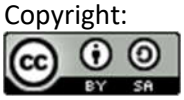
Informatiebeveiliging in huisartsenpraktijken

Een eerste blik op informatiebeveiliging bij huisartspraktijken in de Randstad

Student:	Jeroen Bakker
Identiteitsnummer:	851415519

Datum rapport:	27-02-2018
Datum presentatie:	16-03-2018
Datum einde inschrijving:	22-03-2018

Copyright:



Informatiebeveiliging in huisartsenpraktijken

Een eerste blik op informatiebeveiliging bij huisartspraktijken in de Randstad

Information security in general practices

A first glance at information security in general practices in Randstad

Opleiding:	Open Universiteit, faculteit Management, Science & Technology Masteropleiding Business Process Management & IT
Programma:	Open University of the Netherlands, faculty of Management, Science & Technology Master Business Process Management & IT
Cursus:	IM9806 Afstudeertraject Business Process Management and IT
Student:	Jeroen Bakker
Identiteitsnummer:	851415519
Datum:	27-02-2018
Afstudeerbegeleider:	Hugo Jonker
Meelezer:	Harald Vranken
Versie nummer:	1.0
Status:	definitief

Abstract

Dit empirisch onderzoek creëert een eerste inzicht naar de staat van informatiebeveiliging bij huisartsenpraktijken in de steden Den Haag en Rijswijk. Een zestal diepgaande interviews en vervolgenquêtes liggen ten grondslag aan de resultaten. Het aantal valide reacties op deze enquête was 79. Aanbevelingen zijn gericht op het verhogen van kennis en invoering van processen rondom de NHG-praktijkaccreditering voor het borgen van individuele maatregelen van informatiebeveiliging in de organisatie. Daarnaast is het aannemen van externe hulp bij invulling van informatiebeveiliging binnen de praktijk aanbevolen.

Uit de resultaten kan geconcludeerd worden dat huisartsenpraktijken informatiebeveiliging in hun organisatie zelf veelal op een ad hoc en reactief niveau geregeld hebben en er diverse punten tot verbetering zijn. Als gekeken wordt naar andere onderdelen van de NEN7510 zijn voornamelijk de maatregelen voor personeel onvoldoende toegepast en veelal op basis van vertrouwen, artseneed en jarenlang dienstverband gebaseerd. Waar het gaat om de systemen en patiëntinformatie wordt beheer en onderhoud bijna altijd uitbesteed aan de IT- of applicatieleverancier.

Uit de interview- en enquêteresultaten kan tevens geconcludeerd worden dat alle respondenten de beveiliging van patiëntinformatie uiterst belangrijk vinden en de kosten daarvan minder relevant.

Sleutelbegrippen

Informatiebeveiliging, huisartsenpraktijken, NHG-praktijkaccreditering

“I fear the day when your security requirements kill one of my patients” (Kotz, Fu, Gunter, & Rubin, 2015)

Samenvatting

Doelstelling: Doel van dit empirisch onderzoek is om een eerste inzicht te creëren naar de staat van informatiebeveiliging bij huisartsenpraktijken in de Randstad. Hierbij zal een beeld geschetst worden hoe huisartsenpraktijken informatiebeveiliging op dit moment invullen en zullen aanbevelingen gezocht worden hoe dit verbeterd kan worden.
Methode: Middels een aantal diepgaande interviews wordt een beeld van de huisartsenpraktijk in kaart gebracht. Dit zal met enquêtes worden geverifieerd en is waar mogelijk gegeneraliseerd.
Resultaten: Er zijn voor dit onderzoek zes praktijken geïnterviewd, waarbij één zeer uitgebreid. Hierbij is een beeld ontstaan van de aanwezige inrichting van informatiebeveiliging. Aan de hand van dit beeld is vervolgens een enquête uitgezet waarbij dit beeld getoetst is. Het aantal valide reacties hiervan is 79.
Conclusie en aanbevelingen: Na analyse van de resultaten zijn de conclusies beperkt tot huisartsenpraktijken in regio Den Haag. In andere Randstad steden is een onvoldoende aantal reacties verkregen om conclusies te trekken.
Uit de vergelijking van de resultaten van de interviews en de enquêtes blijkt dat de NHG-praktijkaccreditatie van een huisartsenpraktijk een positieve relatie kan hebben met een goede invulling van alle losse aspecten van informatiebeveiliging binnen de organisatie. Aan te bevelen is dat praktijken de kennis- en processtappen ondernemen die bij een accreditering horen om individuele maatregelen, en de kennis daarover, ten aanzien van informatiebeveiliging beter te borgen in de organisatie.
Ook kan uit de resultaten geconcludeerd worden dat huisartsenpraktijken informatiebeveiliging in hun organisatie zelf veelal op een ad hoc en reactief niveau geregeld hebben en er diverse punten tot verbetering zijn. Als gekeken wordt naar andere onderdelen van de NEN7510 zijn voornamelijk de maatregelen voor personeel onvoldoende toegepast en veelal op basis van vertrouwen, artseneed en jarenlang dienstverband gebaseerd. Waar het gaat om de systemen en patiëntinformatie wordt beheer en onderhoud bijna altijd uitbesteed aan de IT- of applicatieleverancier. Inzicht in uitvoering van dit beheer is echter vaak afwezig binnen de praktijk.
Uit de interview- en enquêteresultaten kan tevens geconcludeerd worden dat alle respondenten de beveiliging van patiëntinformatie uiterst belangrijk vinden en de kosten daarvan minder relevant. Voornamelijk de eigen tijdsinvestering voor onderhoud van systemen en bijhouden van kennis is echter summier en hoogstwaarschijnlijk te weinig om verdere stappen te maken in de informatiebeveiliging binnen de organisatie. Het verder professionaliseren door middel van (de informatiebeveiligingsstappen van) praktijkaccreditatie en het aannemen van externe hulp bij de invulling van informatiebeveiliging binnen de praktijk is daarmee onvermijdelijk.

Summary

Goals: Goal of this empirical study is to create a new insight in the practice of information security inside General Practices in the Randstad (urban agglomeration of 4 largest cities in the Netherlands). This insight will create an image of current practices and can provide recommendations to improve the information security.
Method: With the help of depth interviews a full image is created of the current implementation of information security within General Practices. Through an online survey the results are tested and further generalized.
Results: In this study a total of six General Practices have had a depth interview, where one General Practice has been used to go through the entire NEN7510 certification measure-set. This has created an overview of implemented information security topics. With this overview a survey was held to test this overview. A total of 79 valid reactions have been used for this test.
Conclusions and recommendations: After analysis of the results, the scope of this study must be limited to the region of The Hague. There are not enough results to further generalize this study. Comparing the results of the interviews with the survey, a positive relation between GP accreditation and positive results on individual aspects of the implementation of information security is found. Recommended is that GP's undertake the steps needed to acquire knowledge of and implement new processes that represent individual aspects of NHG-practice accreditation where it involves information security to further secure these aspects in the organization.
Also, it can be concluded that organization of information security is done on an ad hoc and reactive base and that there are several points that can be improved. When the NEN7510 is considered, the topic of personnel is implemented unsatisfactory and mostly done based on trust, the GP's oath and longtime employment. System and patient information is generally under maintenance by an external IT- or application supplier. Insight in the execution of this maintenance is generally unavailable to the General Practice.
Based on the interview and survey results it can be concluded that all respondents find security of patient information very important and costs of this less relevant. Time investment in maintenance of the systems and knowledge upkeep is very low and probably too little to take further steps in improving information security within the organization.
Further professionalization through accreditation and accepting external help for the implementation of information security in the organization seems inevitable.

Inhoudsopgave

1. Samenvatting literatuurstudie

Voorafgaande aan dit empirisch onderzoek is een literatuurstudie uitgevoerd, deze is integraal opgenomen in bijlage 8. Hieronder wordt een samenvatting van deze literatuurstudie besproken om dit empirisch onderzoek in context te kunnen plaatsen.

Aanleiding literatuurstudie
De literatuurstudie is uitgevoerd naar aanleiding van een korte voorstudie naar informatiebeveiliging bij huisartsenpraktijken. Op het gebied van informatiebeveiliging in de zorg is er veel gaande en veel media-aandacht. Er zijn diverse normen en wetten op het gebied van informatiebeveiliging in de zorg. Een onderzoek van de IGZ naar informatiebeveiliging in ziekenhuizen (Inspectie voor de Gezondheidszorg, 2008) laat zien dat niet alle instanties aan de gestelde normen voldeden. Het onderzoek gaf een globaal inzicht in de benodigde kennis en kunde om adequate informatiebeveiliging te regelen binnen een organisatie. Deze kennis lijkt niet aanwezig te kunnen zijn bij kleinere zorgorganisaties als huisartsenpraktijken. Na een kort gesprek met enkele huisartsen is vastgesteld dat informatiebeveiliging niet structureel geregeld is, maar dat het wel wenselijk is om dit beter onder controle te hebben.

Probleemstelling en onderzoeksvragen
Naar aanleiding hiervan is een probleemstelling voor de literatuurstudie opgesteld:
“Is er voldoende managementcapaciteit beschikbaar bij huisartsenpraktijken voor het goed doen van informatiebeveiliging?”

Daarnaast zijn er enkele deelvragen opgesteld om deze probleemstelling te kunnen beantwoorden.

1. Wat is, volgens de wetenschappelijke literatuur, management van informatiebeveiliging binnen de zorgsector?
2. Wat zegt de literatuur over de eisen die gesteld worden aan informatiebeveiliging binnen de zorg?
3. Wat zegt de literatuur over de eisen aan informatiebeveiliging die gesteld worden bij elektronische uitwisseling tussen huisartsenpraktijken?
4. Wat zegt de literatuur over de mate en effectiviteit van inrichting van informatiebeveiliging binnen de zorg?
5. Wat zegt de literatuur over de mate waarin de eisen die gesteld worden aan management van informatiebeveiliging bij huisartsenpraktijken gehaald worden?
6. Wat stelt de literatuur voor als aandachts- en verbeterpunten om te voldoen aan de gestelde eisen?

Onderzoeksaanpak
In het artikel wordt een literatuuroverzicht gegeven waarbij de scope ligt op management van informatiebeveiliging bij elektronische gegevensuitwisseling tussen huisartsenpraktijken.

Er is een verkennend literatuuronderzoek uitgevoerd waarbij in digitale bibliotheken van de OU Bibliotheekcatalogus gezocht is naar literatuur over informatiebeveiliging bij elektronische gegevensuitwisseling tussen huisartsenpraktijken en literatuur die de vraagstellingen van dit literatuuronderzoek ondersteunen om zo reeds gedaan onderzoek in deze richting te kunnen vinden en aan te kunnen sluiten bij de bestaande literatuur.

Aan de hand van de resultaten is uiteindelijk een overzicht gemaakt van de literatuur en zijn de gestelde vragen beantwoord.

Uitvoering
Er is een zoekstrategie bepaald die gebruik maakt van de OU digitale bibliotheken EBSCHOhost, PubMED, Google Scholar, ScienceDirect en SpringerLink. De zoekresultaten zijn aangevuld met resultaten uit de literatuurlijst en suggesties van huisartsen en ICT-bedrijven waarmee gesproken is gedurende het onderzoek.

De zoekresultaten zijn gescand op titel en abstract en gevonden mogelijk relevante artikelen zijn volledig gelezen. Uit de 117 uiteindelijk geselecteerde artikelen is benodigde informatie gehaald en verwerkt in de resultaten.

Resultaten en conclusies
De resultaten zijn in twee onderdelen verwerkt. De metadata, waarbij gekeken zal worden naar wat te zeggen valt over het totaal van gevonden literatuur. De inhoudelijke behandeling van de gevonden literatuur en wat geschreven wordt over management van informatiebeveiliging bij huisartsenpraktijken, wat de voorwaarden zijn voor het goed uitvoeren hiervan en hoe en in welke mate informatiebeveiliging op dit moment wordt beheerst en kan worden verbeterd.

De resultaten op de vragen zijn als volgt:

1. Vraag: Wat is, volgens de wetenschappelijke literatuur, management van informatiebeveiliging binnen de zorgsector?
   Resultaat: Er is onvoldoende literatuur om te generaliseren naar de kleinere zorgsector. Er is voornamelijk literatuur beschikbaar die zich richt op grotere zorgondernemingen als ziekenhuizen.
2. Vraag: Wat zegt de literatuur over de eisen die gesteld worden aan informatiebeveiliging binnen de zorg?
   Resultaat: Er wordt consistent verwezen naar een set wetgeving, standaarden en normen waarop de literatuur modellen voorstelt en implementaties uitwerkt. Er zijn geen “minimale eisen” modellen in de literatuur beschikbaar.
3. Vraag: Wat zegt de literatuur over de eisen aan informatiebeveiliging die gesteld worden bij elektronische uitwisseling tussen huisartsenpraktijken?
   Resultaat: Er zijn in de literatuur geen eisen te vinden. Er is wel wetgeving voor de zorgsector te vinden waar het gaat om eisen aan informatiebeveiliging. Deze wetgeving spreekt over het maken van “passende technische en organisatorische maatregels”.
4. Vraag: Wat zegt de literatuur over de mate en effectiviteit van inrichting van informatiebeveiliging binnen de zorg?
   Resultaat: Bij ziekenhuizen wordt gevonden dat informatiebeveiliging nog wel verbeterd kan worden, echter zijn factoren tijd en kosten een grote beperking. Voor huisartsenpraktijken is geen literatuur gevonden.
5. Vraag: Wat zegt de literatuur over de mate waarin de eisen die gesteld worden aan management van informatiebeveiliging bij huisartsenpraktijken gehaald worden?
   Resultaat: De literatuur laat zien dat het waarschijnlijk niet mogelijk is voor huisartsenpraktijken (en andere kleine zorgorganisaties) om te voldoen aan alle regels en eisen die gesteld worden aan informatiebeveiliging.
6. Vraag: Wat stelt de literatuur voor als aandachts- en verbeterpunten om te voldoen aan de gestelde eisen?
   Resultaat: Er zijn in de zorgsector diverse modellen die kunnen worden toegepast om informatiebeveiliging succesvol binnen een zorgorganisatie te implementeren. Omdat er echter een vraag bestaat of alle eisen wel haalbaar zijn voor kleinere zorgorganisaties, kan gesteld worden dat de literatuur op dit punt niet volledig is.

Conclusie: Gekeken naar de literatuur en de antwoorden op alle deelvragen kan gesteld worden dat de probleemstelling niet kan worden beantwoord. Gebleken is dat er onvoldoende literatuur beschikbaar is om een goed overzicht te maken wat betreft management van informatiebeveiliging bij huisartsenpraktijken. Vanuit de literatuur is er wel voldoende materiaal beschikbaar om te kunnen stellen dat het waarschijnlijk is dat huisartsenpraktijken niet aan alle eisen kunnen voldoen. Gezien de noodzaak van goede informatiebeveiliging van zorgsystemen, die steeds meer koppelingen hebben met andere systemen, is er zeker meer onderzoek nodig op dit vlak.

2. Introductie empirisch onderzoek

In dit hoofdstuk zal een introductie gegeven worden van dit empirisch onderzoek. Ook zullen de context, relevantie, probleemstelling en opdrachtformulering uiteen worden gezet.

2.1. Inleiding

Het onderwerp van dit onderzoek “informatiebeveiliging bij huisartsenpraktijken” is voortgekomen uit het onderzoeksgebied van de afstudeerbegeleider. Hierbij is aangesloten op het onderzoeksgebied IT-security.

Er is steeds meer aandacht voor datalekken in de media en de roep naar veiligheid en privacy klinkt sterk onder de burger. Ook de overheid legt hier steeds zichtbaarder nadruk op, zo ook in de Meldplicht Datalekken (College Bescherming Persoonsgegevens, 2015) die op 1 januari 2016 van kracht is geworden. In de Wet op de Geneeskundige Behandelingsovereenkomst (art. 7:454-456 BW) is dossiervorming wettelijk geregeld. Een van de grootste verzamelingen gevoelige persoonsgegevens is wellicht ons medisch dossier wat het bijna complete medische leven van de Nederlandse burger bevat. Hierbij is goede informatiebeveiliging van alle toegangspunten tot deze informatie dus erg belangrijk.

Hiertoe is een literatuurstudie gedaan met als scope “management van informatiebeveiliging bij elektronische gegevensuitwisseling tussen huisartsenpraktijken”. Uit deze studie is gebleken dat er onvoldoende literatuur beschikbaar is om een goed overzicht te maken wat betreft management van informatiebeveiliging bij huisartsenpraktijken. *Vanuit de literatuur is er wel voldoende materiaal beschikbaar om te kunnen stellen dat het waarschijnlijk is dat huisartsenpraktijken niet aan alle eisen kunnen voldoen. Gezien de noodzaak van goede informatiebeveiliging van zorgsystemen, die steeds meer koppelingen hebben met andere systemen, is er zeker meer onderzoek nodig op dit vlak.*

Dit empirisch onderzoek zal vervolgens invulling proberen te geven aan de vraag naar onderzoek van informatiebeveiliging bij huisartsenpraktijken. Er zal in dit onderzoek getracht worden een start te maken met kenniswerving van informatiebeveiliging bij huisartsenpraktijken.

Om tot deze kennis te komen zal een onderzoeksmethode vastgesteld moeten worden. Hierin zal moeten worden geborgd dat het onderzoek gestructureerd, betrouwbaar en valide is en dat het onderzoek te generaliseren is naar de karakteristieken van de onderzoekspopulatie.

Op basis van de methode zal het onderzoek uitgevoerd worden en resultaten uiteengezet. Met de resultaten zullen vervolgens de deelvragen van dit onderzoek beantwoord worden zodat uiteindelijk ook een conclusie getrokken kan worden ten aanzien van de beantwoording van de vraagstelling van dit onderzoek.

Naast de resultaten en conclusie zal ook worden besproken wat de beperkingen zijn van dit onderzoek. Zo kan de lezer zich een goed beeld vormen van de waarde van dit onderzoek en mogelijkheden tot eventueel vervolgonderzoek.

Als laatste zullen alle referenties worden benoemd en uitwerkingen in de bijlage worden opgenomen, waar deze niet in de tekst passen of deze niet bijdragen aan de leesbaarheid van de tekst maar wel behoren te worden opgenomen in het kader van verantwoording van het onderzoek.

Leeswijzer
Hoofdstuk 1: literatuuronderzoek
Hoofdstuk 2: introductie (context, relevantie, probleemstelling, opdrachtformulering)
Hoofdstuk 3: doel van het empirisch onderzoek
Hoofdstuk 4: methode
Hoofdstuk 5: uitvoering
Hoofdstuk 6: resultaten
Hoofdstuk 7: discussie
Hoofdstuk 8: conclusie en aanbevelingen
Hoofdstuk 9: reflectie
Referenties
Bijlagen

2.2. Context

Dit onderzoek is uitgevoerd als onderdeel van het afstudeertraject van de opleiding Business Process Management & IT aan de Open Universiteit. Het onderwerp van dit onderzoek “management van informatiebeveiliging bij huisartsenpraktijken” is voortgekomen uit het onderzoeksgebied van de afstudeerbegeleider. Hierbij is aangesloten op het onderzoeksgebied IT-security.

Informatiebeveiliging in de zorg gaat in dit onderzoek om het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van alle informatie die benodigd is om patiënten verantwoorde zorg te kunnen bieden.

In dit onderzoek zal de Nederlandse taal worden aangehouden aangezien de te interviewen/enquêteren personen allen Nederlands zijn. Daarnaast zijn overheidspublicaties voor regelgeving en standaarden allemaal in het Nederlands.

Dit onderzoek heeft als doelgroep huisartsenpraktijken in de Randstad. Er is echter geen eenduidige definitie van “Randstad steden” beschikbaar. Daarom zijn voor dit onderzoek de vier grote Randstad steden Amsterdam, Den Haag, Rotterdam en Utrecht genomen, tezamen met alle steden die behoren tot de stadsgewesten en agglomeraties van deze vier Randstad steden.

Het belangrijkste kenmerk hiervan is: grote steden met een groot aantal verstedelijkte gemeenten eromheen. In onderzoeken in Australië is een significant verschil tussen ICT-adoptie in stedelijke en landelijke praktijken gevonden (MacGregor, Hyland, & Harvie, 2009). Omdat de onderzoeker de omgeving zo min mogelijk van invloed wil laten zijn op de resultaten en de verwachting is dat de toegang tot informatie én waarde van informatie bij stedelijke praktijken hoger zal zijn door meer resultaten van gelijksoortige praktijken, zal dit onderzoek zich op stedelijke praktijken richten. Een compleet overzicht van deze steden is in bijlage 1 opgenomen inclusief de gebruikte bronnen voor de samenstelling van deze lijst.

Binnen het onderzoek worden er afkortingen van organisaties gebruikt, welke hier kort zullen worden toegelicht. NHG staat voor Nederlands Huisarts Genootschap. LHV staat voor Landelijke Huisartsen Vereniging en KNMG staat voor Koninklijke Nederlandsche Maatschappij tot bevordering der Geneeskunst. Termen die betrekking hebben op informatiebeveiliging zullen hier niet verder worden toegelicht. De onderzoeker gaat ervan uit dat medeonderzoekers in dit deel van het onderzoeksveld reeds op de hoogte zijn van deze termen. Waar een verdere uitleg op een term of de scope daarvan nodig is, zal dit in de tekst gedaan worden.

2.3. Relevantie

Dit onderzoek tracht via wetenschappelijke en maatschappelijke relevantie een bijdrage te leveren aan zowel wetenschappelijke literatuur als praktijksituaties.

Wetenschappelijke relevantie
In de literatuurstudie is reeds onderkend dat er onvoldoende literatuur op het gebied van informatiebeveiliging in huisartsenpraktijken beschikbaar is. De bestaande literatuur heeft hiermee wel bijgedragen aan de beantwoording van de vragen in het literatuuronderzoek door het inzichtelijk maken van de grenzen van de bestaande literatuur en het identificeren van mogelijke gebreken en/of beperkingen aan de bestaande literatuur. Het empirisch onderzoek zal nu bijdragen aan het leggen van een basis voor verder onderzoek naar informatiebeveiliging bij huisartsenpraktijken.

