Proud Nerds

Whitepaper
Verwerken persoonlijke gezondheidsinformatie op een website

Kenmerk: 2024020HNMG - Whitepaper - verwerken persoonlijke gezondheidsinformatie op website.docx

Auteur: M.A Geurts

Datum: 3 april 2024
Versie: 1.0
Classificatie: Openbaar

Persoonlijke gezondheidsinformatie op een website

Voor wie: Alle zorginstellingen in Nederland, denk aan ziekenhuizen, zorginstellingen, GGD's of huisartspraktijken

Het beschermen van gezondheidsinforamtie op je website is een wettelijke verplichting. Maar, het is meer dan dat. Het is ook cruciaal voor het behouden van vertrouwen, het voorkomen van datalekken en het beschermen van jullie patiënten of cliënten tegen identiteitsdiefstal.

Omdat het beveiligingen van informatie niet makkelijk is, heeft het Nederlands Normalisatie-instituut de NEN7510 opgesteld. Deze norm is specifiek gericht op de beveiliging van gezondheidsinformatie. Het is in Nederland voor alle zorginstellingen verplicht om zich aan de NEN7510 te houden. Daarnaast is ook de algemene verordening gegevensbescherming (AVG) van toepassing. In dit artikel ga ik kijken wat dit concreet betekent voor jouw website. In deze whitepaper lees je over het volgende:

1. Wat is persoonlijke gezondheidsinformatie?

Als we het over gezondheidsinformatie hebben dan maken we onderscheid tussen persoonlijke gezondheidsinformatie (PHI) en openbare gezondheidsinformatie. Dit artikel richt zich op persoonlijke gezondheidsinformatie. Je leest hier hoe je moet omgaan met openbare gezondheidsinformatie.

Als we het hebben over persoonlijke gezondheidsinformatie dan zijn de volgende aspecten van belang:

- **Identificeerbaarheid**: De informatie bevat gegevens die herleidbaar zijn tot een specifiek individu. Dit kan zijn een naam, een geboortedatum, een adres of een identificatienummer.

- **Gezondheidsinformatie**: De informatie bevat gegevens over de gezondheidstoestand of de zorgverlening aan dat individu. Hieronder vallen ook medische uitslagen, betalingen voor gezondheidszorg of het koppelen van een individu aan een zorgprofessional.

Voorbeelden van persoonlijke gezondheidsinformatie zijn: medische dossiers, röntgenfoto's, laboratoriumresultaten, verzekeringsinformatie en andere persoonlijke gegevens over gezondheidszorg.

2. Wat heeft dit met jouw website te maken?

Meestal denk je bij persoonlijke gezondheidsinformatie aan (grote) applicaties die door de zorgprofessionals gebruikt worden zoals een EPD of een ECD. Er wordt dan ook niet zo vaak gedacht aan een 'simpele' website. Maar het komt regelmatig voor dat ook websites persoonlijke gezondheidsinformatie verwerken. Denk hierbij aan:

- Aanmeldformulieren (zorginstellingen)
- Afspraak- of intakeformulier voor een behandeling (ziekenhuizen)
- Aandoeningen of de gezondheidstoestand van leden (patiëntverenigingen, lotgenoten organisaties)
- Afspraakformulier voor bijvoorbeeld een 22-weken afspraak of een afspraak voor een griep- of coronaprik (GGD's)
- Formulieren om infectieziekten te melden (GGD's)

In al deze voorbeelden kan persoonlijke gezondheidsinformatie voorkomen. Hiervoor zijn wel beide ingrediënten nodig: een identificeerbaar individu en gezondheidsinformatie.

3. Wat komt er kijken bij het veilig verwerken van persoonlijke gezondheidsinformatie?

Als je persoonlijke gezondheidsinformatie gaat verzamelen waar moet je dan op letten? De NEN7510 en de AVG geven beide goede handvatten hoe je dit op een veilige manier kunt doen. De volgende zaken zijn van belang bij het verzamelen van persoonlijke gezondheidsinformatie:

- **Toestemming en informeren** (AVG)
  Verkrijg expliciete toestemming van individuen voordat je hun PHI verzamelt en verwerkt. Zorg ervoor dat je duidelijk uitlegt hoe je de informatie gaat gebruiken en of/met wie je deze deelt met andere partijen.

- **Bewaren en verwijderen** (AVG & NEN7510)
  Denk na waar je de gegevens opslaat en bewaar de gezondheidsgegevens niet langer dan noodzakelijk. Zorg dat ze daarna veilig vernietigd worden.

