

PROVISIOR & NEN 7510

NEN 7510 De norm NEN 7510 gaat over informatiebeveiliging binnen de zorgsector: het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van alle informatie die benodigd is om patiënten verantwoorde zorg te kunnen bieden.

Naast het borgen van deze kwaliteitscriteria vereist deze norm ook dat de informatiebeveiligingsmaatregelen op controleerbare wijze zijn ingericht voordat kan worden gesproken over adequate informatiebeveiliging. De norm dient primair als kader, waarbinnen elke belanghebbende de voor zijn/haar proces relevant geachte informatiebeveiliging moet specificeren, inclusief de daarbij behorende maatregelen.

HET VEEL VOORKOMENDE MISVERSTAND

Software hoeft niet te voldoen aan NEN 7510. De zorginstelling dient te voldoen aan NEN 7510. De instelling stelt een pakket van eisen op en legt dit voor bij de softwareleverancier. De leverancier moet, via specificaties, kunnen aantonen dat hij kan voldoen aan de gestelde eisen.

PROVISIOR = AUTORISATIEBEHEER

Informatiebeveiliging betreffende de vertrouwelijkheid van gegevens is onder andere te regelen met goed autorisatiebeheer. Er zijn in de norm enkele specifieke hoofdstukken opgenomen die gaan over autorisaties. Twee van de elf hoofdstukken* uit de norm hebben betrekking op autorisaties.

H8: BEVEILIGINGSEISEN TEN AANZIEN VAN PERSONEEL

8.1.1 Functies en verantwoordelijkheden

In de functieomschrijving moet standaard een onderdeel zijn gewijd aan het aspect informatiebeveiliging. Het gaat daarbij om de volgende onderdelen: rollen, verantwoordelijkheden en beveiligingseisen.

8.3.1 Verantwoordelijkheden bij vertrek van medewerkers

8.3.2 Risico van toegang tot gegevens

8.3.4 Intrekken van toegangsrechten

H11: TOEGANGSBEVEILIGING

11.1.1 Beleid ten aanzien van toegangsbeveiliging (TB)

Op basis van deze toegangsvoorschriften moet de TB handen en voeten krijgen in de vorm van maatregelen en procedures. Zo worden in paragraaf 11.3.1 de autorisatieregels er van afgeleid.

11.2 Identificatie en authenticatie

11.2.1 Registratie van gebruikers

Adequate TB valt of staat met weten wie de gebruikers zijn. Het is daarom essentieel dat iemand wordt geautoriseerd, hij wordt geregistreerd (lieft centraal). De organisatie moet daartoe procedures voor het aan- en afmelden van van gebruikers in het register:

11.2.2 Gebruikersidentificatie

Elke geregistreerde gebruiker dient een unieke gebruikersidentificatie te krijgen, die slechts persoonsgebonden dan wel persoonlijk mag worden gebruikt. Groepsaccounts en dergelijke zijn dus verboden!

11.2.3 Keuze van authenticatiewijze

11.2.4 Beheer van identificatie-/authenticatiesystemen

11.2.6 Gebruik van wachtwoorden en authenticatiemiddelen

11.3 Autorisatie en toegangscontrole

11.3.1 Autorisatieregels

11.3.2 Autorisatieproces

De organisatie moet procedures voor het toekennen en intrekken van autorisaties: Denk verder aan zaken als Identity & Access Management en Role-based Access Control.

11.3.3 Toegang tot gegevens en systemen

VRAGEN

- Hebt u een autorisatieproces dat gekoppeld is aan het functieprofiel binnen uw organisatie?
- Hoe houdt u hierbij rekening met het in-, door- en uitstroombproces van uw medewerkers?