Praktische relevantie
Door het in de literatuurstudie overzichtelijk weergeven van bestaande literatuur en de grenzen hiervan krijgen zorgondernemingen extra houvast op de gestelde eisen aan informatiebeveiliging bij elektronische gegevensuitwisseling tussen huisartsenpraktijken en kan vervolgonderzoek de beperkingen in de literatuur verder verminderen. De uitkomsten uit het empirisch onderzoek kunnen mogelijk gebruikt worden binnen huisartsenpraktijken als referentiekader voor de invulling, spiegeling en verdere verbetering van de eigen informatiebeveiliging. Tevens kunnen aanbevelingen gebruikt worden als startpunt van aandacht voor de grote hoeveelheid wetten, regels en normen waaraan moet worden voldaan.

2.4. Probleemstelling

Na een vluchtige analyse van het onderzoeksgebied lijkt er een praktijkprobleem te zijn rondom informatiebeveiliging van elektronische gegevensuitwisseling bij huisartsenpraktijken. Het lijkt op dit ogenblik onmogelijk om huisartsenpraktijken te laten voldoen aan de eisen van informatiebeveiliging bij onderlinge gegevensuitwisseling. Daarnaast is er zeer beperkt tot geen onderzoek beschikbaar dat de verschillende managementaspecten van informatiebeveiliging van gegevensuitwisseling bij huisartsenpraktijken bekijkt.

De literatuurstudie die reeds is uitgevoerd bevestigt deze punten. Er is hier vastgesteld dat er onvoldoende literatuur beschikbaar is om op het gebied van informatiebeveiliging bij huisartsenpraktijken conclusies te trekken. Daarnaast is bevestigd dat het voor huisartsenpraktijken onmogelijk lijkt om zich volledig aan alle eisen ten aanzien van informatiebeveiliging te houden.

Er bestaat een vraag naar een verkennend onderzoek naar informatiebeveiliging bij huisartsenpraktijken. In dit empirisch onderzoek zal daarom een eerste inzicht gecreëerd worden naar de staat van informatiebeveiliging bij huisartsenpraktijken.

2.5. Opdrachtformulering

Het doel van het empirisch onderzoek zal zijn om invulling te geven aan de vraag naar onderzoek van informatiebeveiliging bij huisartsenpraktijken. Zoals uit de probleemstelling volgt is er verkennend onderzoek nodig om het onderzoeksgebied informatiebeveiliging bij huisartsenpraktijken verder uit te breiden. Er zal in dit onderzoek getracht worden een start te maken met kenniswerving van informatiebeveiliging bij huisartsenpraktijken.

Vanwege afwezigheid van voldoende onderzoek is een verkennende studie gewenst naar informatiebeveiliging bij huisartsenpraktijken. Dit betekent ook dat de vraagstelling zo geformuleerd zal worden dat een verkennende studie mogelijk is en de onderzoeksmethode(n) op hun beurt afgestemd zullen worden op deze vraagstelling. De reden van afwezigheid van voldoende onderzoek naar informatiebeveiliging bij huisartsenpraktijken is niet beantwoord in de literatuurstudie.

Vraagstelling:

- Welke maatregelen nemen huisartsenpraktijken in het kader van informatiebeveiliging?

Om inzicht te krijgen in de maatregelen die huisartsenpraktijken nemen in het kader van informatiebeveiliging zijn een aantal deelvragen gesteld. Dit komt voort uit het feit dat bekend moet worden welke maatregelen er zijn, welke daarvan relevant zijn, hoe huisartsenpraktijken werken en hoe maatregelen met de werkzaamheden samenhangen.

Via beantwoording van de deelvragen en via deze weg ook van de vraagstelling van dit onderzoek zal een eerste beeld gecreëerd worden naar informatiebeveiliging bij huisartsenpraktijken.

Deelvragen:

1. Hoe vullen huisartsenpraktijken informatiebeveiliging nu in?
2. Wordt dit beeld bevestigd bij een grotere groep?
3. Zijn er verschillen te vinden bij de invulling van informatiebeveiliging tussen huisartsenpraktijken?
4. Zijn er gemeenschappelijke aanbevelingen te vinden die de staat van informatiebeveiliging verder kan bevorderen?

3. Doel van het empirisch onderzoek

Aan de hand van de literatuurstudie is duidelijk dat er hoogstwaarschijnlijk te weinig kennis aanwezig is binnen huisartsenpraktijken voor goede informatiebeveiliging. Middels dit empirisch onderzoek kan worden gekeken hoe huisartsenpraktijken op dit moment invulling geven aan informatiebeveiliging. Er kan zo een beeld gevormd worden van de (on)mogelijkheden binnen huisartsenpraktijken voor adequate informatiebeveiliging. Om te weten of iets adequaat geregeld is, zal je een beeld moeten hebben van een bestaande situatie en de gewenste situatie. Zo kan je een verschil weergeven en een standpunt over ‘goed’ innemen.

Om dit doel te bereiken zal er een antwoord worden gezocht op de vraagstelling en deelvragen uit de opdrachtformulering. Omdat er op dit moment nog geen onderzoek naar de inrichting van informatiebeveiliging in huisartsenpraktijken aanwezig is, zal allereerst gefocust worden op het uitlichten van de inrichting van, activiteiten voor en meningen over informatiebeveiliging die bestaan bij huisartsenpraktijken.

Naast deze focus zal er een controle moeten bestaan, zodat gecontroleerd wordt of de opgedane resultaten ook buiten de focusgroep overeind blijven.

Er zal voor de gewenste situatie uitgegaan worden van bestaande wet- en regelgeving. Hierbij wordt specifiek gekeken naar de NEN7510:2011 (NEN.nl, 2011), omdat deze normering ook tijdens audits aangehouden wordt als toetsingsmiddel door verschillende toetsende organisaties en instanties.

Het onderzoek zal zich via de vraagstelling en bijbehorende deelvragen richten op het creëren van beeldvorming over de bestaande situatie van informatiebeveiliging bij huisartsenpraktijken. Het maken en voorstellen van volledige veranderstrategieën voor de verbetering van de inrichting van informatiebeveiliging bij huisartsenpraktijken is geen onderdeel van het doel van deze studie.

4. Methode

Voor het empirisch onderzoek zullen, vanwege de afwezigheid van voldoende voorgaand onderzoek, inductieve benaderingen gebruikt worden. Er zal een verkennend onderzoek gedaan worden om inzicht te kunnen krijgen in wat er precies op het gebied van informatiebeveiliging in huisartsenpraktijken gebeurt.

In dit hoofdstuk zullen de grove stappen en precieze invulling van het onderzoek verder uiteengezet worden. In de paragraaf onderzoeksstrategie zal worden beschreven hoe het onderzoek in grove lijnen wordt aangepakt. In de paragraaf onderzoeksaanpak zal deze aanpak in detail worden beschreven zodat de volledige werkwijze van dit empirisch onderzoek en afwegingen die daarbij zijn gemaakt beschreven zijn.

4.1. Onderzoeksstrategie

Er kunnen aan de hand van het doel van het onderzoek, aangehouden filosofie en benadering verschillende onderzoeksmethodes (Saunders, Lewis, Thornhill, Booij, & Verckens, 2011) aangehouden worden. De verschillende methodes zijn in bijlage 2 weergegeven, samen met een omschrijving van elke methode.

Voor elke methode (hieronder vetgedrukt aangegeven) is na te gaan of deze gebruikt kan worden binnen dit empirisch onderzoek. Dit aan de hand van de eerder vastgestelde onderzoeksvraagstelling en bijbehorende deelvragen. Hieronder zal per methode een korte uitleg gegeven worden waarom deze wel of niet bruikbaar is voor dit empirisch onderzoek.

Het **experiment** doet onderzoek naar verschillen of samenhang van verschillende situaties. In dit onderzoek is echter geen vergelijkingsmateriaal beschikbaar. Het experiment is niet bruikbaar voor dit onderzoek omdat er een verkenning zal worden uitgevoerd. Het gaat in dit geval dus niet om het gecontroleerd beoordelen van een verandering of maken van een vergelijking maar om het schetsen van een complete situatie.

Het oplossen van problemen in een praktische situatie kan via **'action research'**. Hierbij wordt verandering geïnitieerd om tot een oplossing voor een bepaald probleem te komen. De vraag die de onderzoeker hierbij beantwoord is voornamelijk een hoe-vraag. Deze methode van onderzoek is niet geschikt voor dit onderzoek. Er wordt bij dit onderzoek geen verandering gezocht noch de beschrijving daarvan, wat wel het doel van de onderzoeksmethode 'action research' is.

Er kunnen ook beschrijvingen worden gemaakt van het verleden of over veranderingen via administratieve gegevens en documenten. Hiervoor wordt **archiefonderzoek** gebruikt. Deze methode van onderzoek is niet geschikt voor dit onderzoek omdat er niet wordt gezocht naar situaties uit het verleden, noch naar veranderingen in de tijd.

De **'grounded theory'** wordt gebruikt voor de opbouw van een theorie of model. Hierbij wordt eerst een reeks waarnemingen gedaan, aan de hand waarvan een theorie of model opgezet wordt. Op basis hiervan kunnen vervolgens voorspellingen gedaan worden die bevestigd of ontkracht kunnen worden. Deze methode is voor dit onderzoek niet geschikt, omdat niet wordt gezocht naar het voorspellen of verklaren van gedrag of anderzijds het doen van enige voorspellingen.

Voor het verklarende onderzoek is het mogelijk ook inzichten van de betrokkenen te verzamelen. Dit kan middels de **etnografie** methode. Hierbij verklaar je een bepaalde wetenschappelijke wereld vanuit het perspectief van de betrokkene. Deze methode van onderzoek is niet geschikt voor dit onderzoek aangezien de methode zoekt naar de maatschappelijke wereld van de onderzochte persoon, terwijl dit onderzoek juist niet naar de belevingswereld zoekt maar een werkelijke implementatie en uitvoering.

Bij de **enquête** wordt data verzameld om vragen als wie, wat, waar en hoeveel te beantwoorden. Het gaat hier om een methode voor het gestructureerd verzamelen van kwantitatieve gegevens. Deze onderzoeksmethode is bruikbaar voor dit onderzoek. De resultaten uit afgenomen interviews zullen moeten worden gevalideerd tegen een grotere en voor de onderzoeker minder bereikbare populatie. De validatie zal moeten worden gedaan aan de hand van standaardvragen die getest kunnen worden tegen de interviewresultaten. De enquête is hier bij uitstek een goede methode voor het verkrijgen van deze standaardantwoorden om twee redenen. Ten eerste stelt het de onderzoeker in staat om een grote populatie te bereiken zonder inzet van zeer veel tijd. Ten tweede stelt het de onderzoeker in staat om de resultaten gemakkelijk te kunnen analyseren vanwege de gestructureerde vraagvorm en verkregen resultaten.

Het bepalen van een hedendaags verschijnsel kan met de **casestudy**. Hier worden vragen als waarom, wat en hoe beantwoord. Deze onderzoeksmethode past vrij nauw bij dit onderzoek aangezien het doel vooral gericht is op het verschaffen van inzicht in de hedendaagse situatie. De werkwijze van de methode is nagenoeg gelijk aan de manier van onderzoeken die nodig lijkt voor het uitvoeren van dit onderzoek.

Om het onderzoek te kunnen generaliseren en resultaten te valideren zal de casestudy echter niet voldoende zijn. Zo zullen de casestudy en enquêteonderzoek methoden gecombineerd moeten worden om uiteindelijk tot een beeld van de bestaande situatie te komen, gekeken naar de onderzoekspopulatie.

Op basis van de twee bruikbare onderzoeksmethodes kan een onderzoek opgezet worden in grove lijnen. De eerste stap hiervan is om een diepgaand interview te houden met één praktijk om een beeld te krijgen van alle activiteiten die worden uitgevoerd. Daarnaast zal dit interview gebruikt worden om een beeld te krijgen welke maatregelen van de NEN7510 normering ingevuld kunnen worden en wat het standpunt van deze praktijk is ten aanzien van deze maatregelen.

Als tweede zullen vervolgens een vijf tot tiental focusinterviews (korter dan het diepgaande interview) gehouden worden die de basis van kennisverzameling vormen en aanvullingen, afwijkingen en tegenwerpingen kunnen geven op het beeld wat bij de eerste praktijk is geschetst. Zo zal een algemeen beeld ontstaan van de activiteiten die algemeen in een praktijk te vinden zijn en hoe dit aansluit op informatiebeveiliging.

Als laatste zal dit beeld afgezet worden tegen een grotere groep respondenten middels een enquête om het de resultaten uit de afgenomen interviews te kunnen toetsen en deze resultaten te kunnen generaliseren naar een grotere onderzoekspopulatie.

4.2. Onderzoeksaanpak

Op basis van bovenstaande onderzoeksstrategie zal het empirisch onderzoek verder worden ingevuld en uiteindelijk worden uitgevoerd. Vanuit de gekozen methodes komt naar voren op welke wijze gegevens verzameld worden. De werkwijze zal hieronder verder ingevuld worden.

Betrouwbaarheid
Om de betrouwbaarheid van het onderzoek te borgen zullen de randvoorwaarden en genomen stappen duidelijk worden omschreven. Dit moet uiteindelijk zorgen dat resultaten transparant tot stand komen en bij herhaling, ceteris paribus, dezelfde resultaten en conclusies opleveren.

De onderzoeker heeft zelf geen psychologische achtergrond en de onderzoeker zal daarom gebruik maken van reeds gevalideerde instrumenten voor dit onderzoek. Toetsing van de vragen (m.b.t. voorkomen van sturende werking en 'wenselijke' beantwoording) is hierbij gedaan via het gebruik van reeds gevalideerde instrumenten, zoals het gebruik van reeds getoetste vragen uit peer reviewed papers en gepubliceerde afstudeerscripties met een voldoende beoordeling. Tevens zal worden nagegaan of de opgestelde vragen begrijpelijk en eenduidig zijn door deze vooraf te testen bij huisartsen die geen onderdeel uitmaken van de praktijkinterviews. Registratie van reacties van respondenten zal gedaan worden via een surveytool om registratiefouten te voorkomen.

Er is voor dit onderzoek één waarnemer/onderzoeker, wat verschillen in interpretatie wegneemt, maar er ook voor zorgt dat er slechts met één blik naar de resultaten gekeken wordt. Daarnaast zal worden omschreven hoe gegevens verzameld zullen worden. Ook zal een omschrijving volgen van de communicatie die met de respondent of geïnterviewde is gehouden om intentie en informatieverschaffing duidelijk weer te geven. Hiermee kan onder andere gezorgd worden dat voorkennis in het onderzoek, afgegeven vanuit de onderzoeker, kan worden ingezien.
Voor de genomen stappen zal aangegeven worden in hoeverre er voorselectie in het spel is en hoe er wordt gezorgd dat respondenten zo vrij mogelijk zijn om eerlijk te antwoorden. Andere beperkingen op de betrouwbaarheid zullen, waar bekend, besproken worden.

Validiteit
Borging van de validiteit zal gebeuren door het verloop van het onderzoek zo goed mogelijk te beschrijven. Wat betreft de geschiedenis van onderzoek naar informatiebeveiliging binnen huisartsenpraktijken kan er niets gezegd worden over recent uitgevoerde onderzoeken die de kennis over en resultaten van dit onderzoek kunnen beïnvloeden omdat hier geen informatie over is verkregen bij navraag bij NHG, IBGZ of KNMG en uit de literatuurstudie.

De vragenlijsten worden opgesteld met inzet van reeds gevalideerd onderzoek. Ook de interviews zijn gemaakt aan de hand van gevalideerde methodes. Hiermee worden zo veel als mogelijk gevalideerde instrumenten gebruikt bij dit onderzoek om aantasting van de validiteit te voorkomen.

Tijdens de communicatie met respondenten wordt gezorgd voor een maximale vorm van anonimiteit. Daarnaast wordt gezorgd dat er geen indruk is dat dit onderzoek het werk in enige vorm negatief kan beïnvloeden. Zo wordt geprobeerd de antwoorden zo eerlijk en uitgebreid mogelijk te verkrijgen. Tijdens het onderzoek kan het wel voorkomen dat respondenten zich vooraf inlezen over het onderwerp, voordat ze het interview krijgen of enquête invullen. Dit wordt bij de geïnterviewde personen zo veel mogelijk voorkomen door te vragen dit niet te doen. Bij de enquête respondenten is dit niet te voorkomen, echter is de periode van aankondiging en beantwoorden waarschijnlijk korter dan de periode die zit tussen de aankondiging van het interview en afname daarvan.

Informatiebeveiliging is een zeer actueel onderwerp. Ook als er geen directe aandacht aan het onderwerp besteed wordt zal via het nieuws informatie hierover de respondenten kunnen bereiken. Dit is niet te voorkomen, echter zal door de beperkte looptijd van de enquête ten opzichte van de looptijd van organisatorische veranderingen wel een statisch beeld van dit moment gemaakt kunnen worden en daaruit conclusies getrokken over informatiebeveiliging bij huisartsenpraktijken.

Naast geïnformeerde respondenten kan het ook zijn dat er respondenten in de maillijst aanwezig zijn die geen onderdeel van de doelgroep zijn. Dit wordt zo veel mogelijk voorkomen maar er zullen daarnaast ook selectievragen in de enquête worden opgenomen om dit achteraf te kunnen controleren. Resultaten van personen die niet eigenaar of medewerker zijn van een huisartsenpraktijk zullen uit de resultaten gehaald worden.

In het geval van mortaliteit en maturatie vindt de onderzoeker dat de doorloop van dit onderzoek dermate kort is dat deze factoren geen invloed hebben op de validiteit van het onderzoek.

Uiteindelijk zullen er conclusies getrokken worden over de gevonden resultaten. Hiermee zal zo veel mogelijk rekening gehouden worden met de richting van verbanden tussen oorzaak en gevolg, waar dit statistisch weergegeven kan worden en waar dit verband bestaat. Waar dit verband niet significant is, zal dit vermeld worden.

Generaliseerbaarheid
Er zal in dit onderzoek worden geprobeerd verder te kunnen generaliseren dan de geïnterviewde groep huisartsen. Om dit te borgen zullen de karakteristieken van de huisartsenpraktijken worden opgenomen waar dit de anonimiteit niet in het geding brengt. Bij uitleg over de onderzoekspopulatie van de interviews en enquête zal tevens de beperkingen ten aanzien van de generaliseerbaarheid worden besproken. Na uitvoering van het enquêteonderdeel zal tevens worden gecontroleerd of de groep respondenten overeenkomt met de verwachtingen, zodat de daadwerkelijke generaliseerbaarheid bepaald kan worden. De daadwerkelijke mogelijkheden tot het generaliseren van de resultaten zullen bij de conclusies besproken worden.

Bij het verwerken van de resultaten zal moeten worden gewaakt voor logische sprongen en verkeerde aannames. Door vooraf in de aanpak duidelijk te bespreken welke informatie verzameld gaat worden en wat de verwachtingen zijn kan dit meehelpen aan de controle achteraf. Hierbij kan bijvoorbeeld worden gecontroleerd of de onderzoekspopulatie overeenkomt met wat vooraf omschreven is of conclusies op basis van waarden kloppen ten aanzien van de gestelde vragen. Bij het diepte-interview zullen tevens de termen, gebruikt in de NEN7510, worden doorgenomen. Dit moet waarborgen dat de onderzoeker en geïnterviewde/respondenten dezelfde vaktaal spreken en uitgaan van dezelfde aannames wat betreft betekenis van vragen en antwoorden.

Beperkingen aan het onderzoek
Alle beperkingen van dit onderzoek zullen zo veel mogelijk worden besproken bij de relevante onderdelen in de tekst. Daarnaast zijn er nog andere beperkingen die aan dit onderzoek zitten. Zo zal dit onderzoek beperkt zijn omdat interviews rond en in de vakantieperiode plaatsvinden. Hierdoor is de druk op huisartsen (vanwege afwezigheid van collega's) groter en wordt verwacht dat de tijd voor interviews beperkter is dan buiten deze periode verwacht mag worden. Daarnaast is bij een korte rondvraag vastgesteld dat de motivatie tot deelname reeds klein is vanwege de beperkte beschikbare tijd van huisartsen en assistenten. Het onderzoek zal dus waarschijnlijk een beperkte response opleveren en daarmee lastig te generaliseren zijn. De daadwerkelijke mogelijkheden van generalisatie zullen bij de conclusies vastgesteld worden.

Voor dit onderzoek zal aangesloten worden op het onderzoeksgebied IT-security, waarmee de scope van het onderzoek ook beperkt zal worden tot de IT-aspecten van informatiebeveiliging. Informatiebeveiliging op niet-IT-gebieden (zoals bijvoorbeeld volledigheid van ICPC-codering en kwaliteit van opgeslagen informatie) zal hierom niet worden meegenomen in dit onderzoek. Daarnaast is dit onderzoek uitgevoerd bij huisartsenprakijken en is dit onderzoek beperkt tot die steden waarin naar contactgegevens van huisartsen gezocht kon worden. Zo wordt een benadering van alle steden die tot de Randstad behoren gebruikt voor het verkrijgen van toegang. Er is echter geen vaste definitie van de Randstad, waardoor alle steden en gemeenten rondom de agglomeraties van de vier grote steden in Nederland zal worden aangehouden als zoekgebied. De complete lijst met steden die zijn meegenomen staat opgenomen in bijlage 1.

Dit onderzoek is in scope beperkt en resultaten en conclusies verkregen uit dit onderzoek moeten in dit licht gezien worden. De resultaten en conclusies kunnen daarbuiten niet gegeneraliseerd worden.

Beantwoording van de deelvragen
Om inzicht te krijgen in de maatregelen die huisartsenpraktijken nemen in het kader van informatiebeveiliging zijn een aantal deelvragen gesteld. Dit komt voort uit het feit dat bekend moet worden welke maatregelen er zijn, welke daarvan relevant zijn, hoe huisartsenpraktijken werken en hoe maatregelen en de werkzaamheden samenhangen. Met behulp van de onderzoeksaanpak zal een antwoord moeten worden gegeven op de deelvragen, zodat in de conclusie deze deelvragen samen antwoord kunnen geven aan de vraagstelling van dit onderzoek.

