Bijlage 5

Risicoanalyses NEN 7511-2

1. Doel

Het vastleggen van de wijze waarop de risicoanalyses in het kader van NEN 7511-2 zijn uit te voeren, alsmede de risicoanalyse zelf van een aantal deelgebieden.

2. Afkortingen

CODA	Coördinerend doktersassistente
DA	Doktersassistente
NADA	Nachtdoktersassistente
ANW	Avond Nacht en Weekend
RBS	Relatie Beheer Systeem
SLA	Service Level Agreement
SSL	Secure Sockets Layer (een encryptieprotocol dat communicatie op het internet beveiligt, door middel van zowel cryptografie als authenticatie. Dit protocol kan ook gebruikt worden om client/server-applicaties te beveiligen tegen bijvoorbeeld afluisteren).
LSP	Landelijk Schakelpunt

3. De risicoanalyse

3.1 Inleiding

Binnen de NEN 7511-2 wordt om een aantal risicoanalyses gevraagd. Doel van de risicoanalyses is het signaleren en onderkennen van de risico's, het maken van keuzes t.a.v. deze risico's en het treffen van maatregelen voor deze risico's.
Het is zaak de risicoanalyses periodiek te herzien en te beoordelen of de maatregelen tot het gewenste resultaat hebben geleid of bijgesteld dienen te worden. Dit kan afhankelijk zijn van veranderende situaties/inzichten.

3.2 Werkwijze

De CIHN heeft ervoor gekozen voor twee processen een uitgebreide risicoanalyse uit te voeren: de telefonie en het patiëntenregistratiesysteem. Hiervoor is een risicoanalyse methode beschreven (zie bijlage 4) die uitgaat van drie kenmerken: beschikbaarheid, integriteit en veiligheid (BIV). Het risico wordt beschreven als het effect (van een bepaalde fout) keer de kans dat deze optreedt (risico = effect x kans).
Voor beide processen is een risicoanalyse uitgevoerd, zijn conclusies getrokken en risicobeheersmaatregelen vastgesteld. Periodiek worden deze twee risicoanalyses herzien en de maatregelen geëvalueerd.

Voor de andere, in de NEN-norm genoemde, risicoanalyses wordt niet gebruik gemaakt van de bovenstaande uitgebreide methode. Deze risicoanalyses worden in onderliggend document beschreven. Hierbij maken we gebruik van de middelenmatrix (zie bijlage 10). Bij ieder punt komen de volgende aspecten terug: kans, effect, risico, getroffen risicobeheersmaatregelen, en vervolgens de evaluatie hiervan. De risicoanalyses in dit document zullen periodiek gereviseerd worden. Daarbij schatten we kansen en effect opnieuw in, evalueren we maatregelen en nemen we eventueel nieuwe maatregelen. Jaarlijks herzien we het document en passen we het aan.

3.3. Risicoanalyse per deelgebied

Hieronder staat per NEN-norm onderdeel beschreven hoe ermee om te gaan.

3.3.1 Misbruik van en ongeautoriseerde toegang tot gegevens en informatie door derden (NEN-norm 6.2.1a)

Te onderscheiden:

a. Fysieke toegang
b. Logische toegang (tot gegevens, bestanden, informatiesystemen)
    - Patiëntregistratiesysteem
    - Archiveringsbestanden
    - Opnameapparatuur voor telefoongesprekken
    - Relatiebeheersysteem
    - Personeelsinformatiesysteem
    - overige

3.3.2 Gecontinueerd toegang tot gegevens bij beëindiging van aanstelling personeel of beëindiging van relatie met externe gebruiker (NEN-norm 8.3.2)

Denk hierbij aan toegang tot bovenstaande (3.3.1) onderdelen, de fysieke toegang, de UZI-passen en dergelijke (zie bijlage 12, over de autorisatie en toegangsrechten).

3.3.3 Fysieke beveiliging van omgeving (NEN-norm 9.1.1) en identificeren van beveiligde zones voor personeel en/of apparatuur (NEN-norm 9.1.2)

De HAP van de CHN kent drie posten, met drie verschillende situaties. In alle gebouwen kennen we drie zones, te weten openbaar, niet openbaar en gesloten.

a. Openbaar: er zijn ruimtes die vrij toegankelijk zijn voor patiënten en medewerkers (ingang, gang, wachtkamer, patiëntentoilet)/
b. Niet openbaar: dit zijn o.a. ruimtes die alleen toegankelijk zijn met een hulpverlener (bijv. spreek-/behandelkamer, lab) of ruimtes die alleen voor de hulpverleners toegankelijk mogen zijn (belcentrale, balieruimte, medicatiekast, rustruimten).
c. Gesloten: ruimten die alleen met speciale sleutels toegankelijk zijn (routerruimte/ serverruimte, voorraadkamer of ruimtes waar overdag gewerkt wordt).

Beschrijf waar nodig ook de ruimtes met papieren informatie, kasten, plaatsing van servers, et cetera.

3.3.4 De keuze van wijze van authenticatie (NEN-norm 11.2.3a)

- Patiëntregistratiesysteem → keuze voor UZI-passen;
- Archiveringsbestanden;
- Opnameapparatuur voor telefoongesprekken;
- Relatiebeheersysteem
- Personeelsinformatiesysteem

3.3.5 Bedrijfskritische systemen en privacygevoelige gegevens eventueel in aparte netwerken onderbrengen (NEN-norm 11.4.2)

- Patiëntregistratiesysteem;
- Archiveringsbestanden;

- Opnameapparatuur voor telefoongesprekken;
- Relatiebeheersysteem;
- Personeelsinformatiesysteem.

3.3.6 Beveiligingsvoorschriften betreffende nieuwe en/of gewijzigde systemen (NEN-norm 12.1.1a)

Op nieuwe of aangepaste informatiesystemen is beveiliging van toepassing. Maatregelen moeten door een risicoanalyse worden geïdentificeerd. Daarbij wordt op de aspecten beschikbaarheid, integriteit en vertrouwelijkheid gekeken naar:

a. Wettelijke eisen.
b. Afspiegeling van de waarde die de instelling hecht aan het betreffende informatiesysteem.
c. De mogelijke schade als gevolg van falen of ontbreken van beveiliging.

3.3.7 Bepalen van de strategie m.b.t. bedrijfscontinuïteit (NEN-norm 13.1.2a)

De kernactiviteit van de CHN is het telefonisch beantwoorden van medische vragen van patiënten in de ANW-zorg. Op basis van verzoeken wordt een verrichting uitgevoerd die varieert van telefonisch consult tot consult of visite. Essentiële onderdelen in dit proces zijn: gebouwen, telefooncentrale, patiëntenregistratie en -planning, triagisten, huisartsen, internetverbinding, medicatie en huisartsenauto’s met chauffeur. In de leveranciersbeoordeling zijn deze onderdelen ook onder andere als kritische leveranciers vastgesteld.