Geachte heer/mevrouw,

Namens de Nederlandse Federatie van Universitaire Medische Centra (NFU) geven wij een reactie op het concept van de Cyberbeveiligingswet (hierna: Cbw) die op 21 mei 2024 in consultatie is gegaan. Als NFU willen we drie specifieke aandachtspunten naar voren brengen. Verder geven we in de bijlage een overzicht van een aantal korte vragen of bevindingen die voortkomen uit het wetsvoorstel of de bijbehorende memorie van toelichting. De NFU vraagt in het bijzonder aandacht voor:

1. Risicogebaseerd (blijven) werken en aansluiting zoeken bij bestaande kaders
2. (On)duidelijkheid omtrent parameters significante incidenten
3. Onzekere positie onderzoek en onderwijs

Risicogebaseerd (blijven) werken en aansluiting zoeken bij bestaande kaders

UMC's en overige zorginstellingen in Nederland ervaren op diverse assen reeds een hoge mate van compliance druk waarbij we de naleving actief moeten aantonen via bijvoorbeeld certificeringen. Voor informatieveiligheid is dit de NEN7510 norm. De NEN7510 norm is risicogebaseerd en werkt via een Information Security Management System (ISMS). Op basis hiervan worden beslissingen, zoals het treffen van maatregelen, genomen door te kijken naar de waarschijnlijkheid en impact van potentiële risico's in de context van de organisatie.

De laatste jaren zien we een (Europese) ontwikkeling ontstaan die steeds meer een ruled-based benadering hanteert. Hiermee neemt de compliance druk verder toe. Waardoor de ruimte om primaire taken als zorg, onderzoek en onderwijs uit te voeren ook steeds verder onder druk komen te staan. Andere ontwikkeling is dat toezicht(houders) of auditoren niet altijd vertrouwen op uitgegeven certificeringen of voortbouwen op elkaars waarnemingen en daarom een eigen normenkader of aanvullende set aan maatregelen opleggen.

In de memorie van toelichting is onder 5.3.5. opgenomen dat via AMvB maatregelen kunnen worden opgenomen die een hoger cyberbeveiligingsniveau borgen en dat naar verwachting hier gebruik van zal worden gemaakt. Als NFU roepen we op om hier terughoudend mee te zijn en juist aan te sluiten bij de bestaande risicogebaseerde kaders zoals de NEN7510 en niet met zelfstandige maatregelen te komen die separaat getoetst of gecertificeerd dienen te worden.

(On)duidelijkheid omtrent parameters significante incidenten

In de huidige versie van de Cbw zijn nog geen specifieke parameters opgenomen die bepalen wanneer sprake is van een 'significant incident'. Deze parameters worden op een later moment gepubliceerd via een Algemene Maatregel van Bestuur (AMvB). Het thans nog ontbreken van deze parameters vormen een beperkende factor t.a.v. het (tijdig) kunnen implementeren van de Cbw in bestaande (incident)processen.

In de memorie van toelichting lezen we verder dat het Nationaal Cyber Security Centrum (NCSC) een inschatting maakt over de totale incidenten die onder de Cbw zouden komen te vallen. Het zal daarbij gaan om +/- 1000 per jaar. Deze inschatting roept vragen op. Met name omdat juist de parameters voor het melden van significante incidenten ontbreken en er groot aantal nieuwe entiteiten onder de Cbw komen te vallen. De zorgsector in beschouwing nemende gaat het om +/- 1500 entiteiten die onder de Cbw komen te vallen. Nu het NCSC verwacht dat er in totaal 1000 incidenten per jaar zullen zijn, betekent dit dat er alleen al binnen de zorgsector minder dan één incident per instelling per jaar zou zijn. Gezien de complexiteit en de aard van de hedendaagse cyberdreigingen, lijkt deze schatting mogelijk te laag.

Zonder duidelijke en specifieke criteria voor wat als een 'significant incident' wordt beschouwd, is het moeilijk te begrijpen hoe het NCSC tot deze schatting is gekomen. Laat staan om deze schatting als leidend onderdeel op te nemen t.a.v. het bepalen van de regeldruk uit dit wetsvoorstel.

Als NFU roepen we primair op om de aangekondigde AMvB separaat ter consultatie aan te bieden zodat entiteiten die onder de Cbw vallen ook de mogelijkheid krijgen om hier formeel op te kunnen reageren.

Secundair roepen we op om bij de bepaling van de parameters deze af te stemmen met de entiteiten uit de sectoren. Zodat een toepasbare set aan parameters ontstaat die ook door de sectoren kunnen worden gedragen.

Onzekere positie onderzoek en onderwijs

Naast de ziekenhuisfunctie hebben de UMC's nog drie andere publieke taken: de zorg voor topreferente patiënten, het verrichten van wetenschappelijk onderzoek en het opleiden van de zorgprofessionals van de toekomst. Alleen voor de kerntaak zorg/ziekenhuisfunctie worden de UMC's aangewezen als essentiële entiteit onder de Cbw.