Om de deelvragen van dit onderzoek goed te kunnen beantwoorden en daarmee inzicht te krijgen in de maatregelen die huisartsenpraktijken nemen in het kader van informatiebeveiliging moet worden bedacht welke vragen dienen te worden gesteld om een eerste, maar nuttig beeld te krijgen van de huidige staat van informatiebeveiliging bij huisartsenpraktijken. Om te komen tot nuttige vragen die gesteld moeten worden om een eerste beeld te schetsen van de huidige staat van informatiebeveiliging zullen een aantal stappen ondernomen worden. Allereerst zal de literatuur geraadpleegd worden om reeds gebruikte en getoetste opbouw van interview en enquêtevragen te bekijken. Zo is het onderzoek over “Social engineering binnen de Nederlandse Rijksoverheid” (Spijker, 2017) nuttig gebleken voor opbouw van algemene en specifieke vragen en syntax van vraagstelling. Dit onderzoek richt zich op een diepgaande studie van informatiebeveiliging bij de Nederlandse Overheid en de gebruikte methode is daarmee bruikbaar voor deze studie om algemene kennis over informatiebeveiliging op te doen. Een deel van de vragen voor de interviews is afgeleid uit het onderzoek van Spijker.

Om te zien welke praktijkprocessen er nog meer zijn en hoe deze met elkaar communiceren zullen ook de werken “Zo werkt het in de huisartsenpraktijk” (Dolmans, 2009), “Een eigen Praktijk” (Fisscher & van Bemmel, 2015), “Informatiebeveiliging in de zorg” (Wel, 2006) en “Informatiebeveiliging in de huisartsenpraktijk” (Nederlands Huisartsen Genootschap, 2009) gebruikt worden bij het maken van de vragenlijst.

Er moet een compleet beeld geschetst worden van de huisartsenpraktijk op het gebied van informatiebeveiliging. Hierdoor is het vragen naar informatiebeveiliging aan de hand van onderzoek uit andere werkgebieden niet op zichzelf bruikbaar. De huisartsenpraktijken zullen zelf de relevantie voor hun sector moeten tonen. Dit betekent dat er een zeer diepgaand interview moet komen dat zo veel mogelijk aspecten van het werk uitlicht. Gezien de doorlooptijd van dit onderzoek zal dit diepgaande interview gehouden worden met één praktijk. Er zal vervolgens een vervolginterview gehouden worden met enkele andere praktijken waar de opgedane kennis zal worden aangepast of aangevuld.

Zo kan tot een algehele consensus van de basiskennis van informatiebeveiliging bij huisartsenpraktijken gekomen worden. Hiermee voorkom je tevens dat je van meerdere praktijken een zeer grote tijdsinvestering vraagt, wat een grote showstopper lijkt te zijn voor deelname aan onderzoek. Dit laatste blijkt voornamelijk bij rondvraag voor deelname aan de interviews.

Voorafgaande aan de interviews is tevens bekeken hoe een interview kan plaatsvinden. Vragen hierover en de procedure zijn afgeleid van het interviewscript en -vragen van "De interne communicatietaken van medewerkers en managers" (Otten, 2013). Zo kon ik aansluiten bij reeds gedaan onderzoek en gebruikmaken van gevalideerde instrumenten.

Om te zorgen dat de focus interviews zo weinig mogelijk vergeten items bevatten, zal voorafgaand een uitgebreid diepte-interview (praktijk 0 interview) gehouden worden. In dit interview zullen de reeds gemaakte vragen gesteld worden én de NEN7510 normering volledig worden langsgelopen. Eventuele nieuwe vragen zullen op basis van de beantwoording hiervan worden toegevoegd aan de lijst met vragen voor de interviews van de andere praktijken. Gebruikte termen in de informatiebeveiliging zullen worden besproken en waar nodig aangepast aan vergelijkbare termen bij huisartsenpraktijken zodat deze vaktermen gebruikt kunnen worden tijdens vervolginterviews en de af te nemen enquêtes. Dit moet zorgen voor betere communicatie met de andere praktijken die worden geïnterviewd en met de respondenten van de enquête.

Uiteindelijk kan met deze vragenlijst en de daaropvolgende enquête gericht worden op de beantwoording van de deelvragen van dit onderzoek.

<u>Deelvraag 1: Hoe vullen huisartsenpraktijken informatiebeveiliging nu in?</u>
Voor het verkrijgen van diepgaand inzicht over informatiebeveiliging bij huisartsenpraktijken (huidige situatie) zullen interviews afgenomen moeten worden om te zien hoe informatiebeveiliging nu in de praktijk aanwezig is. Deze interviews zullen afgenomen worden aan de hand van de vastgestelde vragenlijst met praktijk 0. Nadat alle interviews zijn afgenomen zullen de data worden gebruikt om een algemeen beeld te vormen van de invulling van informatiebeveiliging bij huisartsenpraktijken. Omdat uitgegaan wordt van gevalideerde instrumenten en normering die een volledig pakket van maatregelen op het gebied van informatiebeveiliging toetst, kan na voltooiing van de interviews gesteld worden dat een diepgaand inzicht op het gebied van informatiebeveiliging is gecreëerd binnen de geïnterviewde populatie.

<u>Deelvraag 2: Wordt dit beeld bevestigd bij een grotere groep?</u>
Na het verkrijgen van diepgaand inzicht over informatiebeveiliging bij de geïnterviewde huisartsenpraktijken zal ook gecontroleerd moeten worden of en in hoeverre deze resultaten te generaliseren zijn naar een grotere populatie. Dit zal gedaan worden middels enquêtes.

Omdat interviews beperkingen kennen ten aanzien van toetsing tegen grotere onderzoeksgroepen zal geprobeerd worden om de verkregen resultaten via een enquête te controleren op een grotere onderzoekspopulatie. Daarnaast heeft de enquête als doel om ook het verder kunnen generaliseren mogelijk te maken. Hierbij zullen, waar mogelijk en bekend, landelijke cijfers worden opgenomen en besproken om zo ook op individuele punten enige generalisatie mogelijk te maken, waar van toepassing.

De enquêtevragen zijn afgeleid van de interviewvragen. Er zijn enkele wijzigingen gemaakt om de open vraagstelling aan te passen naar gesloten vragen voor de enquêtes. Hiervoor is tevens gekeken naar de vraagstelling in het werk "Vertrouwen van zorgverleners in elektronische informatie-uitwisseling en het landelijk EPD: een juridische en sociaal-wetenschappelijke studie naar de positie van zorgverleners" (Ploem et al., 2011). De nieuwe vragen zijn besproken met enkele niet-deelnemende huisartsen om te kunnen toetsen of de vragen en gebruikte termen duidelijk zijn en antwoorden eenduidig gegeven kunnen worden.

Deelvraag 3: Zijn er verschillen te vinden bij de invulling van informatiebeveiliging tussen huisartsenpraktijken?
Tijdens de interviews zal er worden gelet op mogelijke indicatoren die een significant verschil teweeg kunnen brengen bij de invulling van informatiebeveiliging binnen huisartsenpraktijken. Bijvoorbeeld op basis van aanwezigheid van praktijkaccreditatie kan zo'n verschil bestaan. Andere verschillen kunnen bijvoorbeeld ontstaan bij groepen praktijken uit verschillende steden, grootte van de praktijk, aantal medewerkers, enzovoorts.

Omdat er een lage response verwacht wordt zal goed gelet moeten worden op de verschillen die worden bekeken. Het bekijken van een verschil op basis van stad is waarschijnlijk niet mogelijk als het aantal respondenten per stad onder de 10 blijft. De uiteindelijke beoordeling welke verschillen bekeken worden zal na ontvangst van de enquêteresultaten vastgesteld worden.

Na de interviews en afronding van de enquête zal gekeken worden of er een significant verschil bestaat op relevante vlakken. Dit zal in de resultaten worden opgenomen.

Deelvraag 4: Zijn er gemeenschappelijke aanbevelingen te vinden die de staat van informatiebeveiliging verder kunnen bevorderen?
Ook zal na de verwerking van alle resultaten gezocht worden naar overeenkomende resultaten. Hierbij zal worden gekeken of deze, bij verbeterde invulling binnen huisartsenpraktijken, de informatiebeveiliging bij huisartsenpraktijken in het algemeen kan bevorderen. Tevens zal gekeken worden of er gemeenschappelijke resultaten voorkomen waar een oorzaak gevolg relatie in lijkt voor te komen die een betere invulling van informatiebeveiliging binnen de huisartsenpraktijk vertegenwoordigd. Focus zal hierbij liggen op de quick-wins.

Strategie voor verkrijgen van toegang
Om huisartsenpraktijken te kunnen bereiken voor diepte-interviews of de enquête zal allereerst meer achtergrondkennis over beoogde organisatie of groep verzameld moeten worden. Dit zal gedaan worden door gesprekken met reeds bestaande contacten over de groep respondenten. Deze gesprekken zullen met name toegespitst zijn op maximalisatie van de response van enquêtes en bereidheid tot deelname aan interviews. Denk hierbij aan ervaring van "geven van tijd aan onderzoek" en bestaande zorgen t.a.v. publiek onderzoek wegnemen. De toegang is hierbij beperkt vanwege de eindtijd van de studie waardoor interviews en enquête een beperkte looptijd hebben.

Voor de toegang zullen bestaande contacten (huisartsen in de regio Den Haag en Rijswijk) worden gebruikt en nieuwe contacten gezocht worden via deze bestaande contacten in directe omgeving. In de eerste communicatie met huisartsen zal duidelijk gemaakt worden wat het doel van het onderzoek is en welk soort toegang benodigd is. Deze toegang zal ten minste de informatie over de werkzaamheden van de huisarts zelf en de praktijk betreffen, toegespitst op het gebied van informatiebeveiliging. Mogelijke bezwaren, zoals negatieve effecten, zullen bij dit contact zo veel mogelijk worden weggenomen door waarborging van een hoge mate van anonimiteit.

De maillijst voor de enquête zal worden samengesteld aan de hand van verkregen mailadressen aangeleverd door reeds gesproken huisartsen. Daarnaast zullen adressen verkregen worden uit openbare boekwerken zoals het Geneeskundig Adresboek (Nijgh-Periodieken, 2003), internetsites van huisartsen zelf en via navraag huisartsenpraktijken in persoon of per telefoon. In alle gevallen zal geverifieerd worden of de huisarts nog actief is middels een controle op de BIG-registratie.

Na de verzameling van alle adressen zal er een mailing gestuurd worden met de vraag om mee te helpen aan dit onderzoek. In deze mailing zal tevens de link gezet worden naar de enquête. Dit om te zorgen dat er niet éérst goedkeuring moet worden gevraagd en daarna pas een link verstuurd. Door meervoudige acties zal het reactiepercentage zeker lager liggen.

Voor de enquête wordt een lage response verwacht. Deze lage response wordt zo veel mogelijk weggenomen door drempels van response (tijdsduur enquête, gemak van bediening) te beperken en interviewduur zo kort mogelijk te houden. Tevens zullen acties ondernomen worden om de mail zo vertrouwd mogelijk te maken in termen van geloofwaardigheid van tekst en anti-spam blokkades. Daarnaast worden huisartsen aangemoedigd mee te doen door mogelijke voordelen voor de organisatie te belichten. De onderzoeker zal hierbij niet werken met incentives om geïnterviewde huisartsen niet te beïnvloeden in hun beantwoording. Wel zal het delen van de onderzoeksresultaten worden besproken zodat daar voordelen uitgehaald kunnen worden.
De enquête en mailing daarvan is vooraf met enkele niet-deelnemende huisartsen doorgenomen om te bekijken of hij begrijpelijk en aansprekend is. De enquête is daarnaast zo eenvoudig mogelijk gehouden om response zo hoog mogelijk te krijgen. Er is slechts 1-muisklik nodig om vanuit de e-mail akkoord te gaan (toegang te krijgen) met deelname aan de enquête en deze ook te starten. Reacties worden vergemakkelijkt door opbouw van de Surveymonkey website (Eén vraag per keer met duidelijke antwoordmogelijkheden). Er worden geen voorwaarden gesteld aan beantwoording, waardoor er geen foutmeldingen kunnen optreden die het beantwoorden vertragen. Onvolledige reacties zullen uit de uiteindelijke resultaten worden gefilterd. Door de wijze en eenvoud van invullen hoopt de onderzoeker deze onvolledige reacties zo laag mogelijk te houden.

In de e-mail zal uitleg opgenomen worden over het onderzoek en achtergrond van de onderzoeker. Daarnaast is het LinkedIN profiel van de onderzoeker bijgewerkt, mochten artsen een profielcheck uitvoeren van de onderzoeker. Op basis van de uitvoering kan het zijn dat er aanvullende maatregelen genomen worden om de response te verhogen, dit zal dan verder worden uitgelegd in de uitvoering en resultaten.

Steekproef enquête
Het behalen van een significante steekproef over “huisartsenpraktijken in Nederland” is hoogstwaarschijnlijk niet haalbaar binnen de gestelde tijdslimieten van de opleiding. Daarbij is te verwachten dat een laag reactiepercentage moet worden verwacht van ingestuurde enquêtes, zeker als deze veel vragen betreffen. Er moet dus worden nagedacht over hoe de huisartsen(praktijken) met zo weinig mogelijk inspanning zo veel mogelijk informatie kunnen leveren. Bij een kleine groep praktijken is interviewen middels persoonlijk contact mogelijk. Hierbij is de geïnvesteerde tijd groter en is fysieke aanwezigheid nodig. Dit legt een grote belasting op de gevraagde inspanning en is daarom niet mogelijk bij een grotere groep. Bij een grotere groep praktijken zal alleen een korte vragenlijst gegeven moeten worden, om het reactiepercentage enigszins voldoende te krijgen.

Het onderzoek moet dan ook gezien worden als een verkenning van informatiebeveiliging bij huisartsenpraktijken (hoe ziet het eruit, hoe doen ze het). Vragen waar nu geen antwoord op te vinden is in de literatuur. Er zal niet ingaan worden op statistisch significante getallen over de gehele populatie, maar slechts een mogelijke aanleiding gezocht worden voor groter onderzoek.

Uiteindelijk zal worden geprobeerd om ten minste 50 volledige enquêtereacties te behalen. Zo kan gekeken worden of het onderzoek enigszins gegeneraliseerd kan worden en eerste antwoorden op de vraagstelling geformuleerd kunnen worden.

Door middel van tussentijdse feedbackverwerking zal de methode van informatieverzameling verbeterd worden zodat het aantal behaalde resultaten zo groot mogelijk gemaakt wordt.
Zo zal de input van eerder onderzoek, het diepte-interview en de focusinterviews gebruikt worden om vragenlijst en response zo goed mogelijk te verkrijgen.
Binnen de verzending van de enquêtemailing zal tevens een iteratief component aanwezig zijn zodat fouten en verbeterpunten uit de eerste verzendingen bij vervolgzendingen verbeterd zijn en waar mogelijk extra waarde toevoegen ten aanzien van de beantwoording van vragen en het verkregen responsepercentage.

Uitleg informatiebeveiliging aan respondent
Tijdens het interview zullen vragen naar voren komen die betrekking hebben op informatiebeveiliging. Er zal allereerst gevraagd worden waar de respondent aan denkt bij informatiebeveiliging. Dit is een onderdeel van de vragen, dat alleen zonder bias kan worden beantwoord als dit vóór verdere uitleg is gevraagd. Daarna zal worden gecommuniceerd wat bedoeld wordt bij het praten over informatiebeveiliging zodat de scope van vragenbeantwoording voor overige vragen duidelijk is.

De uitleg hiervan is als volgt:
“
Informatiebeveiliging heeft drie doelstellingen, namelijk het zo goed mogelijk waarborgen van:

- Beschikbaarheid van gegevens
- Vertrouwelijkheid van gegevens (privacy van patiënten)
- Betrouwbaarheid/integriteit van gegevens

Informatiebeveiliging in het algemeen gaat hierbij in op alles wat betrekking heeft op deze drie termen. Wij zullen tijdens dit interview echter alleen ingaan op de IT-aspecten van informatiebeveiliging, samen met de maatregelen die in de NEN7510 besproken worden.
“

Na deze uitleg zullen de rest van de vragen besproken worden met de respondenten.

5. Uitvoering

In dit hoofdstuk zal uiteen worden gezet hoe de vastgestelde methode en aanpak vervolgens daadwerkelijk in uitvoering is gebracht. Hierbij zal worden ingegaan op de verzameling van gegevens, verkrijgen van toegang tot de huisartsenpraktijken, afname van de interviews, ontwerp en afname van de enquête en vooraf besproken optimalisaties ten aanzien van responseoptimalisatie en borging van betrouwbaarheid, validiteit en generaliseerbaarheid.

Van alle interviews zijn de gegevens van de praktijken in de bijlage opgenomen.
Voor het verkennende interview is een beroep gedaan op praktijk 0. Met deze arts zijn meerdere besprekingen geweest. Allereerst zijn de algemene vragen doorgenomen. Daarna is ook de NEN7510 doorgenomen. Hierbij is bij elke maatregel gevraagd of de arts activiteiten heeft die onder deze maatregel vallen. Van dit interview met alle onderdelen is het volledige verslag opgenomen in bijlage 5.

De vragen die vooraf zijn opgesteld aan de hand van de besproken literatuur en gebruikt zijn voor het diepte-interview van praktijk 0 zijn de volgende:

Algemeen:
- Hoeveel medewerkers telt de praktijk?
- Welke functie vervult U?
- Welke functies zijn er te vinden in deze praktijk?
- Geef een korte beschrijving van elke functie met bijbehorende verantwoordelijkheden.

Inrichting van informatiebeveiliging (op basis van NEN7510)
- Kunt u een beschrijving geven van de werkzaamheden en activiteiten in de praktijk?
- Welke systemen en applicaties zijn in de praktijk aanwezig?
- Hoe worden deze systemen en applicaties onderhouden?
- Zijn er overeenkomsten met de leverancier van deze systemen en applicaties?
- Hoe worden risico's weggenomen m.b.t. deze systemen en applicaties?
- Bij het contact met patiënten, hoe zorgt U dat dit privé blijft?
- Hoe zorgt U dat relevante informatie goed opgeslagen wordt?
- Zijn de systemen van opslag beschermt tegen bedreigingen en fouten?
- Is er een personeelsbeleid?
- Vindt er screening van bestaande en nieuwe medewerkers plaats?
- Is er een functie- en toegangsbeleid?
- Is er een handboek of schriftelijke uitleg van procedures?

Voor de vragen m.b.t. inrichting van informatiebeveiliging is de NEN7510:2011 tevens het toetsingsdocument. Hier is elke paragraaf aangehouden als losstaand punt dat wel of niet (beargumenteerd) is geïmplementeerd in de praktijk.

De volgende hoofdstukken uit de norm NEN7510:2011 (NEN.nl, 2011) zijn met praktijk 0 doorgenomen tijdens het interview en opgenomen in de bijlage:
H5 Beveiligingsbeleid
H6 Organisatie van informatiebeveiliging
H7 Beheer van bedrijfsmiddelen
H8 Personeel
H9 Fysieke beveiliging en beveiliging van de omgeving
H10 Beheer van communicatie- en bedieningsprocessen
H11 Toegangsbeveiliging
H12 Verwerving, ontwikkeling en onderhoud van informatiesystemen
H13 Beheer van informatiebeveiligingsincidenten
H14 Bedrijfscontinuïteitsbeheer
H15 Naleving

Adressenverzameling
Voor het verzamelen van contactgegevens van huisartsenpraktijken is het internet afgespeurd naar "huisartspraktijk in <stad>" en de websites naar e-mailadressen en namen. Daarnaast is rondgevraagd bij reeds gecontacteerde huisartsen of zij contactgegevens van collega's kunnen en mogen geven. Ook is het Geneeskundig adresboek Nederland (2003-2004) doorlopen, waarbij alle namen en adressen van huisartsenpraktijken uit de Randstadsteden zijn geselecteerd.

Na de verzameling zijn alle verzamelde namen en adressen in het online BIG-register (CIBG) gecontroleerd zodat zeker is dat de e-mailadressen verwijzen naar geregistreerde huisartsen.

Ook is de NHG gevraagd of de enquêtelink gedeeld kon worden met haar leden. In de reactie werd verwezen naar de algemene tekst op haar website: “Het NHG beschikt enkel over de gegevens van de leden (niet iedere huisarts is lid van het NHG). In verband met bescherming van persoonsgegevens (Wet Bescherming Persoonsgegevens) geeft het NHG geen namen, adressen of andere gegevens van de leden af. Voor adressen van huisartsen kunt u de Geneeskundige Adresgids (inlog nodig) raadplegen. U kunt ook het NIVEL (Nederlands Instituut voor onderzoek van de gezondheidszorg) raadplegen.”

Na een tweede reactie van de NHG werden de volgende ontwikkelingen aangegeven in relatie tot het onderzoek:
“

- LHV Academy biedt een cursus informatiebeveiliging aan voor de huisartspraktijk, die wordt redelijk goed bezocht
- In de NPA - praktijkaccreditering huisartsen - werken we aan een eerste keuzemodule informatiebeveiliging, die komt als het goed is in 2017 beschikbaar
- Samen met Nictiz en een aantal andere koepels in de eerstelijn hebben we voor de HIS-leveranciers een programma van eisen opgesteld voor logging van toegang, en eentje voor identificatie/authenticatie/autorisatie. In de praktijkwijzer zal - ook in 2017 - een stuk scholing/uitleg worden opgenomen over hoe de huisartspraktijk om moet gaan met de logging
- LHV gaat meekijken met de praktijkwijzer, op hun verzoek nemen we een onderdeel op ‘veilige praktijkinrichting’
- Dit najaar (2017) doen we een onderzoek naar secure mail/ secure chat

“

Er is in relatie tot de aangekondigde ontwikkelingen geen verder contact geweest met de NHG tijdens het verloop van het onderzoek.