- **Beperk de toegang tot de gezondheidsgegevens** (NEN7510)
  Zorg ervoor dat alleen medewerkers die geautoriseerd zijn, toegang hebben tot de gezondheidsgegevens. Zorg er ook voor dat de toegang goed beveiligd is.

- **Zorg voor veilig transport van de gezondheidsgegevens** (NEN7510 & NEN7512)
  De gezondheidsgegevens die op de website verzameld worden zullen naar jouw organisatie verstuurd moeten worden. Hier kan veel mis gaan. Er zal dan ook aandacht besteed moeten worden aan het veilig transporteren van de gegevens.

- **Externe partners** (AVG & NEN7510)
  Als je externe dienstverleners inschakelt, zoals een webbouwer, hostingproviders of analysepartners, zorg dan dat ook zij voldoen aan dezelfde privacy- en veiligheidsnormen.

- **Analyseer de risico's** (AVG)
  Bij het verwerken van persoonlijke gezondheidsinformatie op een website is het vaak nodig om een Data Protection Impact Assessment (DPIA) uit te voeren. Een DPIA staat ook wel bekend als een gegevensbeschermingseffectbeoordeling.

Het is belangrijk om je te realiseren dat het verwerken van persoonlijke gezondheidsinformatie op een openbare website complex is en dat alle aspecten van privacy en beveiliging correct worden behandeld. In de volgende paragrafen wordt verder ingegaan op de verschillende onderdelen en hoe Proud Nerds jou daarbij kan helpen.

3.1 Toestemming en informeren

Vraag altijd om toestemming als je persoonlijke gezondheidsinformatie gaat verzamelen. In de regel doe je dit voordat de gegevens ingevuld worden. De patiënt of cliënt moet begrijpen waarvoor hij toestemming geeft. Maak dus in gebruikelijke taal duidelijk waarvoor je toestemming vraagt! Informeer ook waarom je de (gezondheids)gegevens nodig hebt en hoe je hiermee omgaat. Achteraf moet je namelijk aan kunnen tonen dat de gebruiker toestemming heeft gegeven. Je kan de toestemming dan ook het beste bewaren bij de opgevraagde data.

Proud Nerds gelooft in standaardisatie en hebben daarom een module ontwikkelt om op een juiste manier de gebruiker te informeren, de toestemming te vragen en deze op een correcte wijze te bewaren. Deze module gaat verder dan het standaard toestemmingsvinkje wat je vaak bij formulieren tegenkomt die geen persoonlijke gezondheidsinformatie verzamelen. Zo pseudonimiseren wij bijvoorbeeld de toestemming, wat het nmoeilijker maakt de gegevens te herleiden naar individuen.

3.2 Bewaren en verwijderen

De persoonlijke gezondheidsinformatie moet natuurlijk ergens opgeslagen worden. Aangezien iedere locatie een nieuw risico vormt is het belangrijk dat het aantal locaties waar deze gegevens worden opgeslagen tot een minimum wordt beperkt.

Vaak heb je niet in de gaten waar de gegevens worden opgeslagen. Het kan zomaar zijn dat je je marketing tools, zoals Google Analytics of Hotjar, zo hebt ingesteld dat zij ook gegevens die in formulieren worden ingevuld analyseren en bewaren. Dit is natuurlijk niet wenselijk.

Als je de persoonlijke gezondheidsinformatie ergens opslaat dan wil je ook dat de gegevens zo snel mogelijk weer verwijderd worden als ze, op die plek, niet meer nodig zijn. Wist je dat de gegevens die in het formulier worden ingevuld vaak op de webserver opgeslagen voordat ze verstuurd of opgehaald worden? Bijlagen worden meestal ook nog op andere plekken op de webserver opgeslagen. Het is van belang dat je precies weet waar wat komt te staan en dat er een geautomatiseerd proces is om deze gegevens ook weer te wissen.

Proud Nerds heeft een methode ontwikkelt die het aantal plekken waar de gegevens worden opgeslagen minimaliseert. Middels deze methode wordt de informatie ook automatisch weer verwijderd als het verstuurd of opgehaald is. Ook helpen wij om marketing tools, die gebruikt worden om de website te analyseren, zo in te stellen dat deze geen toegang hebben tot de persoonlijke gezondheidsinformatie.

3.3 Beperk de toegang tot de gezondheidsgegevens

Vaak zijn mensen de zwakste schakel als het om beveiliging gaat. Daarom is het van belang om zo min mogelijk medewerkers toegang tot de persoonlijke gezondheidsinformatie te geven. Vergeet externe partijen hierbij niet, zoals de hostingprovider, de webbouwer, maar bijvoordeeld ook het (marketing)bureau die de analyses uitvoert.