In de NIS2 lezen we dat onderwijsinstellingen met name als ze kritieke onderzoeksactiviteiten uitvoeren ook onder de richtlijn kunnen vallen, mits deze worden aangewezen door de Minister van Onderwijs, Cultuur en Wetenschap. Als UMC's voldoen we met al onze kerntaken aan de criteria van onderwijs en onderzoek. Als we de details in de memorie van toelichting echter lezen zien we een verwijzing naar artikel 1.1. onder g Wet op hoger onderwijs en wetenschappelijke onderzoek (hierna: WHW). In het betreffende artikel wordt verwezen naar de in de bijlage behorende bij de WHW. Daar staan de UMC's opgesomd maar niet vallende onder de definiëring zoals is aangegeven in artikel 1.1. onder g WHW. De UMC's zijn namelijk gedefinieerd onder artikel 1.13 WHW met een verwijzing naar dezelfde bijlage.

Naar het oordeel van de NFU is dit een omissie in het huidige wetvoorstel. Naast artikel 1.1 onder g WHW zou namelijk ook een verwijzing moeten plaatsvinden naar artikel 1.13. WHW zodat UMC's ook voor de overige kerntaken (onderwijs/onderzoek) formeel aangewezen kunnen worden als belangrijke/essentiële entiteit onder de Cbw.

Een aanwijzing vanuit de Minister van Onderwijs, Cultuur en Wetenschap is voor de UMC's niet bezwaarlijk. De UMC's maken namelijk op dit moment bij de inrichting en toepassing van Informatieveiligheid/cyberweerbaarheid geen onderscheidt tussen de drie kerntaken. Het niet aanwijzen vanuit de Minister van Onderwijs, Cultuur en Wetenschap zou er toe leiden dat (incident)processen voor iedere kerntaak juist anders moet worden ingericht omdat straks maar een deel onder de reikwijdte van de Cbw zal vallen.

De NFU roept daarom op om voorgaande in het wetsvoorstel te corrigeren en te overwegen om de UMC's aan te wijzen als essentiële/belangrijke entiteit binnen de sector onderwijs/onderzoek zodat daarmee alle kerntaken onder de reikwijdte van de Cbw vallen.

Tot slot is in de bijlage van deze consultatiereactie een korte lijst opgenomen met overige vragen en bevindingen uit het wetsvoorstel en de memorie van toelichting.

Namens de NFU / UMC's van Nederland,

mr. Sander Vols

Chief Information Security Officer (CISO), Radboudumc

Bijlage: Overige vragen en bevindingen

Wetvoorstel:

- **Algemeen:** Als UMC's werken we met patiëntdata / bijzondere persoonsgegevens. We vragen om aandacht voor de verwerking van zeer gevoelige gegevens door de betrokkenen (o.a. CSIRT, toezichthouder, etc.).
- **Algemeen:** De definitie en omschrijving van een incident is nog onduidelijk en niet SMART beschreven
- In artikel 29,30 en 31 Cbw: wordt aangegeven dat een incident moet worden gemeld aan het CSIRT en aan de bevoegde autoriteit. Het is niet duidelijk of de inhoud van de rapportage naar beide betrokkenen kan verschillen.
- Artikel 32, lid 1, Cbw: het is onduidelijk wat wordt bedoeld met 'onverwijld' en wat de inhoud van de melding zou moeten zijn aan ontvangers van diensten.
- In artikel 36 Cbw: is sprake van de 'coördinator'. Kan deze coördinator of instantie wel onafhankelijk opereren.
- Hoofstuk 16 toezicht en handhaving: artikel 67 e.v. Wat betreft de UMC's is het niet de bedoeling een nieuw toetsingskader binnen de zorg te introduceren, maar de NEN 7510 van toepassing te verklaren als leidend principe. Dit is ook niet in overeenstemming met een risicogebaseerde aanpak die reeds wordt toegepast binnen de zorgsector in Nederland. Wij opteren dan ook voor het 'pas toe of leg uit' principe in plaats van opgelegde verplichte maatregelen.

Memorie van Toelichting

- Paragraaf 5.3.5, hierin wordt de mogelijkheid beschreven om via delegatie aan essentiële en belangrijke entiteiten op te leggen dat zij bepaalde ICT-producten, ICT-diensten en ICT-processen gebruiken die zijn gecertificeerd op grond van artikel 49 van de Cyberbeveiligingsverordening (EU) 2019/881 (Cybersecurity Act (CSA). Indien deze mogelijkheid wordt toegepast zal deze de regeldruk en kosten binnen de zorg verhogen.
- Paragraaf 5.7.6. In deze paragraaf wordt de beveiligingsscan als instrument voor de toezichthoudende instantie uiteengezet. Als UMC's vragen wij ons wat het nut en de noodzaak is van deze beveiligingsscan.
- Paragraaf 8.1.3, Waar op zijn de hier genoemde getallen, zoals 1.000 incidenten en 480 minuten gebaseerd? Dit kan per incident, sector verschillen en is naar het idee van de UMC's niet goed te onderbouwen.