Daarnaast is naar vakgroepen voor huisartsen gezocht. Hierbij werd verwezen naar de universitaire vakgroepen huisartsgeneeskunde die hun onderzoeksnetwerk van huisartsen kunnen benaderen, te bereiken via de site van de vakgroep Huisartsgeneeskunde Maastricht (Maastricht-University). De verantwoordelijke voor deze vakgroep heb ik aangeschreven en heb overlegd of deze vakgroep wat voor mij kon betekenen met betrekking tot het verkrijgen van meer response op de enquête in de vorm van toegang verschaffing of delen van de enquêtelink onder haar leden. Helaas was dit niet het geval.

Voor het verzamelen van reacties van respondenten van de enquête zijn een aantal survey websites bekeken. Hierbij zijn thesistools.com en surveymonkey.com uiteindelijk nader bekeken voor gebruik in dit onderzoek. Er is hierbij voor surveymonkey.com gekozen vanwege de uitgebreide ondersteuning van verschillende browsers en apparaten waardoor grotere eenvoud bij het invullen van de enquête wordt verwacht en daarmee dus ook een hoger responsepercentage.

Binnen Surveymonkey is een betaald plan aangevraagd en is voor elke respondent een reactielink aangemaakt, 1080 in totaal. Omdat op deze manier reacties zichtbaar worden, kunnen herinneringen verstuurd worden aan respondenten die nog niet hebben gereageerd. Aangezien de onderzoeker de gebruikersvoorwaarden van Surveymonkey wil opvolgen, zullen het bijhouden van de reacties en uiteindelijke mailverzending (handmatig) buiten Surveymonkey om uitgevoerd worden. Daarnaast zijn twee bijkomende voordelen van deze enigszins arbeidsintensieve methode dat foutberichten met mailadresverhuizingen kunnen worden omgezet naar het nieuwe adres en dat beter op anti-spam filters geanticipeerd kan worden bij verzending van de mailing.

Optimalisatie mailing

De tekst van de begeleidende e-mail is doorgesproken met enkele artsen om de mailing zo aansprekend mogelijk te maken. Tevens is de “geschatte invulduur” toegevoegd aan de hand van een geautomatiseerde schatting van SurveyMonkey en enkele keren proef-invullen om mensen een reëel beeld van de tijdsbesteding voor deze enquête te geven. Aangezien dit onder 10 minuten is (ongeveer 8), is de verwachting dat dit als positief zal worden ervaren door de beoogde respondenten, zoals ook enkele artsen aangeven dit te ervaren op basis van de geschatte tijdsduur. Het aantal vragen (37) is weggelaten uit de tekst omdat dit als “veel” ervaren kan worden. Alléén de vermelding van de geschatte tijdsduur zal dan positiever worden ontvangen.

Optimalisatie van de enquêteverzending is gedaan door de spam-score vooraf te testen via mail-tester.com met een gewenste score van 10/10. Dit om de kans op blokkering door spamfilters of verplaatsen naar “ongewenste” mailfolders te voorkomen, wat het leespercentage verhoogt.

Keuzes voor optimalisatie van het verzendmoment van de enquête zijn als volgt:

- De mailing moet bij voorkeur binnenkomen als de beoogde respondent zijn/haar spam heeft weggewerkt. Dit betekent dat de mailing niet aan het begin van de werkdag moet plaatsvinden. Daarnaast moet de mailing niet plaatsvinden op tijdstippen dat mensen juist spam verwachten (buiten werktijd en nacht).
- Beste zendtijden zijn nagegaan door gebruik te maken van spamrapportages van spam gedurende de werkweek (SecurityIntelligence)
    - De meest rustige tijd vanuit spam-oogpunt is: Doordeweekse dagen tussen 16.00u en 18.00u (14.00u en 16.00u UTC) en na 29-okt tussen 15.00u en 17.00u (i.v.m. wintertijd). In weekenden is de meest-rustige-tijd-verdeling lastiger te maken, daarnaast zal voor vele werkadressen deze mail met de maandagochtend “bulk” meekomen, dit is dus geen wenselijk verstuurmoment. Tevens is de vrijdagmiddag om dezelfde reden niet meegenomen.
- Aan het einde van de werkdag is verder niet de meest wenselijke situatie omdat dan de kans bestaat dat de mail bij de bulk van de nacht terecht komt.

Samenvattend is gekomen tot een voorkeursmoment voor verzending op dinsdag t/m donderdag in de vroege middag (13.00u tot 15.00u).

De mailing is met bovenstaand schema en optimalisaties ten aanzien van verzending verstuurd in porties van 25. Zo kan tussentijds gecontroleerd worden op verzendings- en tekstfouten. Hiermee kan de mailing, indien nodig, verder verbeterd worden voordat de gehele maillijst is verzonden. Daarnaast wordt door verzending van kleine volumes het aantal NDR-berichten (Non-Delivery Reports zijn teruggestuurde berichten als een bericht niet afgeleverd kan worden) per uur verlaagd, waardoor de kans kleiner is dat tussentijds alsnog een spamscore gehaald wordt en vervolgzendingen in de spamfolder bij de ontvanger terecht komen. Als laatste heeft deze verzendingsmethode een iteratief verbeterkarakter, zodat nieuwe inzichten aan de hand van reeds verzonden e-mailberichten kunnen worden gebruikt bij de resterende ontvangers.

In de mailing wordt gevraagd om de link ook te delen met collega huisartsen en andere medewerkers van de praktijk. Om dit te faciliteren is in het verzamelprogramma opgenomen dat de enquête meerdere keren mag worden ingevuld. Dit zorgt ervoor dat meerdere collega’s achter een gezamenlijke werkplek of internetlijn (binnen één gebouw) de enquête kunnen invullen zonder foutmeldingen.

Naast de mailing heb ik mijn LinkedIN profiel aangepast zodat de ontvanger online kan controleren of de tekst uit de mail (onderzoek n.a.v. studie aan OU) overeenkomt met mij als persoon (student aan de OU). Dit verhoogt de geloofwaardigheid van de mailing en daarmee ook het uiteindelijke reactiepercentage van de respondenten.

Uitvoering interviews
De uitgewerkte interviews zijn in de bijlage opgenomen. In de interviews zelf is een vloeiend gesprek aangehouden, waardoor vragen door elkaar beantwoord kunnen zijn en meer commentaar gegeven kan zijn dan enkel het antwoord op de vraag of vragen. Alle interviews zijn opgenomen met een voicerecorder om afgenomen gesprekken zo precies mogelijk te kunnen uitwerken. In de uitwerking zijn de individuele antwoorden vervolgens op volgorde van vraagnummer opgenomen om het overzichtelijk te houden voor de onderzoeker. Opmerkingen die niet direct bij de ene vraag pasten zijn geplaatst bij de corresponderende vraag als antwoord. Opmerkingen die niet passen binnen het onderzoek of slaan op een of meerdere patiënten zijn weggelaten. Er zijn gedurende de interviews geen patiëntcases besproken.

Aan de hand van de bespreking met praktijk 0 is de vragenlijst verder uitgewerkt. Om de antwoorden op deze vragen te vinden zijn interviews uitgevoerd met enkele andere huisartsenpraktijken (3 á 5), waarbij de eerste praktijk dus als basis heeft gediend.

Uitvoering mailing enquête
Via mail-tester.com is de uiteindelijke e-mail getest. Er is een score van 10/10 behaald.
Eerste verzendlijst bevatte bij controle vóór verzending nog fouten in titel en achternaam van diverse respondenten. Dit komt door de meervoudige invoering (monnikenwerk) waarbij automatische scheiding van voorletters en achternaam voor enkele fouten heeft gezorgd. Na alle correcties op de gehele adreslijst te hebben toegepast waren de eerste 25 adressen verstuurd op dinsdag 10-okt 15.00u.

Na het versturen van de eerste batch is nog een laatste tekst aangepast:
“[…] mee te helpen aan deze enquête” is aangepast naar “[…] mee te helpen aan dit onderzoek”.
Op navolgende dagen zijn de overige berichten verstuurd.
Van alle afwezigheidsberichten zijn de “gewijzigde e-mailadressen” ook opgenomen in de eerstvolgende verzendlijst.

Vanuit de binnengekomen resultaten zijn vervolgens alle onvolledige reacties en reacties van respondenten die niet tot de doelgroep behoorden weggehaald.

Er waren ongeveer 42 correcte resultaten binnengekomen na een periode van twee weken sinds het uitsturen van de complete mailing. Uiteindelijk is op een vrijdag een extra herinnering per e-mail verstuurd aan alle mogelijke respondenten (personen waar geen reactie of NDR van is ontvangen). De reden om dit op een vrijdag te versturen, tegen eerder vastgesteld schema in, is omdat tijdens het ontvangen van de resultaten een overgroot deel van de resultaten in het weekend leek te verschijnen en een extra mailing vóór het weekend lijkt daarom voor het verhogen van het responsepercentage nuttig te zijn. Ook hier is de mailing gesplitst over enkele vrijdagen verstuurd. Direct volgend op deze extra mailing zijn er nog ruim 30 resultaten binnengekomen. Vanwege de beperkte onderzoeksperiode is het verkrijgen van resultaten twee weken na deze laatste herinnering gestopt.

6. Resultaten

In dit hoofdstuk zullen de resultaten van het onderzoek besproken worden. Hier komt de uitvoering van de vooraf opgestelde methode en aanpak aan bod en zijn de resultaten van de afgenomen interviews en response op de enquête terug te vinden. De volledige uitwerkingen van de interviews zijn opgenomen in bijlage 5. De resultaten van de enquête zijn te vinden in bijlage 6.

Er is bij huisartsen in Den Haag en Rijswijk gevraagd of een interview afgenomen mag worden. Deze artsen zijn gekozen op basis van bestaande contacten met huisartsen in de buurt van de woonplaats van de onderzoeker. Op basis van navraag bij deze huisartsen zijn contactgegevens verkregen van enkele HAGRO (Huisartsengroep Haaglanden) praktijken. In totaal zijn 17 huisartsenpraktijken gevraagd mee te helpen. Er hebben uiteindelijk 7 huisartsen van 6 huisartsenpraktijken akkoord gegeven en met hun is een interviewmoment afgesproken. Met 1 van de huisartsen is het interview vroegtijdig onderbroken en er is daarbij geen nieuw moment voor vervolg gekomen. De beperkte set resultaten van dit korte interview zijn niet opgenomen in dit onderzoek.

<u>Interview praktijk 0</u>
Er is met één praktijk (praktijk 0) een zeer diepgaand interview gehouden uitgespreid over enkele dagen. Deze omvatte het doorspreken van de NEN7510 en het stellen van opgestelde vragen en verder opstellen van de vragenlijst voor de overige interviews. De antwoorden die zijn gekregen op de gestelde vragen zijn gebruikt om een eerste beeld te krijgen van de huidige staat van informatiebeveiliging bij huisartsenpraktijken.

Het interview met praktijk 0 is in een tijdsperiode van enkele dagen gehouden vanwege de grootte van de door te nemen stof en beperkte beschikbare tijd van de huisarts per contactmoment. Het opgenomen gesprek en gemaakte aantekeningen zijn samengevoegd en zijn vervolgens uitgewerkt en opgenomen in de bijlage van dit document.

<u>Wat viel op tijdens het interview met praktijk 0?</u>
Aan de hand van het interview met praktijk 0 valt op dat er redelijk wat maatregelen op het gebied van informatiebeveiliging (on)bewust zijn genomen. Echter zijn veel van deze maatregelen niet vastgelegd in procedure documenten. Er valt op dat veel activiteiten ad hoc worden uitgevoerd en door de praktijkmedewerkers zelf geregeld worden. Een voorbeeld hiervan is dat updates automatisch geïnstalleerd worden, maar de systemen periodiek per stuk worden langsgelopen om te controleren of dit ook netjes gebeurd. Ook valt op dat maatregelen die te maken hebben met personeel, toegang en verwerking van persoonsgegevens niet genomen zijn maar dat uitgegaan wordt van correcte naleving op basis van vertrouwen in de medewerkers en correcte handelingswijze geborgd is via de afgelegde eed.
In het interview komt tevens naar voren dat de kantoortijden bijna geheel aan patiënt gerelateerde activiteiten wordt besteed. Een groot deel van de administratieve werkzaamheden en alle onderhoudswerkzaamheden worden buiten de kantoortijden uitgevoerd.
Uit de doorgelopen maatregelen ten aanzien van de NEN7510 norm valt tevens op te maken dat er geen gedocumenteerde rapportages worden gemaakt of KPI’s worden bijgehouden als het gaat om informatiebeveiliging.

Focusinterviews

Op basis van de antwoorden van praktijk 0 en het werk van “Social engineering binnen de Nederlandse Rijksoverheid” (Spijker, 2017) is een nieuwe lijst met vragen samengesteld die het beeld van informatiebeveiliging van huisartsenpraktijken verder neerzet. De nieuwe vragenlijst is tevens getest bij een drietal huisartsen, die niet deelnemen aan de interviews, om te zien of deze lijst begrijpelijk en eenduidig opgesteld is. De volledige vragenlijst is opgenomen in bijlage 4.

Deze vragenlijst is verder gericht op het inzichtelijk krijgen van de maatregelen die genomen zijn rondom informatiebeveiliging. Hierbij wordt zowel gevraagd naar het gedocumenteerde deel als de praktische implementatie.

De focusinterviews zijn gehouden bij praktijken 1 t/m 5. Deze interviews zijn afgenomen op basis van de vastgestelde vragenlijst na het interview met praktijk 0. Ook de opnames van deze interviews zijn vervolgens geheel uitgewerkt en in de bijlage opgenomen.

Wat viel op na de focusinterviews?

Na het uitvoeren van de focusinterviews zijn de resultaten van deze vijf interviews én die van praktijk 0 naast elkaar gelegd.

Uit deze samenvoeging kan vervolgens feitelijke informatie gehaald worden over de antwoorden die gegeven zijn. De geïnterviewde praktijken kunnen de individuele vragen identiek, gedeeltelijk afwijkend of juist geheel verschillend beantwoorden. Hieronder zullen de relevante resultaten besproken worden, die de deelvraag “Hoe vullen huisartsenpraktijken informatiebeveiliging nu in?” moet beantwoorden.

Op basis van de hoofdstukken van de NEN7510 zullen de antwoorden van de gehouden interviews samengevat worden.

H5 - Beveiligingsbeleid en H6 - Organisatie van informatiebeveiliging

In de resultaten is te zien dat beantwoording van de vragen “welke functies en werkzaamheden vervult u en de andere medewerkers in de praktijk” en “kunt u een beschrijving van uw werkzaamheden en activiteiten op een reguliere werkdag geven?” beide gericht zijn op werkzaamheden rondom de patiënt en dat er geen enkele vermelding voorkomt van activiteiten die betrekking hebben op bijvoorbeeld informatiebeveiliging van systemen of informatiebeveiliging binnen de praktijk.

H7 - Beheer van bedrijfsmiddelen

Uit de resultaten blijkt dat gebruikte applicaties en systemen vrijwel altijd worden beheerd door een IT- of applicatie leverancier. Er wordt in deze situatie altijd uitgegaan, in de vorm van een aanname (zonder onderbouwing met behulp van rapportages) van de praktijkhouder, van gedegen onderhoud door deze partij.

H8 - Personeel

Ten aanzien van personeel zijn er werkinstructies beschikbaar in de praktijken. Deze zijn gericht op het goed omgaan met de applicaties en systemen. Overige procedures voor medewerkers, zoals screening en toegangsbeleid zijn veelal niet ingericht. Terugkerend antwoord is dat medewerkers al zeer lang in dienst zijn en dat er geruime tijd geen wijzigingen in de praktijk zijn geweest.

H9 - Fysieke beveiliging en beveiliging van de omgeving
In alle praktijken waar een interview is afgenomen, is de praktijk fysiek zo ingericht dat gesprekken tussen arts/assistent en patiënt niet afgeluisterd kunnen worden. Daarnaast zijn in alle gevallen ook gesloten ruimten aanwezig waar systemen van de praktijk aanwezig zijn. In bijna alle gevallen is hier bewust over nagedacht door de geïnterviewde huisartsen.

H10 - Beheer van communicatie- en bedieningsprocessen
Er is in alle gevallen een werkinstructie aanwezig voor gebruik van de HIS-applicatie en de belangrijkste toegangsprocedures voor medische applicaties. Wat betreft beheer en behandeling van informatie en informatiesystemen wordt dit uitgevoerd zoals de norm voorschrijft, echter er wordt hier geen logboek of andere vorm van rapportage van bijgehouden. Juist beheer en correcte verwerking door derden wordt aangenomen op basis van aangegane overeenkomsten.

H11 - Toegangsbeveiliging
Waar het gaat om toegangsbeveiliging hebben alle medewerkers hun eigen inloggegevens. Hierbij wordt zelden een wachtwoord gedeeld. Beleid omtrent deze toegang is er niet en inrichting is op basis van ad hoc gebruik en noodzaak van toegang. Controles op deze beveiliging zijn niet ingericht.

H12 - Verwerving, ontwikkeling en onderhoud van informatiesystemen
Er wordt in geen van de gevallen vooraf bewust nagedacht over eisen ten aanzien van informatiebeveiliging waar het gaat om aanschaf van nieuwe systemen. Wel worden eisen gesteld ten aanzien van beschikbaarheidswaarborgen in de vorm van SLA of garantieovereenkomst. Waar het gaat om updates en ander onderhoud wordt dit veelal door een externe IT-organisatie uitgevoerd. Waar dit niet het geval is wordt dit handmatig gedaan door een praktijkmedewerker.

H13 - Beheer van informatiebeveiligingsincidenten en H14 - Bedrijfscontinuïteitsbeheer
Mocht er bij de praktijken een IB-incident plaatsvinden zal dit in alle gevallen reactief worden opgepakt. Er zijn geen procedures aanwezig die voorschrijven hoe te acteren in dergelijke gevallen. Veiligstellen van patiëntinformatie door het maken van back-ups wordt via de leverancier van de HIS-applicatie geleverd. Hierbij wordt uitgegaan van de overeenkomst met deze partij die de juiste werking van de back-ups borgt.

H15 - Naleving
Kennis over de wet- en regelgeving die van toepassing is op het gebied van informatiebeveiliging is nagenoeg afwezig. Alle praktijken geven hierbij aan dat nascholing dit onderwerp ook niet of nauwelijks behandelt. Kennis over te nemen maatregelen komt de praktijk binnen via nieuwsbrieven of enthousiaste collega's.

Als laatste geven alle praktijken aan dat beveiliging van de patiëntrelatie en -informatie zeer belangrijk is. Ze geven hierbij aan dat informatiebeveiliging voornamelijk tijd en geld zal kosten, maar dat het nu eenmaal moet.

Net als bij praktijk 0 laten de interviews zien dat op alle vragen een antwoord gegeven kan worden waaruit de invulling van maatregelen op het gebied van informatiebeveiliging blijkt. Er wordt veel gedaan op basis van de professionaliteit van en het vertrouwen in de medewerkers. Er worden echter geen rapportages gemaakt of KPI's bijgehouden. De verdere uitwerking van de enquêtevragen zal in dit geval gericht moeten worden op vragen over "hoe doe je", "wat is er geregeld" en "wie doet". Vragen over specifieke performance en doelstellingen in de vorm van KPI's zullen waarschijnlijk niet of negatief beantwoord worden. In het kader van optimalisatie van de enquête zullen deze worden weggelaten.
Wat verder vermeld kan worden is dat van de zes geïnterviewde praktijken er vier geen praktijkaccreditering hebben en twee wel.

Enquête
Voor de enquête zijn mailadressen verzameld van actieve huisartsen. Voor het krijgen van toegang tot e-mailadressen is gebruik gemaakt van openbare boekwerken (Geneeskundig adresboek) en internetsites van huisartsen zelf. Daarnaast zijn deze gegevens verkregen via navraag bij de huisartsenpraktijken (in persoon of per telefoon). In totaal zijn 1080 mailadressen verzameld.
Na het versturen van alle mailberichten is vastgesteld dat er 490 berichten niet af te leveren waren. Daarnaast zijn er 23 reacties geweest van huisartsen die nog wel BIG-geregistreerd waren maar niet meer zelf actief. Hierdoor blijft er een potentiele reactiebasis over van 567 gemailde huisartsen.

Enquêteresultaten hebben betrekking op 79 respondenten met een volledige enquête die binnen de onderzoeksscope vallen. Dit is een reactiepercentage van ongeveer 14%.

Vertegenwoordiging van het percentage respondenten per stad is via www.kiesuwhuisarts.nl verkregen. Bij navraag heeft NIVEL aangegeven dat deze site de volledige dataset huisartsenpraktijken bevat, maar voor aantallen er handmatig moet worden geteld per stad. Actualiteit van de dataset is onbekend.

Alléén voor Den Haag, Zoetermeer en Rijswijk waren de respondentaantallen hoog genoeg om significantie te controleren. Dit was in alle gevallen hoger dan 5% (Den Haag 16 uit 170, Zoetermeer 5 uit 53 en Rijswijk 12 uit 15 huisartsenpraktijken) op basis van een snelle optelsom van de huisartsenpraktijken de genoemde website. De response van Zoetermeer is hierbij wel hoger dan 5% maar resultaten kunnen beoordeeld worden als twijfelachtig vanwege het zeer beperkte absolute aantal respondenten.

Opvallende resultaten uit de enquêteresultaten?
Gekeken naar de beantwoording van de enquêtevragen kan het resultaat daarvan ook tegen de eerder gemaakte samenvatting van de interviews gelegd worden.

Een verschil tussen de interviews en enquête kan gevonden worden in het percentage praktijken met een NHG-praktijkaccreditering. Dit is in de enquête ongeveer 80% geaccrediteerde praktijken versus 20% niet-geaccrediteerde praktijken. Dit was bij de interviews vier niet-geaccrediteerde en twee geaccrediteerde (ongeveer 67% niet en 33% wel) praktijken.

