. Is er een procedure voor het melden en afhandelen van storingen?		
83. Worden door gebruikers gemelde storingen in computer- of communicatiesystemen geregistreerd?		
84. Is er een procedure vastgesteld voor het melden van incidenten?		
85. Zijn medewerkers ervan op de hoogte gesteld dat zij mogelijke aanwezigheid van een zwakke plek in de beveiliging moeten rapporteren?		
86. Is er een procedure vastgesteld voor de afhandeling van incidenten?		