De toegang tot de gezondheidsgegevens moet ook goed beveiligd zijn. Proud Nerds maakt, als het om persoonlijke gezondheidsinformatie gaat, daarom altijd gebruik van individuele accounts en Multi-Factor authenticatie (MFA). Ook worden de gegevens geëncrypt opgeslagen in onze databases en wordt de toegang tot de gegevens gelogd. Zo kun je achteraf altijd zien wie er op welk tijdstip toegang tot de gegevens heeft gehad.

Als de persoonlijke gezondheidsinformatie is opgehaald bij de website, dan zijn deze zaken natuurlijk ook van belang. Op de processen die hierna volgen heeft de webbouwer geen invloed, dat is de verantwoordelijkheid van jullie zelf en de eventuele leveranciers waar de gegevens uiteindelijk terecht komen. Door het volgen van de hierboven genoemde aspecten wordt alles geborgd. Je kan Proud Nerds altijd om advies of assistentie vragen om de vervolgprocessen samen op te zetten en in te richten.

3.4 Zorg voor veilig transport van de gezondheidsgegevens

Veel aanvallen van hackers richten zich op het transport van informatie. Ze proberen bijvoorbeeld af te luisteren of het transport om te leiden via hun eigen servers. Informatie versturen via e-mail is om deze redenen dan ook niet zo veilig. Proud Nerds maakt daarom geen gebruik van e-mail om de persoonlijke gezondheidsinformatie te versturen. Beveiligde e-maildiensten zoals Zivver of Zorgmail kunnen een optie zijn, maar daarmee introduceer je ook een aantal nieuwe zwakke plekken.

Proud Nerds heeft een module ontwikkeld die de ingevulde gegevens geëncrypt opslaat op de webserver. Nadat het formulier is ingevuld ontvangt de zorgorganisatie mail dat er nieuw formulier is ingevuld en dat de gegevens opgehaald kunnen worden. Deze mail bevat een link naar de plek waar de gegevens opgehaald kunnen worden. Voordat de gegevens opgehaald kunnen worden moet eerst ingelogd worden met multi-factor authenticatie. Eventueel kan de verbinding nog verder worden beveiligd zodat de link alleen aangeroepen kan worden vanuit de zorgorganisatie zelf.

Als de data is opgehaald dan wordt deze automatisch verwijderd van de webserver Daarnaast wordt de data ook automatisch verwijderd na het verstrijken van een bepaalde tijdsperiode.

3.5 Externe partners

Als je samenwerkt met externe partners die (mogelijk) bij de persoonlijke gezondheidsinformatie kunnen, dan moet je met hen afspraken maken. Zo mogen partners uiteraard alleen bij de gegevens als dit noodzakelijk is. Je legt deze afspraken vast in een verwerkingsovereenkomst. In deze verwerkingsovereenkomst staan een aantal verplichte juridische zaken en leg je vast welke gegevens de partner mag verwerken. Ook staat in deze overeenkomst dat deze partner gebonden is aan dezelfde beveiligingseisen die de zorgorganisatie zelf hanteert.

3.6 Analyseer de risico’s

De AVG vereist dat er een Data Protection Impact Assessment (DPIA) wordt uitgevoerd als je een mogelijk risicovolle verwerking gaat uitvoeren. Een DPIA is een proces dat helpt om de privacyrisico’s te identificeren, te evalueren en te beheren. In deze DPIA zullen de in dit artikel benoemde punten naar voren komen, maar je mag de DPIA niet overslaan. Je moet achteraf kunnen aantonen dat je goed hebt nagedacht over alle mogelijke (privacy)risico’s en of je de adequate maatregelen hebt genomen om deze te adresseren.

Het uitvoeren van een DPIA is best lastig, al helemaal als als je dit nog nooit gedaan hebt. Proud Nerds heeft hier ervaring mee, ook met het verwerken van persoonlijke gezondheidsinformatie via een website. Proud Nerds heeft dan ook de juiste kennis en ervaring in huis om hierbij kunnen helpen.

4. Hulp nodig bij het online verwerken van persoonlijke gezondheidsinformatie?

Al met al komt er dus best wat kijken bij het verzamelen van persoonlijke gezondheidsinformatie via een website. Maar er zijn gelukkig geen onoverkoombare drempels. Proud Nerds kent valkuilen en kan jou ondersteunen bij een passende inrichting en de bijbehorende procedures en maatregelen.

Wil je meer weten, neem dan contact op met één van onze consultants.