Als verder naar de resultaten van de enquête gekeken wordt, komt naar voren dat in de resultaten ongeveer de helft van de praktijken een verantwoordelijke hebben aangewezen voor informatiebeveiliging in de organisatie. Daarnaast laten de resultaten zien dat ongeveer de helft van de praktijken beleid voor informatiebeveiligingsincidenten heeft, voornamelijk bij praktijken met een accreditering. Ook neemt een grote meerderheid van de praktijken informatiebeveiligingsaspecten mee in de beslissing voor aanschaf van nieuwe applicaties en medische apparatuur. Deze resultaten wijken af van de interviewresultaten, waar in geen enkel geval beleid was voor informatiebeveiligingsincidenten of bewust nagedacht wordt over informatiebeveiliging bij aanschaf van applicaties of systemen.

Resultaten ten aanzien van onderhoud en beheer van systemen laten eenzelfde beeld zien als in de interviews reeds is geschetst. Ook de resultaten ten aanzien van werktijd laten zien dat administratieve en onderhoudstaken niet passen binnen de reguliere werktijd van de respondent.

Alle praktijken, ongeacht wel of geen accreditatie, geven aan dezelfde minimale set fysieke beveiligingsaspecten te hanteren (gesloten ruimten en andere maatregelen ten aanzien van afluisteren). Dit komt tevens overeen met de resultaten die bij de praktijken uit de interviews is waargenomen.

Waar het gaat om toegang worden zo af en toe wachtwoorden gedeeld. Dit komt ook overeen met de resultaten uit de interviews. Opgemerkt kan worden dat ongeveer 1/5 van de praktijken aangeeft nooit wachtwoorden van medewerkers te vervangen als deze de organisatie verlaat. Het resultaat van de interviews dat er geen controles plaatsvinden op de toegangsbeveiliging komt hiermee overeen.

Net als bij de interviews geeft het grootste deel van de praktijken aan dat beveiliging van de patiëntrelatie en -informatie zeer belangrijk is. Ze geven hierbij aan dat informatiebeveiliging voornamelijk tijd en geld zal kosten, maar dat het nou eenmaal moet als gekeken wordt naar de gewenste patiëntrelatie en naar de wetgeving.

<u>Verschillen wel of geen praktijkaccreditatie</u>
Naast het bekijken van individuele resultaten van de interviews en enquêtes is gezocht naar een verschil tussen de praktijken die geen NHG-accreditatie bezitten en de praktijken die deze accreditatie wel bezitten.

Er is alléén naar verschil op basis van dit aspect gezocht, omdat deze waarde voldoende resultaten heeft opgeleverd om een vergelijking te kunnen maken met enige significante uitkomst. Door dit te doen wordt de deelvraag “Zijn er verschillen te vinden bij de invulling van informatiebeveiliging tussen huisartsenpraktijken?” tevens beantwoord.

Er zijn significante verschillen gevonden op basis van groepen wel/geen NHG-accreditering bij beantwoording van vragen 5, 6, 7, 22 en 35 die hieronder verder zullen worden uitgelicht. Een volledig overzicht van de statistische analyse die gedaan is, is opgenomen in bijlage 7.

- Vraag 5: Hoeveel patiënten heeft de praktijk (ongeveer)?

	Hele dataset	Met NHG	Zonder NHG
Minimale waarde:	1200	1200	1300
Maximale waarde:	15000	15000	10000
Gemiddeld:	4945	5382	3349
Standaardafwijking:	3245	3390	1939

- Vraag 6: Hoeveel medewerkers heeft de praktijk?

	Hele dataset	Met NHG	Zonder NHG
Minimale waarde:	2	2	3
Maximale waarde:	50	50	25
Gemiddeld:	12,14	13,56	6,94
Standaardafwijking:	8,77	9,00	5,23

- Vraag 7: Hoeveel uren werkt u gemiddeld op een werkdag?

	Hele dataset	Met NHG	Zonder NHG
Minimale waarde:	5	5	9
Maximale waarde:	12	12	11
Gemiddeld:	9,44	9,35	9,74
Standaardafwijking:	1,54	1,70	0,55

- Vraag 22: Wordt bij telefonisch overleg de identiteit van de andere partij (bv. specialist) geverifieerd voordat patiëntinformatie gedeeld wordt?

Antwoordkeuze	**Hele dataset**	**Met NHG**	**Zonder NHG**
Altijd	20 (25,32%)	18 (29,03%)	2 (11,76%)
Meestal	22 (27,85%)	19 (30,65%)	3 (17,65%)
Soms	10 (12,66%)	10 (16,13%)	-
Bijna nooit	17 (21,52%)	10 (16,13%)	7 (41,18%)
Nooit	10 (12,66%)	5 (8,06%)	5 (29,41%)

- Vraag 35: Hoe groot zijn volgens u de gevolgen voor de praktijk als vertrouwelijke informatie op straat komt?

Antwoordkeuze	**Hele dataset**	**Met NHG**	**Zonder NHG**
Groot	16 (20,25%)	10 (16,13%)	6 (35,29%)
Middel	45 (56,96%)	36 (58,06%)	9 (52,94%)
Klein	14 (17,72%)	12 (19,35%)	2 (11,76%)
Anders, namelijk	4 (5,06%)	4 (6,45%)	-

Onder “anders, namelijk:” werd “weet niet” 3x geantwoord en 1x “hangt van de situatie af”.

7. Discussie

In dit hoofdstuk zullen de aspecten worden behandeld die de waarde van de onderzoeksresultaten beïnvloeden en die moeten worden meegenomen bij de beoordeling van de resultaten en uiteindelijke conclusies door de lezer van dit document.

De onderzoeker/interviewer heeft geen psychologie achtergrond. Dit feit is meegenomen in het ontwerp van dit onderzoek om negatieve effecten ten aanzien van de betrouwbaarheid, voortkomend uit dit feit, teniet te doen. De gestelde vragen zijn niet getoetst op optimale beantwoording in termen van bijvoorbeeld sturende eigenschappen en wenselijke beantwoording. Wel is eerder onderzoek naar informatiebeveiliging gebruikt om als gevalideerd instrument in te zetten. Ook zijn de vragen voorafgaande aan de interviews en enquêtes getest bij een groep huisartsen die niet deelneemt aan de enquête of interviews. De reden hiervan is om dit onderzoek vergelijkbaar te maken en kwaliteit van eerder onderzoek te benutten om de betrouwbaarheid te verbeteren. Surveymonkey is gebruikt voor het verwerken van enquêtereacties en het voorkomen van fouten in de resultaten.

Er is zo veel mogelijk rekening gehouden met negatieve invloeden die de respondent kan voelen ten aanzien van het invullen van de enquête en de invloeden die hem verhinderen de vragen eerlijk te beantwoorden. Dit is gedaan door vooraf aan te geven dat privacy gegarandeerd blijft en eerlijke antwoorden helpen bij een juist beeld van de werkelijke situatie. Hierdoor wordt zo veel als mogelijk gezorgd dat de respondent geen kwetsbaarheid voelt ten aanzien van zijn eigen individu.

Voor verschil tussen wel/geen NHG-accreditatie is T-toets gebruikt. Door deze toets is géén richting te geven aan het gevonden resultaat. Daarnaast is de steekproef beperkt dus kunnen er andere invloeden meespelen bij het verkrijgen van deze cijfers zonder dat deze zichtbaar worden in de verkregen resultaten.

Ten aanzien van de totale onderzoekspopulatie is geen valide steekproef gehaald, zoals vooraf was ingeschat. Er is ook te zien dat een overgroot deel van de respondenten uit de regio Den Haag komt. Dit maakt de generaliseerbaarheid richting “Randstadsteden” onvoldoende geldig. Op basis van de cijfers is naar individuele steden Den Haag en Rijswijk wel te generaliseren.

Er zijn, naast de overwegingen die reeds in de tekst besproken zijn, verschillende aspecten overwogen om dit onderzoek invulling te geven. Zo is er een volgordelijkheid in de vragenlijst aangebracht omdat deze informatie naar de praktijk brengt. Daardoor wordt de basiskennis van deze praktijk veranderd. Er is zo veel mogelijk geprobeerd de volgorde van vragen zo neer te zetten dat eerdere vragen geen invloed hebben op beantwoording van latere vragen.
Er is binnen dit onderzoek uitgegaan van drie typen praktijken, namelijk solo-, duo- en groepspraktijken. Dit zijn de drie typen praktijken waar onderscheid in wordt gemaakt in onder andere “Zo werkt het in de huisartsenpraktijk” (Dolmans, 2009) en “Een eigen Praktijk” (Fisscher & van Bemmel, 2015). Andere groepsindelingen, zoals op basis van medewerkers, zijn niet gebruikt. Er is gekozen om niet op basis van andere karakteristieken (zoals aantal medewerkers of stad) te groeperen omdat het aantal resultaten niet voldoende zou zijn om er gegronde uitspraken over te kunnen doen.

Er is door de onderzoeker gekozen om de scope van respondenten beperkt te houden. Zo zijn leveranciers uitgesloten van deelname aan dit onderzoek. Dit is gedaan om het verkrijgen van toegang beperkt te houden tot interne medewerkers van de praktijken en de doorloop van het onderzoek enigszins onder controle te houden. Het verkrijgen van toegang tot leveranciers van de praktijken zou hebben betekend dat er meerdere malen contact zou moeten zijn met de praktijk. Dit is in de onderzoeksaanpak uitgesloten als mogelijkheid omdat dit het aantal respondenten ernstig zou beperken en de doorloop van dit onderzoek ernstig in gevaar zou brengen.

Als laatste is overwogen één onderzoeksmethode aan te houden ten aanzien van de twee (case study en enquête) die nu zijn gebruikt. Door het gebruik van meerdere methoden wordt het uiteindelijk onderzoeksresultaat namelijk onvoorspelbaar. Zo kunnen de enquêteresultaten de resultaten van de interviews tegenspreken. De resultaten van beide methoden kunnen echter wel van belang zijn en daarom zullen beide aangehouden worden. Tevens is het bereiken van een grotere populatie binnen een beperkte tijd alleen mogelijk bij gebruik van enquêtes en het verkrijgen van zeer diepgaande informatie alleen via interviews. Deze twee zijn nodig om enige waarde aan dit onderzoek te kunnen geven zodat het als basis kan dienen voor volgende onderzoekers.

8. Conclusies en aanbevelingen

Er zijn aan de hand van de resultaten een aantal aanbevelingen te vinden. Vanwege de beperkte set respondenten kunnen de conclusies niet als statistisch significant aangenomen worden voor de scope “huisartsenpraktijken in de Randstad”. Gemaakte conclusies blijven hierbij beperkt tot de individuele steden Den Haag en Rijswijk.

Daarnaast is er een verschil aanwezig tussen het wel of niet aanwezig zijn van NHG-accreditering in praktijken bij de resultaten van de interviews en enquêtes. Dit is wellicht te verklaren door het verschil in grootte van het gebied waar de interview of de enquêtes werden afgenomen. Hierbij is het waarschijnlijk dat de enquêteresultaten het juiste beeld tonen van deze resultaten.

In de resultaten zijn de eerste vier deelvragen reeds beantwoord. De laatste deelvraag “Zijn er gemeenschappelijke aanbevelingen te vinden die de staat van informatiebeveiliging verder kunnen bevorderen?” is aan de hand van de resultaten nu ook te beantwoorden.

Uit de interviews bleek dat er een opvallend verschil aanwezig is tussen NHG geaccrediteerde huisartsenpraktijken en niet-geaccrediteerde praktijken waar het gaat om het hebben van een duidelijk beeld van de werking van processen en benodigdheden voor informatiebeveiliging binnen de organisatie. De enquêteresultaten laten eenzelfde verschil zien waar het gaat om het hebben van een vaste plek voor informatiebeveiliging in overleggen, van een aangewezen verantwoordelijke voor informatiebeveiliging en van genomen beslissingen t.a.v. de aanschaf van applicaties en systemen mede op basis van informatiebeveiligingsaspecten.

De accreditatie van een huisartsenpraktijk zou hierbij een positieve relatie hebben met een goede invulling van alle losse aspecten van informatiebeveiliging binnen de organisatie. De richting van deze relatie is echter niet aangetoond in dit onderzoek. Aan te bevelen is dat praktijken de kennis- en processtappen ondernemen die bij een accreditering horen om individuele maatregelen, en de kennis daarover, ten aanzien van informatiebeveiliging beter te borgen in de organisatie. Een verdere verhoging van het aantal geaccrediteerde huisartsenpraktijken zou van deze stappen een logisch gevolg zijn en mogelijk bijdragen aan het borgen van de genomen stappen in de organisatie.

Op basis van de beantwoording van alle deelvragen is nu ook een antwoord te geven op de vraagstelling van dit onderzoek: “Welke maatregelen nemen huisartsenpraktijken in het kader van informatiebeveiliging?”

Uit de resultaten kan geconcludeerd worden dat huisartsenpraktijken informatiebeveiliging in hun organisatie zelf veelal op een ad hoc en reactief niveau geregeld hebben en er diverse punten tot verbetering zijn.
Als gekeken wordt naar andere onderdelen van de NEN7510 zijn voornamelijk de maatregelen voor personeel onvoldoende toegepast en veelal gebaseerd op basis van vertrouwen, artseneed en jarenlang dienstverband. Waar het gaat om fysieke beveiliging lijken alle praktijken voldoende te scoren. Uit de interviews kwam naar voren dat dit zichtbare maatregelen (met direct zichtbare positieve consequenties) zijn. Dit kan een reden zijn dat deze maatregelen daardoor zo compleet zijn toegepast.

Waar het gaat om de systemen en patiëntinformatie wordt beheer en onderhoud bijna altijd uitbesteed aan de IT- of applicatieleverancier. Hiervoor is, zo blijkt uit de interviews, de overeenkomst met deze partij voldoende om aan te nemen dat dit beheer en onderhoud goed uitgevoerd wordt. Kennis hierover en inzicht in de uitvoering is echter afwezig binnen de praktijk en daarom niet beschikbaar in dit onderzoek.

Wat naast dit beeld nog opvalt is dat alle praktijkhouders véél werk buiten kantoortijden verrichten (+12 uren p.d.). Dit is naar voren gekomen in zowel de interviews als de enquêtes.

Uit de interview- en enquêteresultaten kan tevens geconcludeerd worden dat alle respondenten de beveiliging van patiëntinformatie uiterst belangrijk vinden en de kosten daarvan minder relevant. Voornamelijk de eigen tijdsinvestering voor onderhoud van systemen en bijhouden van kennis is echter summier en hoogstwaarschijnlijk te weinig om verdere stappen te maken in de informatiebeveiliging binnen de organisatie. Het verder professionaliseren door middel van praktijkaccreditatie en het aannemen van externe hulp bij invulling van informatiebeveiliging binnen de praktijk is daarmee onvermijdelijk.

Dit onderzoek kan als basis gezien worden voor het verkrijgen van inzicht naar de invulling van informatiebeveiliging bij huisartsenpraktijken. Vanwege de beperkingen in tijd en scope is er echter voor een beperkte populatie resultaten behaald.

Vervolgonderzoek is gewenst bij een grotere populatie. Gezien de positieve reacties van huisartsen ten aanzien van mailberichten vanuit artsenorganisaties is een poging tot deelname van deze organisaties aan de verspreiding van dergelijke onderzoeken aan te bevelen als vervolgonderzoek uitgevoerd wordt.

9. Reflectie

In dit hoofdstuk wordt teruggekeken op het uitgevoerde onderzoek en de getrokken conclusies. In dit onderzoek is er een aantal stappen ondernomen om de kwaliteit van het onderzoek en de daaruit verkregen resultaten te verhogen. Zo is vooraf nagedacht over de te nemen stappen en over de mogelijke uitkomsten. Daarnaast is vooraf neergezet wat er tijdens de verwerking en resultaten gedaan zal worden om zo herhaalbaarheid en inzichtelijkheid te creëren. In de discussie is bekeken of de resultaten nog in hetzelfde licht bekeken konden worden als vooraf vastgesteld. Terugkijkend op het onderzoek kunnen er wel een aantal verbeteringen worden gemaakt.

Gekeken naar de definitie van de scope is het aanhouden van “de Randstad” als scope geen goede keuze geweest om twee redenen. De eerste reden is dat de definitie niet vastligt. Hiermee zijn de steden die wel of niet binnen de scope passen niet voor elke onderzoeker hetzelfde en dit verlaagt de kwaliteit van het onderzoek. Dit is zo veel als mogelijk tenietgedaan door alle meegenomen steden in een overzicht op te nemen. De tweede reden is dat de hoeveelheid respondenten voor een significante steekproef hiermee ver buiten de beperkte tijdsscope van dit onderzoek liggen. De hoeveelheid geïnvesteerde tijd voor het verkrijgen van toegang tot respondenten voor de enquête is bij nader inzien te hoog geweest voor de scope “de Randstad”. Het aantal werkelijk behaalde respondenten is lager geweest dan de scope doet vermoeden. Gezien de harde tijdsbeperking had de scope “de Randstad” niet gekozen moeten worden.

Er is vooraf niet met de geïnterviewde praktijken gesproken over de verzending van de mailing aan de beoogde respondenten van de enquête. Dit had wellicht gezorgd dat de verdere optimalisatie van reacties door de extra vrijdagverzending reeds in de voorbereiding opgemerkt had kunnen worden en is daarmee een leermoment voor de onderzoeker geweest.

Gekeken naar de persoonlijke situatie van de onderzoeker is dit onderzoek ook een opgave gebleken. Bij de start van dit onderzoek waren de geboorte van een zoon en de aankoop van een nieuw huis niet in zicht, maar deze zijn er wel gekomen. Met beperkende gebeurtenissen (ten aanzien van het onderzoek) is echter geen rekening gehouden. Achteraf gezien hebben deze punten gezorgd voor uitloop ten opzichte van de geplande eindtijd van het onderzoek en hebben deze punten ook gezorgd voor een beperking van de beschikbare energie die juist nodig was om dit onderzoek af te ronden. Opname van “wat lucht” in de planning had dit wellicht voorkomen.

Door de langere doorlooptijd zijn de resultaten ook wat minder relevant geworden. Dit komt door de continue aandacht voor het onderwerp informatiebeveiliging in de media en artsenorganisaties die een lerend effect op de praktijken zal hebben. Ik verwacht echter dat de doorlooptijd kort genoeg is dat er zeker nog leerpunten uit het onderzoek gehaald kunnen worden voor zowel andere onderzoekers als de praktijk.

De conclusies die in het onderzoek gemaakt zijn, zijn wat mij betreft voldoende geborgd door gebruik van gevalideerde instrumenten en voldoende voorbereiding ten aanzien van het wegnemen van onzekere factoren. Dit resultaat moet wel in het licht van de beperkte scope gezien worden.

Wat betreft deze reflectie zou ik willen afsluiten met een quote die ik, komende bij het einde van dit onderzoek, ben gaan zien als mijn grootste weerstand en struikelblok.

“The more something threatens your identity, the more you will avoid doing it.”
-- Manson’s law of Avoidance, link: https://markmanson.net/procrastination

Referenties

CIBG, a. BIG-register. Retrieved from https://zoeken.bigregister.nl/zoeken

College Bescherming Persoonsgegevens. (2015, 21-9-2015). De meldplicht datalekken in de Wet bescherming persoonsgegevens (Wbp). *Consultatieversie.* Retrieved from https://www.cbpweb.nl/sites/default/files/atoms/files/richtsnoeren_meldplicht_datalekken.pdf

Dolmans, A. J. (2009). Zo werkt het in de huisartsenpraktijk: Bohn Stafleu van Loghum.

Fisscher, Y., & van Bemmel, C. (2015). Een eigen praktijk. In Y. Fisscher & C. van Bemmel (Eds.), (pp. 97-104): Bohn Stafleu van Loghum.

Inspectie voor de Gezondheidszorg. (2008). Informatiebeveiliging ziekenhuizen voldoet niet aan de norm: Inspectie voor de Gezondheidszorg.

Kotz, D., Fu, K., Gunter, C., & Rubin, A. (2015). Security for Mobile and Cloud Frontiers in Healthcare. *Communications of the ACM, 58*(8), 21-23. doi:10.1145/2790830

Maastricht-University. Voor onderzoekers. Retrieved from http://www.huisartsgeneeskundemaastricht.nl/wat-bieden-wij/onderzoek/voor-onderzoekers.html

MacGregor, R. C., Hyland, P. N., & Harvie, C. (2009). Do organisational characteristics explain the differences between drivers of ICT adoption in rural and urban general practices in Australia? *Australasian Journal of Information Systems, 16*(1), 77-97.

Nederlands Huisartsen Genootschap. (2009). Informatiebeveiliging in de huisartsenpraktijk *NHG-PraktijkWijzer*.

NEN.nl. (2011). NEN7510:2011. *Medische informatica - Informatiebeveiliging in de zorg.* Retrieved from https://www.nen.nl/NEN-Shop/Norm/NEN-75102011-nl.htm

Nijgh-Periodieken. (2003). *Geneeskundig Adresboek Nederland (2003-2004)*: Nijgh Periodieken B.V.

Otten, M. (2013). De interne communicatietaken van medewerkers en managers: Universiteit Twente.

Ploem, M. C., Zwaanswijk, M., Wiesman, F. J., Verheij, R. A., Friele, R. D., & Gevers, J. K. M. (2011). *Vertrouwen van zorgverleners in elektronische informatie-uitwisseling en het landelijk EPD: een juridische en sociaal-wetenschappelijke studie naar de positie van zorgverleners* (9789071433825). Retrieved from Amsterdam/Utrecht: http://www.nivel.nl/sites/all/modules/wwwopac/adlib/publicationDetails.php?database=ChoicePublicat&priref=1001999

Saunders, M., Lewis, P., Thornhill, A., Booij, M., & Verckens, J. P. (2011). *Methoden en technieken van onderzoek*: Pearson Education.

SecurityIntelligence. All in a Spammer's Workweek: Where Do the Busiest Spammers Work Around the Clock? Retrieved from https://securityintelligence.com/all-in-a-spammers-workweek-where-do-the-busiest-spammers-work-around-the-clock/

Spijker, D. (2017). Social engineering binnen de Nederlandse Rijksoverheid: Open Universiteit.

Wel, J. v. d. (2006). Informatiebeveiliging in de zorg.

Bijlage 1 – Steden opgenomen in de scope van het onderzoek

In deze bijlage is een overzicht opgenomen van alle steden waarvan de huisartsen zijn opgezocht in het Geneeskundig adresboek en via andere zoekmethoden die beschreven zijn in deze studie.

Aalsmeer
Albrandswaard
Almere
Alphen aan de Rijn
Amersfoort
Amstelveen
Amsterdam
Apeldoorn
Arnhem
Barendrecht
Beemster
Bennebroek
Bergen
Beverwijk
Blaricum
Bloemendaal
Boskoop
Breda
Brielle
Bunnik
Bussum
Capelle aan den IJssel
Capelle ad IJssel
De Bilt
Delft
Den Bosch
Den Haag
Diemen
Dordrecht
Edam-Volendam
Gooise Meren
Gouda
Haarlem
Haarlemmerliede
Haarlemmermeer
Heemskerk
Heemstede
Heerhugowaard
Hellevoetsluis
Hendrik-Ido-Ambacht
Hillegom
Hilversum
Houten
Huizen
IJsselstein
IJsselstein en Zeist
Katwijk
Krimpen aan den Ijssel
Landsmeer
Lansingerland
Laren
Leiden
Leiderdorp
Leidschendam-Voorburg
Lisse
Maarssen
Maassluis
Maastricht
Midden-Delfland
Naarden
Nieuwegein
Nijmegen
Nissewaard
Oegstgeest
Oostzaan
Ouder-Amstel
Papendrecht
Pijnacker-Nootdorp
Purmerend
Ridderkerk
Rijswijk
Rotterdam
Schiedam
Sliedrecht
Soest
Spaarnwoude
Spijkenisse
Stichtse Vecht
Tilburg
Uithoorn
Utrecht
Velsen
Vianen
Vlaardingen
Voorschoten
Waddinxveen
Wassenaar
Waterland
Weesp
Westland
Westvoorne
Woerden
Wormerland
Zaanstad
Zandvoort
Zoetermeer
Zuidplas
Zwijndrecht
Zwolle

Bronnen die voor deze samenstelling zijn gebruikt:
https://zoek.officielebekendmakingen.nl/stcrt-2010-14074.html
https://nl.wikipedia.org/wiki/Utrecht_(agglomeratie)
https://nl.wikipedia.org/wiki/Randstad_(gebied)
https://www.infomil.nl/onderwerpen/geluid/uitvoering-kartering/uitvoering-nederland/aanwijzing-overheden/
http://www.Randstadregion.eu/uploads/2017/07/Randstad-monitor-2016.pdf

Bijlage 2 - Onderzoekmethodes

In deze bijlage is de tabel met de verschillende onderzoekmethodes opgenomen. Deze tabel is samengesteld op basis van de methoden beschreven in Saunders (2005) en geeft een korte omschrijving per methode wat voor onderzoek het is, wat de functie van de methode is, wat voor vraagstelling erbij past en of deze methode geschikt is voor dit empirisch onderzoek.

Type onderzoek	**Omschrijving**	**Onderzoek naar**	**Geschikt?**	
Het experiment	Bestuderen van causale verbanden	Verschil/samenhang	Nee	
De enquête	Methode om gestructureerd te interviewen, kwantitatieve gegevensverzameling	Wie, wat, waar en hoeveel	Ja	
De casestudy	Onderzoek van een bepaald hedendaags verschijnsel	Waarom, wat en hoe?	Ja	
'action research'	Onderzoek naar oplossen van problemen via verandering	Hoe?	Nee	
De 'grounded theory'	Opbouwen van theorie of model	Gedrag voorspellen of verklaren	Nee	
De etnografie	Beschrijven en verklaren van de wetenschappelijke wereld van de betrokkene, vanuit hun perspectief	Inzicht in context van betrokkene	Nee	
archiefonderzoek	Onderzoek over administratieve gegevens en documenten	Beschrijven over verleden of veranderingen	Nee	

Onderstaande teksten zijn 1-op-1 overgenomen uit Saunders (2005) en zijn extra uitleg voor de tekst die in hoofdstuk 4.1 is opgenomen met onderwerp onderzoeksstrategie.

Het experiment

Het doel van een experiment is het bestuderen van causale verbanden, om na te gaan of er verandering in één onafhankelijke variabele een verandering teweegbrengt in een andere, afhankelijke variabele (Hakim, 2000).

We gebruiken experimenten daarom over het algemeen in verklarend onderzoek om 'verschil' vragen en 'samenhang'-vragen te kunnen beantwoorden.

In het klassiek experiment zijn er twee groepen, waarvan de leden willekeurig over de groepen zijn verdeeld. Dit betekent dat de twee groepen exact gelijksoortig zijn in alle aspecten die relevant zijn voor het onderzoek, behalve dat de ene groep wél en de andere groep niet aan de geplande interventie of manipulatie wordt blootgesteld.

De afhankelijke variabele, […] wordt gemeten vóór en na de manipulatie van de onafhankelijke variabele voor zowel de experimentele groep als voor de controlegroep. Zo kan er een vergelijking tussen de groepen vóór en na de interventie worden gemaakt.

De etnografie

Het doel ervan is het beschrijven en verklaren van de maatschappelijke wereld waarin de onderzochte personen leven, op de manier zoals zij die zouden beschrijven en verklaren.

De enquête

De enquête wordt ingezet wanneer is besloten om gestructureerd te interviewen […] en wordt het meest gebruikt om 'wie, wat, waar en hoeveel'-vragen te beantwoorden.

Ze maken het mogelijk om op zeer economische wijze een grote hoeveelheid gegevens uit een omvangrijke populatie te verzamelen. Deze gegevens, vaak verkregen met behulp van een gestructureerde vragenlijst, worden gestandaardiseerd, waardoor we ze gemakkelijk kunnen vergelijken.

De casestudy

De casestudy is 'een methode voor het doen van onderzoek die gebruikmaakt van een empirisch onderzoek van een bepaald hedendaags verschijnsel binnen de actuele context, waarbij van verschillende soorten bewijsmateriaal gebruikt wordt gemaakt'.

De casestudy is vooral interessant als je een goed begrip wilt krijgen van de context van het onderzoek en de processen die worden doorlopen (Morris en Wood, 1991). Deze methode is heel geschikt voor het geven van antwoorden op de vraag 'waarom?', en ook op de vragen 'wat?' en 'hoe?'. Daarom gebruiken we de casestudy meestal in verklarend en verkennend onderzoek.

We kunnen verschillende methoden toepassen voor het verzamelen van gegevens. Vaak worden ze in combinatie met elkaar gebruikt. Dit kunnen onder andere zijn: interviews, waarneming, documentaire-analyse en vragenlijsten.

Als je een casestudymethode volgt, moet je waarschijnlijk verschillende gegevensbronnen gebruiken en trianguleren. Met triangulatie bedoelen we het gebruik van verschillende methoden voor het verzamelen van gegevens om er zeker van te zijn dat de gegevens je werkelijk vertellen wat je denkt dat ze je vertellen.

'action research'

Action research verschilt […] van andere vormen van toegepast onderzoek door de expliciete nadruk op actie, namelijk het bevorderen van veranderingen binnen het bedrijf. Het is daarom bijzonder geschikt voor de 'hoe'-vragen.

De 'grounded theory'

Je kunt het […] zien als het 'opbouwen van een theorie of model' door een combinatie van inductie en deductie. Een 'grounded-theory'-model os volgens Goulding (2002) vooral nuttig voor onderzoek waarin wordt geprobeerd om gedrag te voorspellen en te verklaren, en waarbij de nadruk ligt op het ontwikkelen van een theorie of model.

Archiefonderzoek

Archiefonderzoek, waarin administratieve gegevens en documenten de voornaamste bron van gegevens zijn. Hoewel de term 'archief' een historische betekenis suggereert, kan het zowel op recente als op historische documenten slaan (Bryman, 1989).

Een archiefonderzoekmethode maakt onderzoeksvragen mogelijk die gericht zijn op het verleden en de veranderingen in de loop van de tijd, of ze nu verkennend, beschrijvend of verklarend zijn.

Bijlage 3 - Communicatietemplates

Voorbeeld belscript eerste contact aanvraag tot afnemen interviews:

“Goedendag met Jeroen Bakker,

Op dit moment ben ik bezig met een onderzoek naar informatiebeveiliging bij huisartsenpraktijken.

Uw praktijk is voor mij interessant omdat het valt binnen de scope van mijn onderzoek.
Mijn onderzoeksdoel is tweeledig;
- Mijn studie afronden met een bijdrage aan de wetenschappelijke literatuur voor informatiebeveiliging bij huisartsenpraktijken
- Praktijken voorzien van verbeterpunten voor hun eigen praktijk

Graag maak ik met U een afspraak voor dit interview, wat ongeveer één uur zal duren.

Uiteraard zal het gehele interview en uitwerking daarvan vertrouwelijk behandeld worden en zal slechts de vestigingsplaats van de praktijk gepubliceerd worden omdat deze relevant is voor de scope van het onderzoek.
Praktijknamen zullen wel (apart van het onderzoek) kenbaar gemaakt worden aan de toetsingscommissie van de opleiding ter verificatie van een juist afstudeerproces.

Bent U geïnteresseerd dan kan ik de resultaten van het onderzoek na afloop naar u toezenden. “

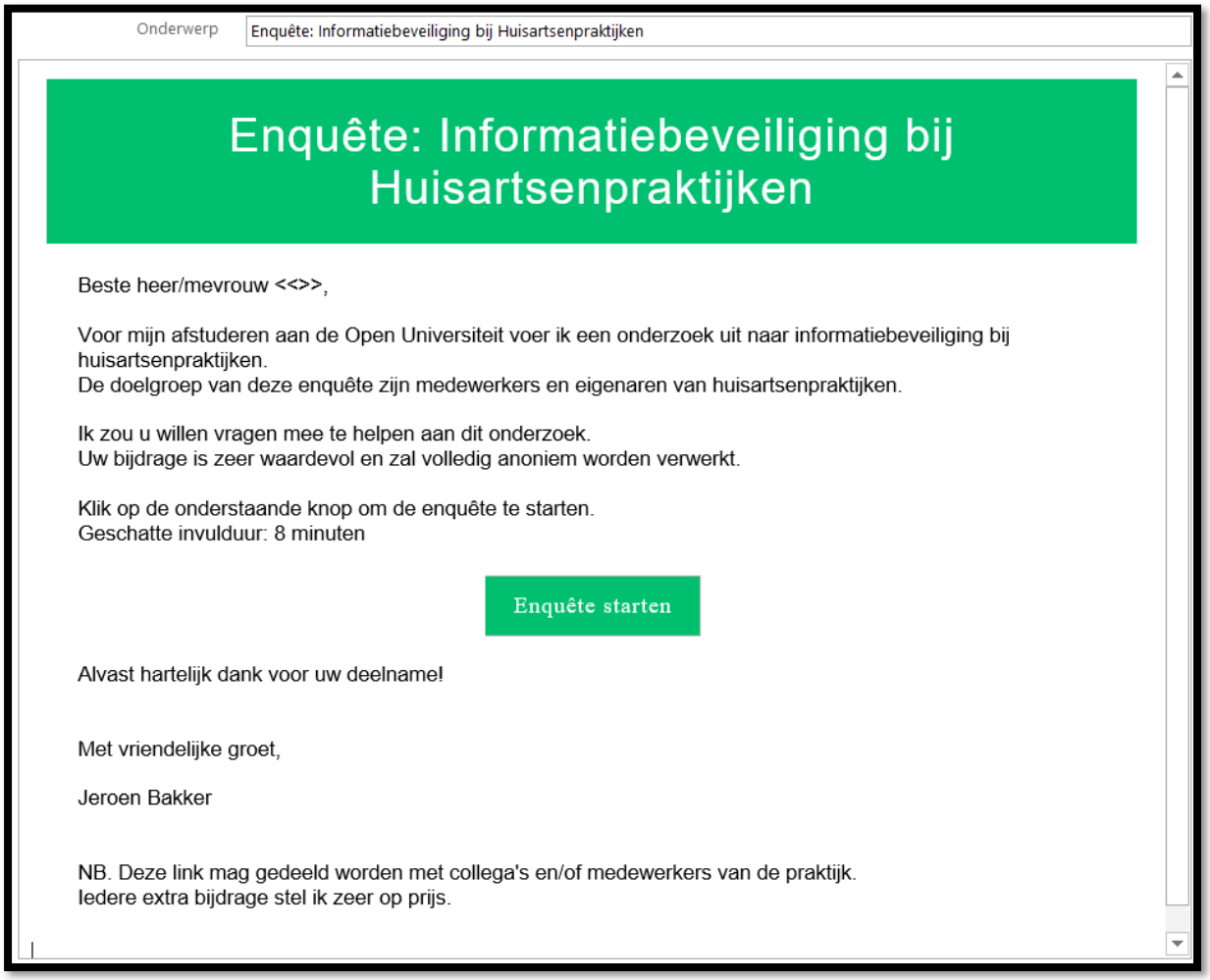
Voorbeeld belscript eerste contact aanvraag tot afnemen enquêtes:

“Goedendag met Jeroen Bakker,

Op dit moment ben ik een onderzoek aan het houden naar informatiebeveiliging bij huisartsenpraktijken in de Randstad. Op dit moment houd ik een diepte-interview bij praktijken in de regio Den Haag en wil ter verificatie van de resultaten een aantal korte vragen stellen. Ik begrijp dat u het druk heeft, maar zou graag deze korte vragenlijst naar u toesturen. Mag ik van u een e-mailadres waarheen dit gestuurd kan worden? Uiteraard zullen de antwoorden vertrouwelijk behandeld worden en zal slechts de vestigingsplaats van de praktijk genoemd worden omdat deze relevant is voor de scope van het onderzoek.

Bent U geïnteresseerd dan kan ik de resultaten van het onderzoek na afloop naar u toezenden. “

Voorbeeld e-mail aanvraag tot afnemen enquêtes:



Voorbeeld e-mail herinnering aanvraag tot afnemen enquêtes (zelfde als hierboven, inclusief onderstaande toegevoegde eerste alinea):

Het zou kunnen zijn dat eerdere berichtgeving ten aanzien van deze enquête aan uw aandacht is ontsnapt. Echter uw input is voor mij zeer waardevol.
Ik zou het dan ook zeer waarderen als u deze enquête invult.
Mocht dit bericht uw reactie kruisen, dan kunt u deze eenmalige herinnering verder negeren.

Bijlage 4 - Overzicht interview- en enquêtevragen

Interviewvragen

* Interview vragen zijn opgesteld n.a.v. analyse van vragenlijsten van eerdere onderzoeken en de gesprekken met praktijk 0. Antwoorden op vragen 1 t/m 6 (m.u.v. 3) zijn opgenomen in een aparte bijlage en zullen alléén voor de examencommissie (Open Universiteit) inzichtelijk worden gemaakt.

Algemene informatie:

1. Naam geïnterviewde persoon
2. Naam praktijk
3. Locatie praktijk
4. Soort praktijk: Solo-praktijk/ duo-praktijk/ HOES/ HOED/ anders
5. Aantal patiënten (ongeveer)?
6. Hoeveel medewerkers telt de praktijk?
7. Welke functies en werkzaamheden bestaan er in de praktijk?
8. Welke functie vervult u?
9. Tot welke vertrouwelijke informatie heeft u toegang tijdens het uitvoeren van uw functie?

Vooraf

1. Waar denkt u aan bij Informatiebeveiliging?
2. Houd u zichzelf bezig met Informatiebeveiliging binnen of buiten uw praktijk?
3. Worden er in de praktijk audits uitgevoerd op informatiebeveiliging?
4. Heeft de praktijk een accreditering (evt. waarbij Informatiebeveiliging getoetst wordt)?

Interviewvragen

5. Kunt u een beschrijving geven van uw werkzaamheden en activiteiten op een reguliere werkdag geven?
6. Zijn er buiten de reguliere werkzaamheden nu nog activiteiten die u niet genoemd heeft?
7. Met welke mensen hebt u op een reguliere werkdag te maken?
8. Welke systemen en applicaties zijn in de praktijk aanwezig?
    a. Beheert uzelf of een van de praktijkmedewerkers dit systeem zelf?
    b. Hoe worden deze onderhouden?
    c. Wordt er regelmatig onderhoud uitgevoerd (back-ups, updates)?
    d. Is er contact of een overeenkomst met een leverancier voor onderhoud?
    e. Is er een systeem/applicatiebeheerder voor deze applicatie?
    f. Is de toegang tot het systeem of applicatie beperkt tot specifieke medewerkers?
9. In uw contact met patiënten:
    a. Hoe zorgt u dat de contactmomenten privé blijven
    b. Hoe zorgt u dat relevante data goed opgeslagen wordt?
    c. Weet u hoe de systemen van opslag beschermd zijn tegen bedreigingen en fouten?
10. Staat Informatiebeveiliging op de agenda bij overleggen (zoals werkoverleggen en met collega's)?
11. Wordt Informatiebeveiliging buiten de vooraf geplande overleggen besproken?
    a. Zo ja, wat wordt er zoal besproken?

12. Is er een personeelsbeleid?
    a. Worden nieuwe en bestaande medewerkers gescreend?
    b. Is er voor de medewerkers een functie- en toegangsbeleid?
    c. Worden accounts uitgeschakeld of wachtwoorden gewijzigd bij medewerkers die uit dienst gaan?
13. Is er een handboek of schriftelijke uitleg van de procedures in de praktijk?
14. Wachtwoordbeleid:
    a. Worden moeilijke wachtwoorden afgedwongen?
    b. Vervallen wachtwoorden periodiek?
    c. Wachtwoorden vervangen bij uitdienst medewerkers?
    d. Heeft iedere gebruiker een eigen gebruikersnaam en wachtwoord?
    e. Bent u op de hoogte van wachtwoorden van andere medewerkers?
    f. Zijn andere medewerkers op de hoogte van wachtwoorden van u?
15. Bescherming systemen:
    a. Worden er updates uitgevoerd op systemen en applicaties? (vr. 8c)
        i. Hoe vaak wordt dit gedaan?
    b. Is er antivirus bescherming aanwezig op alle werkplekken?
    c. Is veilige e-mailcommunicatie mogelijk met artsen en patiënten?
    d. Wordt gebruik gemaakt van een veilige internetverbinding?
16. Hoe gaat u om met het verwijderen van vertrouwelijke data en datadragers?
17. Aanschaf nieuwe applicaties of systemen
    a. Is er beleid voor aanschaf van nieuwe systemen of applicaties?
18. Is er een aangewezen persoon verantwoordelijk voor Informatiebeveiliging?
19. Hoe wordt omgegaan met IB-incidenten
    a. Wegvallen gegevens (brand/virus/systeemcrash/etc)
    b. Inzage door onbevoegden (hack/nieuwsgierige patiënt/etc)

<u>Tijdsbesteding</u>

1. Hoeveel uren werkt u gemiddeld?
    a. Tijdsbesteding aan patiëntcontacten (spreekuur, visites, brieven, post invoeren)
    b. Tijdsbesteding aan niet-patiëntgebonden uren
        i. Denk aan financiële administratie, bestellingen, onderhoud praktijk apparatuur, personeelsbeleid en -overleg, nascholing/overleggen
2. Zijn er activiteiten die u door de werkdruk niet binnen de reguliere werkweek gedaan krijgt?
    a. Hoe lost u dit op?
3. Denkt u dat informatiebeveiliging u meer tijd zal kosten of u tijd zal opleveren? Waarom?
4. Vind u dat u voldoende tijd beschikbaar heeft om onderhoud op uw systemen en applicaties uit te voeren?
5. Vind u dat u voldoende tijd beschikbaar hebt om uzelf op de hoogte te houden op het gebied van informatiebeveiliging?

<u>Eigen inbreng</u>

1. Zijn er punten waar jullie weleens discussie over hebben als het gaat om informatiebeveiliging? Worden deze opgelost?
    a. Denk bijvoorbeeld aan vraagstukken rondom privacy/ patiëntgegevens
2. Vind u dat uw praktijk voldoende op de hoogte is van informatiebeveiliging?
3. Vind u dat uw praktijk voldoende beschermd?
4. Op welke vlakken ziet u zelf verbetermogelijkheden?
5. Wat zijn volgens u de mogelijke gevolgen als vertrouwelijke informatie op straat komt?

Enquêtevragen

* Enquête vragen zijn opgesteld n.a.v. de vragenlijst van de interviews, de afgenomen interviews en overleg met huisartsen voor begrijpelijke vraagstelling.

Vraag 1: Wat is de praktijkvorm van uw huisartsenpraktijk?
Vraag 2: Welke functie vervult u binnen de praktijk?
Vraag 3: Heeft de praktijk een NHG-Praktijkaccreditering?
Vraag 4: Wat is de vestigingsplaats van de huisartsenpraktijk?
Vraag 5: Hoeveel patiënten heeft de praktijk (ongeveer)?
Vraag 6: Hoeveel medewerkers heeft de praktijk?
Vraag 7: Hoeveel uren werkt u gemiddeld op een werkdag?
Vraag 8: Hoeveel uren hiervan zijn voor patiëntencontacten?
Vraag 9: Hoeveel uren hiervan zijn voor overige werkzaamheden voor de praktijk?
Vraag 10: Is er binnen de praktijk voldoende tijd beschikbaar voor:
Vraag 11: Heeft Informatiebeveiliging een vaste plek op de agenda bij overleggen?
Vraag 12: Is er een aangewezen medewerker verantwoordelijk voor informatiebeveiliging binnen de organisatie?
Vraag 13: Hoe wordt omgegaan met informatiebeveiligingsincidenten?
Vraag 14: Wordt informatiebeveiliging meegenomen in de beslissing voor aanschaf van nieuwe applicaties en medische apparatuur?
Vraag 15: Wie voorziet de HIS-applicatie van uw praktijk van (beveiligings)updates?
Vraag 16: Hoe vaak worden er updates op de HIS-applicatie geïnstalleerd?
Vraag 17: Hoe vaak wordt er een back-up gemaakt van de HIS-applicatie?
Vraag 18: Hoe vaak worden er updates op de werkplekken geïnstalleerd?
Vraag 19: Is er een overeenkomst met de leverancier van de HIS-applicatie voor onderhoud?
Vraag 20: Op hoeveel werkplekken is antivirus bescherming aanwezig in de praktijk?
Vraag 21: Wordt er gebruik gemaakt van veilige e-mailcommunicatie voor overleg van patiëntinformatie met collegae?
Vraag 22: Wordt bij telefonisch overleg de identiteit van de andere partij (bv. specialist) geverifieerd voordat patiëntinformatie gedeeld wordt?
Vraag 23: Wie mag er bij systemen of applicaties met patiëntgegevens?
Vraag 24: Hoe wordt uw computer vergrendeld als u de ruimte verlaat?
Vraag 25: Worden wachtwoorden gedeeld met andere medewerkers?
Vraag 26: Wanneer wordt de toegang tot systemen uitgeschakeld als een medewerker uit dienst gaat?
Vraag 27: Wanneer worden algemeen bekende wachtwoorden vervangen als een medewerker de organisatie verlaat?
Vraag 28: Welke controles worden gedaan bij het aanstellen van nieuwe medewerkers?
Vraag 29: Word patiëntinformatie op papier versnipperd of via een gecertificeerd bedrijf vernietigd?
Vraag 30: Hoe wordt met afgedankte USB-schijven en -sticks omgegaan?
Vraag 31: Welke maatregelen zijn genomen om binnen de praktijk gesprekken met patiënten privé te houden?
Vraag 32: Vindt u dat uw praktijk voldoende op de hoogte is van informatiebeveiliging?
Vraag 33: Is het toepassen van informatiebeveiliging (IB) binnen de praktijk de investering waard?
Vraag 34: Hoe belangrijk is informatiebeveiliging voor uw praktijk?
Vraag 35: Hoe groot zijn volgens u de gevolgen voor de praktijk als vertrouwelijke informatie op straat komt?
Vraag 36: Gaat u naar aanleiding van deze enquête aanpassingen maken in uw praktijk (op het gebied van informatiebeveiliging)?
Vraag 37: Aantal keren dat de respondent “weet niet” beantwoord op een vraag (automatisch berekend antwoord)

Bijlage 5 - Uitgewerkte interviews

Praktijk 0 - Huisarts NP (interviewtijd +- 6 uur)
Locatie praktijk: Rijswijk

Welke functie vervult u: Huisarts (inmiddels NP), Praktijkhouder
Welke functies en werkzaamheden vervullen de andere medewerkers in de praktijk?

- Artsen (3x):
    - Aansturing praktijk
    - HR
    - Apparatuur onderhouden
    - Financiële en contractuele zaken regelen
    - Facilitaire zaken regelen
    - Behandelen patienten
    - Overleggen met specialisten
- Assistenten (2x):
    - Ondersteuning artsen
    - Patiëntbezoeken inplannen
    - Patiëntinformatie verwerken
    - Patiëntvragen beantwoorden
    - Klaarzetten behandelapparatuur
    - Op orde houden behandelapparatuur en -werktuigen
- POH (praktijk ondersteunende huisarts) (GGZ inzet via Shop)
    - Behandeling psychische klachten van patiënten
- Longverpleegkundige (ZZP)
    - Begeleiding mensen met longklachten/ stoppen met roken
    - Begeleiding in optimalisatie van de longfunctie
- Diabetesverpleegkundige (lease via Florence)
    - Begeleiding diabetespatiënten door voorlichting en voorschrijven medicatie.

Kunt u een beschrijving geven van de werkzaamheden en activiteiten in de praktijk?

- De dag is voornamelijk ingevuld met patiëntcontacten. Daarnaast worden patiëntdossiers bijgewerkt op basis van lab-uitslagen en brieven. Ook controleer ik de inkoop en werk andere administratie bij.
- Met de assistenten heb ik overleg n.a.v. telefonische vragen of controlevragen (medische verantwoording) voor handelen. Daarnaast overleg ik met andere huisartsen/praktijk medewerkers. Met andere artsen voornamelijk betreffende waarneming e.d...
- Daarnaast houd ik in de gaten bij welke patiënten langsgegaan moet worden. Dit kan bij de meeste patiënten uit m'n uit hoofd, maar ook er is ook een lijst "kwetsbare ouderen" beschikbaar als onderdeel van de HIS-applicatie.

Welke systemen en applicaties zijn in de praktijk aanwezig?

- Binnen de praktijk zijn een server, een aantal werkplekken en wat andere medische apparatuur aanwezig. De server wordt gebruikt voor de HIS-applicatie en als opslag voor alle bestanden. De werkplekken worden gebruikt voor toegang tot de HIS-applicatie, overige lokale applicaties zoals Word/Excel en voor toegang tot medische (uitwissel)websites en normaal internet gebruik.

Hoe worden deze systemen en applicaties onderhouden?

- De server en werkplekken onderhoud ik zelf. De server staat zo ingesteld dat hij automatisch updates installeert, de werkplekken loop ik eens per maand langs om na te gaan of er nog updates van Windows en het antiviruspakket klaarstaan.
- Overige medische apparatuur wordt onderhouden door de assistenten. Voor technische zaken is soms een onderhoudscontract met de leverancier, maar meestal wordt het gebruikt tot dat het apparaat stuk is en dan wordt een nieuwe besteld.

Zijn er overeenkomsten met de leverancier van deze systemen en applicaties?

- Ja, er is een overeenkomst met de leverancier van de HIS-applicatie voor uitgifte van updates van het programma en de G-standaard. Er is geen overeenkomst voor systemen, dit wordt ad hoc geregeld als dat nodig is.

Hoe worden risico's weggenomen m.b.t. deze systemen en applicaties?

- Door regelmatig de systemen langs te lopen probeer ik te zorgen dat deze helemaal up-to-date en veilig zijn. Daarnaast is er een eZorg internetverbinding met verplichte proxyinstellingen die een hoge mate van filtering heeft waardoor virussen minder kans hebben binnen te komen.

Bij het contact met patiënten, hoe zorgt U dat dit privé blijft?

- De werkkamer zelf is afgesloten tijdens de gesprekken, daarnaast worden er geen gesprekken op de gang of in de wachtkamer gevoerd. Ook is de deur dicht als er telefonisch wordt overlegd.

Hoe zorgt U dat relevante informatie goed opgeslagen wordt?

- We maken gebruik van ICPC-codes voor het noteren van patiëntklachten en diagnoses. Omdat dit standaardcodes zijn, zijn ze voor iedereen leesbaar. Eigen aantekeningen worden daarnaast ook zo veel mogelijk opgeslagen om het beeld/verhaal van de patiënt zo goed mogelijk te tonen.

Zijn de systemen van opslag beschermd tegen bedreigingen en fouten?

- Er wordt dagelijks een back-up gemaakt van de complete HIS-applicatie. Mocht er iets fout gaan kan die ook worden teruggezet. Het herproduceren van gegevens van diezelfde werkdag kost wat tijd, maar is wel mogelijk a.h.v. agenda, notities en eigen geheugen.

Is er een personeelsbeleid?

- Nee, dit is niet aanwezig. Wel hebben we een vaste werkwijze. We hebben met eventuele sollicitanten een gesprek en kijken of alle diploma's en bijscholing op orde is.

Screening bestaande en nieuwe medewerkers?

- Dit gebeurt niet, iedereen heeft de eed afgelegd en daarnaast bekijk je alleen het functioneren.

Functie- en toegangsbeleid?

- Is niet aanwezig, toegang wordt ad hoc ingeregeld op basis van de functie die hij/zij gaat vervullen. Dit wordt door mij ingesteld in de applicaties.

Is er een handboek of schriftelijke uitleg van procedures?

- Er is een korte werkinstructie voor nieuwe/tijdelijke assistenten om te kunnen inloggen in de HIS-applicatie, verder wordt alles mondeling uitgelegd waar nodig.

Uitvraag over toepassing van maatregelen uit de NEN7510 bij Praktijk 0
* Hierbij is de maatregel en uitleg aan de praktijkhouder voorgelezen en gevraagd “Is dit bij jullie geregeld? Ligt toe hoe dit is geregeld of waarom niet.

H5 - Beveiligingsbeleid

Maatregel	5.1.1.: Beleidsdocument voor informatiebeveiliging
Uitleg uit normdocument	De directie behoort een beleidsdocument voor informatiebeveiliging goed te keuren, te publiceren en kenbaar te maken aan alle werknemers en relevante externe partijen.
Opmerkingen Praktijkhouder van praktijk 0	De term directie is voor huisartsenpraktijken niet duidelijk. Er wordt hier eigenlijk altijd de term praktijkhouder aangehouden. Binnen de praktijk is er voornamelijk mondeling beleid, zoals; - Gebruik websites zo veel mogelijk beperken tot noodzakelijk voor de uitvoering van het werk - Voorzichtig omgaan met mailverkeer (niet zomaar bijlagen openen) Als praktijkhouder ben ik hier initiatiefnemer. Het is vooral de geïnteresseerde assistente/praktijkmanager die hier primaire taak heeft voor veilig omgaan met de systemen en dit te bespreken met collega’s.

Maatregel	5.1.2.: Beoordeling van het informatiebeveiligingsbeleid
Uitleg uit normdocument	Het informatiebeveiligingsbeleid behoort met geplande tussenpozen, na het optreden van een omvangrijk informatiebeveiligingsincident of zodra zich belangrijke wijzigingen voordoen, te worden beoordeeld om te bewerkstelligen dat het geschikt, toereikend en doeltreffend blijft.
Opmerkingen Praktijkhouder van praktijk 0	Bij praktijken wordt er voornamelijk reactief geacteerd bij het bekijken van risico’s voor de patiënt en systemen in de praktijk. Dit wordt geïnitieerd door incidenten of grote verandering in databehandeling (denk aan verandering van applicatie, provider of grotere updates).

H6 - Organisatie van informatiebeveiliging

Maatregel	6.1.1.: Betrokkenheid van de directie bij informatiebeveiliging
Uitleg uit normdocument	De directie behoort informatiebeveiliging binnen de organisatie actief te ondersteunen door duidelijk richting te geven, betrokkenheid te tonen en expliciet verantwoordelijkheden voor informatiebeveiliging toe te kennen en te erkennen.
Opmerkingen Praktijkhouder van praktijk 0	Dit is binnen onze praktijk niet van toepassing. We hebben geen expliciete verantwoordelijkheid toegekend al blijft de huisarts/praktijkhouder natuurlijk verantwoordelijk voor wat er gebeurt. Betrokkenheid is er wel, al is dat meer vanuit eigen interesse dan er over veiligheid wordt nagedacht.

Maatregel	6.1.2.: Coördinatie van informatiebeveiliging
Uitleg uit normdocument	Vertegenwoordigers uit verschillende delen van de organisatie met relevante rollen en functies behoren activiteiten voor informatiebeveiliging te coördineren.
Opmerkingen Praktijkhouder van praktijk 0	Er zijn binnen de praktijk geen verantwoordelijke benoemd of rollen verdeeld. Natuurlijk voel ik mijzelf wel verantwoordelijk voor het op orde hebben van systemen waarin patiëntgegevens staan.

Maatregel	6.1.3.: Toewijzing van verantwoordelijkheden voor informatiebeveiliging
Uitleg uit normdocument	(a) Alle verantwoordelijkheden voor informatiebeveiliging behoren duidelijk te zijn gedefinieerd. (b) Organisaties die patiëntgegevens verwerken, behoren de verantwoordelijkheden voor de beveiliging van patiëntgegevens eenduidig toe te wijzen.
Opmerkingen Praktijkhouder van praktijk 0	Hetzelfde antwoord als bij 6.1.1 en 6.1.2 is van toepassing.

Maatregel	6.1.4.: Goedkeuringsproces voor middelen voor de informatievoorziening
Uitleg uit normdocument	Er behoort een goedkeuringsproces voor nieuwe middelen voor de informatievoorziening te worden vastgesteld en geïmplementeerd.
Opmerkingen Praktijkhouder van praktijk 0	Er zijn binnen de praktijk duidelijk afspraken over de inkoop gemaakt. Dit is vooral voor de borging van de controle op financiële middelen.

Maatregel	6.1.5.: Geheimhoudingsovereenkomst
Uitleg uit normdocument	Eisen voor vertrouwelijkheid die een weerslag vormen van de behoefte van de organisatie aan beveiliging van informatie behoren in een geheimhoudingsovereenkomst te worden vastgesteld. Deze eisen en deze overeenkomst behoren regelmatig te worden beoordeeld.
Opmerkingen Praktijkhouder van praktijk 0	In de praktijk gaan we uit van het feit dat alle medewerkers de eed hebben afgelegd en goed opgeleid zijn. Een geschreven geheimhoudingsovereenkomst is niet aanwezig.

Maatregel	6.1.6.: Contact met overheidsinstanties
Uitleg uit normdocument	Er behoren geschikte contacten met relevante overheidsinstanties te worden onderhouden.
Opmerkingen Praktijkhouder van praktijk 0	Er is zo af en toe contact met het IGZ. Dit is echter altijd vanuit hun geïnitieerd.

Maatregel	6.1.7.: Contact met speciale belangengroepen
Uitleg uit normdocument	Er behoren geschikte contacten met speciale belangengroepen of andere specialistische platforms voor beveiliging en professionele organisaties te worden onderhouden.
Opmerkingen Praktijkhouder van praktijk 0	Er is contact met de LHV en diverse andere huisartsenverenigingen. Dit is vooral nodig voor informatieverschaffing en hulp bij lastigere juridische vraagpunten.

Maatregel	6.1.8.: Onafhankelijke beoordeling van informatiebeveiliging
Uitleg uit normdocument	De benadering van de organisatie voor het beheer van informatiebeveiliging en de implementatie daarvan (dat wil zeggen beheer doelstellingen, beheersmaatregelen, beleid, processen en procedures voor informatiebeveiliging) behoren onafhankelijk en met geplande tussenpozen te worden beoordeeld of zodra zich significante wijzigingen voordoen in de implementatie van de beveiliging.

Opmerkingen Praktijkhouder van praktijk 0	Eens in de tijd loop ik alle systemen langs of ze nog netjes updaten en bijgewerkt zijn met anti-virus updates. Verder worden serversystemen eens in de paar jaar vervangen, waarbij ook het besturingssysteem vernieuwd wordt. Verder zijn er geen structurele onderdelen van beheer aanwezig.

Maatregel	6.2.1.: Identificatie van risico's die betrekking hebben op externe partijen
Uitleg uit normdocument	De risico's voor de informatie en informatievoorziening van de organisatie vanuit bedrijfsprocessen waarin externe partijen betrokken zijn, behoren te worden geïdentificeerd en er behoren geschikte beheersmaatregelen te worden geïmplementeerd voordat toegang wordt verleend
Opmerkingen Praktijkhouder van praktijk 0	De systemen zelf zijn alleen op locatie beschikbaar, verder zijn er voor brand e.d. verzekeringen afgesloten en back-ups offsite beschikbaar. Er is verder met de schoonmaak van het gebouw een contract. Met politie en brandweer is eens in de tijd overleg en er zijn controles van de (openbare) ruimte, vluchtwegen en brandinstallaties.

Maatregel	6.2.2.: Beveiliging in de omgang met klanten
Uitleg uit normdocument	Alle geïdentificeerde beveiligingseisen behoren te worden geadresseerd voordat klanten toegang wordt verleend tot de informatie of bedrijfsmiddelen van de organisatie.
Opmerkingen Praktijkhouder van praktijk 0	Toegang wordt alleen in persoon gegeven tot een kopie van het dossier of mondelinge toelichting. Origineel wordt alleen door de arts of assistent behandeld en per aangetekende post of digitale uitwisseling overgedragen aan nieuwe behandelend arts.

Maatregel	6.2.3.: Beveiliging in overeenkomsten met een derde partij
Uitleg uit normdocument	In overeenkomsten met derden waarbij sprake is van toegang tot, het verwerken van, communicatie van of beheer van informatie of informatievoorziening van de organisatie, of toevoeging van producten of diensten aan informatievoorziening waarbij sprake is van toegang, behoren alle relevante beveiligingseisen te zijn opgenomen.
Opmerkingen Praktijkhouder van praktijk 0	Er is met de andere gebouwgebruikers en onderhoudspartijen daarvan een overeenkomst. Verder zijn er duidelijke protocollen als het gaat om informatie-uitwisseling met spoeddiensten en collega artsen.

H7 - Beheer van bedrijfsmiddelen

Maatregel	7.1.1.: Inventarisatie van bedrijfsmiddelen
Uitleg uit normdocument	Alle bedrijfsmiddelen behoren duidelijk te zijn geïdentificeerd en er behoort een inventaris van alle belangrijke bedrijfsmiddelen te worden opgesteld en bijgehouden.
Opmerkingen Praktijkhouder van praktijk 0	Medische apparatuur wordt netjes onderhouden en eens in de tijd vervangen. Computers worden vervangen indien ze verouderd zijn (reageren niet meer goed of besturingssysteem moet vernieuwd worden). Hier is geen centrale lijst van.

Maatregel	7.1.2.: Verantwoordelijken voor de bedrijfsmiddelen
Uitleg uit normdocument	Alle informatie en bedrijfsmiddelen die verband houden met de informatievoorziening behoren een 'verantwoordelijke' te hebben in de organisatie.

Opmerkingen Praktijkhouder van praktijk 0	Ik voel me als praktijkhouder verantwoordelijk om alles netjes bij te houden en te zorgen dat mijn medewerkers niet achter een dermate trage computer zitten dat ze er last van hebben.

Maatregel	7.1.3.: Aanvaardbaar gebruik van bedrijfsmiddelen
Uitleg uit normdocument	Er behoren regels te worden vastgesteld, gedocumenteerd en geïmplementeerd voor aanvaardbaar gebruik van informatie en bedrijfsmiddelen die verband houden met informatievoorziening.
Opmerkingen Praktijkhouder van praktijk 0	Ik bespreek met de medewerkers van de praktijk zo af en toe de nieuwe functies of gewijzigde procedures van applicaties. Daarnaast bespreken we regelmatig de procedures voor correcte verwerking van binnenkomende patiëntinformatie. Verder vraag ik ook collega's in het gebouw om te letten op hun systeembeveiliging.

Maatregel	7.2.1.: Richtlijnen voor classificatie
Uitleg uit normdocument	Informatie behoort te worden geclassificeerd met betrekking tot de waarde, wettelijke eisen, gevoeligheid en onmisbaarheid voor de organisatie.
Opmerkingen Praktijkhouder van praktijk 0	Voor invoering van patiëntinformatie wordt de ICPC-codering gebruikt. Daarnaast wordt gevoelige informatie van een extra vlaggetje in de applicatie voorzien.

Maatregel	7.2.2.: Labeling en verwerking van informatie
Uitleg uit normdocument	(a) Er behoren geschikte, samenhangende procedures te worden ontwikkeld en geïmplementeerd voor de labeling en verwerking van informatie overeenkomstig het classificatiesysteem dat de organisatie heeft geïmplementeerd. (b) Alle informatiesystemen die patiëntgegevens verwerken, behoren de gebruikers, bijvoorbeeld via een inlogboodschap, te wijzen op de vertrouwelijkheid van de gegevens die via het systeem toegankelijk zijn. Documenten met patiëntgegevens behoren van het kenmerk 'vertrouwelijk' te zijn voorzien.
Opmerkingen Praktijkhouder van praktijk 0	Er zijn protocollen voor verwerking van patiëntinformatie. Neem bijvoorbeeld voor de ICPC-codering. Er zijn verder geen boodschappen of andere meldingen dat iets vertrouwelijk is. Alle informatie binnen de praktijk is van deze aard.

H8 – Personeel

Maatregel	8.1.1.: Rollen en verantwoordelijkheden
Uitleg uit normdocument	De rollen en verantwoordelijkheden van werknemers, ingehuurd personeel en externe gebruikers ten aanzien van beveiliging behoren te worden vastgesteld en gedocumenteerd overeenkomstig het beleid voor informatiebeveiliging van de organisatie.
Opmerkingen Praktijkhouder van praktijk 0	Alle rollen van de medewerkers liggen vast. Hier is geen documentatie van, echter wordt dit ook regelmatig besproken.

Maatregel	8.1.2.: Screening
Uitleg uit normdocument	Verificatie van de achtergrond van alle kandidaten voor een dienstverband, ingehuurd personeel en externe gebruikers, behoort te worden uitgevoerd overeenkomstig relevante wetten, voorschriften en ethische overwegingen, en

	behoort te worden afgestemd op de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend, en de waargenomen risico's.
Opmerkingen Praktijkhouder van praktijk 0	De andere artsen en assistenten zijn al meerdere jaren in dienst. Deze hebben allen hun eed afgelegd. Er is bij de gewisselde assistenten wel gekeken of de opleiding is afgerond. Verder is er geen screening.

Maatregel	8.1.3.: Arbeidsvoorwaarden
Uitleg uit normdocument	(a) Als onderdeel van hun contractuele verplichting behoren werknemers, ingehuurd personeel en externe gebruikers de algemene voorwaarden te aanvaarden en ondertekenen van hun arbeidscontract. In dit contract behoren hun verantwoordelijkheden en die van de organisatie ten aanzien van informatiebeveiliging te zijn vastgelegd. (b) Een organisatie die patiëntgegevens verwerkt, behoort in de aanstellingsvoorwaarden van medewerkers, vrijwilligers of contractanten die patiëntgegevens verwerken of gaan verwerken, een verklaring op te nemen over de geheimhouding en zorgvuldigheid die daarbij is vereist vanuit het informatiebeveiligingsbeleid van de organisatie.
Opmerkingen Praktijkhouder van praktijk 0	Er zijn geen aparte voorwaarden voor geheimhouding. Alle medewerkers hebben de eed afgelegd en behoren zich netjes te gedragen.

Maatregel	8.2.1.: Directieverantwoordelijkheid
Uitleg uit normdocument	De directie behoort van werknemers, ingehuurd personeel en externe gebruikers te eisen dat ze beveiliging toepassen overeenkomstig vastgesteld beleid en vastgestelde procedures van de organisatie.
Opmerkingen Praktijkhouder van praktijk 0	Dit wordt regelmatig besproken, dat ze netjes werken met de systemen waarop ze acties verrichten.

Maatregel	8.2.2.: Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging
Uitleg uit normdocument	(a) Alle werknemers van de organisatie en, voor zover van toepassing, ingehuurd personeel en externe gebruikers, behoren geschikte training en regelmatige bijscholing te krijgen met betrekking tot beleid en procedures van de organisatie, voor zover relevant voor hun functie. (b) Een organisatie die patiëntgegevens verwerkt, behoort ervoor te zorgen dat opleiding en training inzake informatiebeveiliging zijn geregeld voor alle medewerkers bij aanvang van het dienstverband en dat in regelmatige opfrissing van de kennis is voorzien.
Opmerkingen Praktijkhouder van praktijk 0	Ik houd mijzelf via diverse e-mail berichten en bladen op de hoogte. De interessante stukken deel ik met collega's en in de praktijk hebben we tijdens overleg soms punten die het werk beïnvloeden of waar op gelet moet worden.

Maatregel	8.2.3.: Disciplinaire maatregelen
Uitleg uit normdocument	Er behoort een formeel disciplinair proces te zijn vastgesteld voor werknemers die inbreuk op de beveiliging hebben gepleegd.
Opmerkingen Praktijkhouder van praktijk 0	Is niet aanwezig.

Maatregel	8.3.1.: Beëindiging van verantwoordelijkheden

Uitleg uit normdocument	De verantwoordelijkheden bij beëindiging of wijziging van het dienstverband behoren duidelijk te zijn vastgesteld en toegewezen.
Opmerkingen Praktijkhouder van praktijk 0	Is niet vastgelegd. De medewerkers hebben hun eed afgelegd, die blijft ook na einde dienstverband gelden.

Maatregel	8.3.2.: Retournering van bedrijfsmiddelen
Uitleg uit normdocument	Alle werknemers, ingehuurd personeel en externe gebruikers behoren alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben te retourneren bij beëindiging van hun dienstverband, contract of overeenkomst.
Opmerkingen Praktijkhouder van praktijk 0	Er zijn geen bedrijfsmiddelen die worden meegenomen buiten de praktijk anders dan de sleutel. Deze wordt ingeleverd bij einde dienstverband.

Maatregel	8.3.3.: Intrekken van toegangsrechten
Uitleg uit normdocument	De toegangsrechten van alle werknemers, ingehuurd personeel en externe gebruikers tot informatie en IT-voorzieningen behoren te worden ingetrokken bij beëindiging van het dienstverband, het contract of de overeenkomst of behoort na wijziging te worden aangepast.
Opmerkingen Praktijkhouder van praktijk 0	Zie ook antwoord 8.3.2. Toegang tot systemen is alleen lokaal.

H9 - Fysieke beveiliging en beveiliging van de omgeving

Maatregel	9.1.1.: Fysieke beveiliging van de omgeving
Uitleg uit normdocument	Er behoren toegangsbeveiligingen (barrières zoals muren, toegangspoorten met kaartsloten of een bemande receptie) te worden aangebracht om ruimten te beschermen waar zich informatie en IT-voorzieningen bevinden. Dit geldt in het bijzonder voor ruimten waar patiëntgegevens worden bewaard en waar informatiesystemen met patiëntgegevens zijn opgesteld
Opmerkingen Praktijkhouder van praktijk 0	Alle ruimtes van de praktijk zijn afsluitbaar en standaard gesloten (vallen ook in het slot). Ze kunnen enkel met “druppel” opengemaakt worden. Ook de gangen tussen de praktijken zijn voorzien van afsluitbare en standaard gesloten deuren richting de algemene ruimte. De wachtruimte is algemene ruimte en vrij toegankelijk na binnenkomst van het gebouw en wordt gebruikt door alle praktijken. Het gebouw wordt ’s avonds afgesloten. IT-servervoorzieningen zitten in een apart (en afgesloten) kamer.

Maatregel	9.1.2.: Fysieke toegangsbeveiliging
Uitleg uit normdocument	Beveiligde zones behoren te worden beschermd door geschikte toegangsbeveiliging, om te bewerkstelligen dat alleen bevoegd personeel wordt toegelaten.
Opmerkingen Praktijkhouder van praktijk 0	Zie ook 9.1.1

Maatregel	9.1.3.: Beveiliging van kantoren, ruimten en faciliteiten
Uitleg uit normdocument	Er behoort fysieke beveiliging van kantoren, ruimten en faciliteiten te worden ontworpen en toegepast.

Opmerkingen Praktijkhouder van praktijk 0	Zie ook 9.1.1

Maatregel	9.1.4.: Bescherming tegen bedreigingen van buitenaf
Uitleg uit normdocument	Er behoort fysieke bescherming tegen schade door brand, overstroming, aardschokken, explosies, oproer en andere vormen van natuurlijke of menselijke calamiteiten te worden ontworpen en toegepast
Opmerkingen Praktijkhouder van praktijk 0	Er is een brandinstallatie in het gebouw aanwezig. Verder is het terrein redelijk onbeveiligd. Hier zijn grotendeels verzekeringen voor afgesloten waar het geen natuurrampen betreft.

Maatregel	9.1.5.: Werken in beveiligde ruimten
Uitleg uit normdocument	Er behoren een fysieke bescherming en richtlijnen voor werken in beveiligde ruimten te worden ontworpen en toegepast.
Opmerkingen Praktijkhouder van praktijk 0	Alle ruimten zijn van elkaar gescheiden en afgesloten. Zo kan elk gesprek worden gevoerd zonder dat anderen dit kunnen opvangen. Aan alle medewerkers is de instructie gegeven deuren zo veel mogelijk dicht te laten om deze reden.

Maatregel	9.1.6.: Openbare toegang en gebieden voor laden en lossen
Uitleg uit normdocument	Toegangspunten zoals gebieden voor laden en lossen en andere punten waar onbevoegden het terrein kunnen betreden, behoren te worden beheerst en indien mogelijk worden afgeschermd van IT-voorzieningen, om onbevoegde toegang te voorkomen.
Opmerkingen Praktijkhouder van praktijk 0	Alleen de wachtruimte is openbaar gebied. Hier zijn geen stroom- of netwerkpunten aanwezig.

Maatregel	9.2.1.: Plaatsing en bescherming van apparatuur
Uitleg uit normdocument	Apparatuur behoort zo te worden geplaatst en beschermd dat risico's van schade en storing van buitenaf en de gelegenheid voor onbevoegde toegang worden verminderd tot een vooraf door de organisatie bepaald niveau.
Opmerkingen Praktijkhouder van praktijk 0	Apparatuur is alleen geplaatst in ruimten waar medewerkers bij kunnen door middel van een sleutel.

Maatregel	9.2.2.: Nutsvoorzieningen
Uitleg uit normdocument	Er behoren maatregelen te worden getroffen om de gevolgen van stroomuitval en onderbrekingen van andere nutsvoorzieningen te beperken.
Opmerkingen Praktijkhouder van praktijk 0	Er is een UPS bij de server geplaatst. Verder is geen maatregel tegen stroomuitval genomen. De praktijk kan ook zonder HIS systeem wel korte tijd blijven functioneren.

Maatregel	9.2.3.: Beveiliging van kabels
Uitleg uit normdocument	Voedings- en telecommunicatiekabels die voor dataverkeer of ondersteunende informatiediensten worden gebruikt, behoren tegen interceptie of beschadiging te worden beschermd.
Opmerkingen Praktijkhouder van praktijk 0	Netwerkkabels zijn in de wanden weggewerkt en er zijn geen over de grond lopende kabels aanwezig. Waar ze wel vrij liggen kunnen geen medewerkers

	lopen. Hetzelfde geldt voor stroomkabels. In openbare ruimten zijn deze kabels geheel afwezig.

Maatregel	9.2.4.: Onderhoud van apparatuur
Uitleg uit normdocument	Apparatuur behoort op correcte wijze te worden onderhouden, om te waarborgen dat de apparatuur in goede staat verkeert en de geleverde informatiediensten beschikbaar blijven.
Opmerkingen Praktijkhouder van praktijk 0	Updates worden regelmatig geïnstalleerd. Tevens wordt periodiek verouderde apparatuur en software vervangen.

Maatregel	9.2.5.: Beveiliging van apparatuur buiten het terrein
Uitleg uit normdocument	(a) Apparatuur buiten de terreinen behoort te worden beveiligd waarbij rekening wordt gehouden met de diverse risico's van werken buiten het terrein van de organisatie. (b) Een organisatie die patiëntgegevens verwerkt, behoort te zorgen voor toestemming voor elk gebruik buiten de instelling van medische apparaten die gegevens registreren en/of doorgeven, met inbegrip van apparatuur die, al of niet permanent, in gebruik is bij ambulante medewerkers en mogelijk tot hun vaste uitrusting behoort.
Opmerkingen Praktijkhouder van praktijk 0	Er is geen apparatuur buiten de praktijkkamers aanwezig.

Maatregel	9.2.6.: Veilig verwijderen of hergebruiken van apparatuur
Uitleg uit normdocument	Wanneer apparatuur wordt verwijderd die opslagmedia bevat, behoort de organisatie te bewerkstelligen dat alle gevoelige gegevens en in licentie gebruikte programmatuur worden vernietigd of op veilige wijze worden overschreven.
Opmerkingen Praktijkhouder van praktijk 0	Opslagmedia van apparatuur wordt eens in de zoveel tijd vernietigd zodat data op deze media nooit meer hersteld kunnen worden.

Maatregel	9.2.7.: Verwijdering van bedrijfseigendommen
Uitleg uit normdocument	Apparatuur, informatie en programmatuur van de organisatie mogen niet zonder toestemming vooraf van de locatie worden meegenomen.
Opmerkingen Praktijkhouder van praktijk 0	Alle informatie behoort op de praktijk te blijven, medische apparatuur voor huisbezoeken vrijgesteld.

H10 - Beheer van communicatie- en bedieningsprocessen

Maatregel	10.1.1.: Gedocumenteerde bedieningsprocedures
Uitleg uit normdocument	Bedieningsprocedures behoren te worden gedocumenteerd, worden bijgehouden en beschikbaar worden gesteld aan alle gebruikers die deze nodig hebben.
Opmerkingen Praktijkhouder van praktijk 0	Er zijn korte handleidingen aanwezig voor invalkrachten of nieuwe medewerkers.

Maatregel	10.1.2.: Wijzigingsbeheer
Uitleg uit normdocument	Wijzigingen in de informatievoorziening en informatiesystemen behoren te worden beheerst met een formeel en gestructureerd proces dat niet onbedoeld afbreuk doet aan de informatievoorziening en de continuïteit van zorg
Opmerkingen Praktijkhouder van praktijk 0	Er is geen formeel proces voor wijzigingen in apparatuur of software.

Maatregel	10.1.3.: Functiescheiding
Uitleg uit normdocument	Taken en verantwoordelijkheidsgebieden behoren te worden gescheiden om gelegenheid voor onbevoegde of onbedoelde wijziging of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.
Opmerkingen Praktijkhouder van praktijk 0	Er is een duidelijke scheiding tussen arts, praktijkhouder en assistenten. Het gaat hier om toegang binnen de HIS-applicatie en toegang tot de financiële systemen.

Maatregel	10.1.4.: Scheiding van faciliteiten voor ontwikkeling, testen en productie
Uitleg uit normdocument	De organisatie behoort omgevingen voor ontwikkeling, testen en voor instructiedoeleinden, gescheiden te houden van de productieomgeving (fysiek of virtueel) om het risico van onbevoegde toegang tot of wijzigingen in het productiesysteem te verminderen.
Opmerkingen Praktijkhouder van praktijk 0	Er wordt voor grotere testen gebruik gemaakt van een restore van een back-up (aparte instantie van productie) voordat de productie wordt geüpdatet.

Maatregel	10.2.1.: Dienstverlening
Uitleg uit normdocument	Er behoort te worden bewerkstelligd dat de beveiligingsmaatregelen, definities van dienstverlening en niveaus van dienstverlening zoals vastgelegd in de overeenkomst voor dienstverlening, door een derde partij worden geïmplementeerd en uitgevoerd en actueel worden gehouden door die derde partij.
Opmerkingen Praktijkhouder van praktijk 0	Er is geen derde partij die beheer doet op de systemen.

Maatregel	10.2.2.: Controle en beoordeling van dienstverlening door een derde partij
Uitleg uit normdocument	De diensten, rapporten en registraties die door de derde partij worden geleverd, behoren regelmatig te worden gecontroleerd en beoordeeld.
Opmerkingen Praktijkhouder van praktijk 0	Niet van toepassing, zie 10.2.1

Maatregel	10.2.3.: Beheer van wijzigingen in dienstverlening door een derde partij
Uitleg uit normdocument	Wijzigingen in de dienstverlening door derden, waaronder het bijhouden en verbeteren van bestaande beleidslijnen, procedures en maatregelen voor informatiebeveiliging, behoren te worden beheerd, waarbij rekening wordt gehouden met de onmisbaarheid van de betrokken bedrijfssystemen en -processen en met heroverweging van risico's.
Opmerkingen	Niet van toepassing, zie 10.2.1

Praktijkhouder van praktijk 0	

Maatregel	10.3.1.: Capaciteitsbeheer
Uitleg uit normdocument	Het gebruik van middelen behoort te worden gecontroleerd en afgestemd en er behoren verwachtingen te worden opgesteld voor toekomstige capaciteitseisen met het oog op de vereiste systeemprestaties.
Opmerkingen Praktijkhouder van praktijk 0	Hier wordt geen beleid op gevoerd. Ik vervang systemen indien ik dit nodig vind.

Maatregel	10.3.2.: Systeemacceptatie
Uitleg uit normdocument	De organisatie behoort acceptatiecriteria vast te stellen voor nieuwe informatiesystemen, upgrades en nieuwe versies en behoort geschikte testen uit te voeren voorafgaand aan de acceptatie.
Opmerkingen Praktijkhouder van praktijk 0	Dit wordt per gebeurtenis gedaan om te kunnen vaststellen wat aangekocht dient te worden indien van toepassing.

Maatregel	10.4.1.: Maatregelen tegen kwaadaardige programmatuur
Uitleg uit normdocument	Er behoren maatregelen te worden getroffen voor detectie, preventie en herstel om te beschermen tegen virussen en andere kwaadaardige programmatuur en er behoren geschikte maatregelen te worden getroffen om het risicobewustzijn van de gebruikers te vergroten.
Opmerkingen Praktijkhouder van praktijk 0	Er is op alle systemen antivirussoftware aanwezig. Verder wordt er gebruik gemaakt van een veilige internetverbinding (proxy eZorg).

Maatregel	10.4.2.: Maatregelen tegen “mobile code”
Uitleg uit normdocument	Als gebruik van ‘mobile code’ is toegelaten, behoort de configuratie te bewerkstelligen dat de geautoriseerde ‘mobile code’ functioneert volgens een duidelijk vastgesteld beveiligingsbeleid, en behoort te worden voorkomen dat onbevoegde ‘mobile code’ wordt uitgevoerd.
Opmerkingen Praktijkhouder van praktijk 0	Hier zijn geen maatregelen tegen genomen.

Maatregel	10.5.1.: Reservekopieën (back-ups)
Uitleg uit normdocument	(a) Er behoren stelselmatig back-upkopieën van informatie en programmatuur te worden gemaakt en de herstelprocedure behoort regelmatig te worden getest, overeenkomstig het vastgestelde back-upbeleid. (b) Een organisatie die patiëntgegevens verwerkt, behoort van alle patiëntgegevens back-upkopieën te maken en in een veilige omgeving op te slaan om de beschikbaarheid te waarborgen.
Opmerkingen Praktijkhouder van praktijk 0	Er wordt dagelijks een back-up gemaakt. De juiste inhoud wordt ook dagelijks automatisch gecontroleerd.

Maatregel	10.6.1.: Maatregelen voor netwerken
Uitleg uit normdocument	Netwerken behoren adequaat te worden beheerd en beheerst om ze te beschermen tegen bedreigingen en om beveiliging te handhaven voor de

	systemen en toepassingen die gebruikmaken van het netwerk, waaronder informatie die wordt getransporteerd.
Opmerkingen Praktijkhouder van praktijk 0	Er is een veilige internetverbinding (eZorg) aanwezig die monitort op virussen e.d. Er zijn geen aparte beveiligingen gemaakt voor het netwerk binnen de praktijk.

Maatregel	10.6.2.: Beveiliging van netwerkdiensten
Uitleg uit normdocument	Beveiligingskenmerken, niveaus van dienstverlening en beheer eisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in elke overeenkomst voor netwerkdiensten, zowel voor diensten die intern worden geleverd als voor uitbestede diensten.
Opmerkingen Praktijkhouder van praktijk 0	Dit is niet uitgevoerd.

Maatregel	10.7.1.: Beheer van verwijderbare media
Uitleg uit normdocument	Er behoren procedures te zijn vastgesteld voor het beheer van verwijderbare media.
Opmerkingen Praktijkhouder van praktijk 0	Verwijderbare media wordt vernietigd zodra het niet langer door de praktijk wordt gebruikt.

Maatregel	10.7.2.: Verwijdering van media
Uitleg uit normdocument	Alle gegevens op verwijderbare media behoren op veilige wijze te worden overschreven of de media behoren te worden vernietigd wanneer deze niet meer nodig zijn, overeenkomstig formele procedures.
Opmerkingen Praktijkhouder van praktijk 0	Zie ook 10.7.1

Maatregel	10.7.3.: Procedures voor de behandeling van informatie
Uitleg uit normdocument	(a) Er behoren procedures te worden vastgesteld voor de behandeling en opslag van informatie om deze te beschermen tegen onbevoegde openbaarmaking of misbruik. (b) Media met patiëntgegevens behoren fysiek te worden beveiligd. Op de staat en locatie van media met patiëntgegevens behoort controle te worden uitgeoefend.
Opmerkingen Praktijkhouder van praktijk 0	Hier is geen procedure voor. Alle informatie dient binnen de praktijk te blijven.

Maatregel	10.7.4.: Beveiliging van systeemdocumentatie
Uitleg uit normdocument	Systeemdocumentatie behoort te worden beschermd tegen onbevoegde toegang
Opmerkingen Praktijkhouder van praktijk 0	Er is geen specifieke systeemdocumentatie anders dan algemene installatiehandleidingen van leveranciers.

Maatregel	10.8.1.: Beleid en procedures voor informatie-uitwisseling

Uitleg uit normdocument	Er behoren formeel beleid, formele procedures en formele beheersmaatregelen te zijn vastgesteld om de uitwisseling van informatie via het gebruik van alle typen communicatiefaciliteiten te beschermen.
Opmerkingen Praktijkhouder van praktijk 0	De koepelorganen voor artsen geven hiervoor procedures af. Deze volgt de praktijk.

Maatregel	10.8.2.: Uitwisselingsovereenkomst
Uitleg uit normdocument	Er behoren overeenkomsten te worden vastgesteld voor de uitwisseling van informatie en programmatuur tussen de organisatie en externe partijen.
Opmerkingen Praktijkhouder van praktijk 0	Deze overeenkomst is niet aanwezig en onbekend.

Maatregel	10.8.3.: Fysiek transport van media
Uitleg uit normdocument	Media die informatie bevatten, behoren te worden beschermd tegen onbevoegde toegang, misbruik of corrumperen tijdens transport buiten de fysieke begrenzing van de organisatie.
Opmerkingen Praktijkhouder van praktijk 0	Dit is niet van toepassing.

Maatregel	10.8.4.: Elektronische berichtenuitwisseling
Uitleg uit normdocument	Informatie die een rol speelt bij elektronische berichtuitwisseling behoort op geschikte wijze te worden beschermd.
Opmerkingen Praktijkhouder van praktijk 0	Dit wordt gedaan via een veilige uitwisselroute binnen het HIS-pakket. Bestanden worden via een beveiligde verbinding naar de ontvangende arts of specialist verstuurd.

Maatregel	10.8.5.: Systemen voor bedrijfsinformatie
Uitleg uit normdocument	Beleid en procedures behoren te worden ontwikkeld en geïmplementeerd om informatie te beschermen die een rol speelt bij de onderlinge koppeling van systemen voor bedrijfsinformatie
Opmerkingen Praktijkhouder van praktijk 0	Hier is geen beleid voor opgesteld.

Maatregel	10.9.1.: E-commerce
Uitleg uit normdocument	Informatie die een rol speelt bij e-commerce en die via openbare netwerken wordt uitgewisseld behoort te worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en modificatie
Opmerkingen Praktijkhouder van praktijk 0	Dit is niet van toepassing.

Maatregel	10.9.2.: Onlinetransacties
Uitleg uit normdocument	Informatie die een rol speelt bij onlinetransacties, behoort te worden beschermd om herhaling van transacties, onvolledige overdracht, onjuiste routing, onbevoegde wijziging van berichten, onbevoegde openbaarmaking, onbevoegde duplicatie of weergave van berichten te voorkomen

Opmerkingen Praktijkhouder van praktijk 0	Dit is niet van toepassing.

Maatregel	10.9.3.: Openbaar beschikbare informatie
Uitleg uit normdocument	(a) De betrouwbaarheid van de informatie die beschikbaar wordt gesteld op een openbaar toegankelijk systeem, behoort te worden beschermd om onbevoegde modificatie te voorkomen. (b) Openbaar beschikbare zorginformatie (te onderscheiden van patiëntgegevens) behoort systematisch te worden gearchiveerd. (c) Van openbaar beschikbare zorginformatie behoort de bron of auteur te zijn vermeld.
Opmerkingen Praktijkhouder van praktijk 0	Dit is niet van toepassing.

Maatregel	10.10.1.: Aanmaken audit-logbestanden
Uitleg uit normdocument	Er behoren auditlogbestanden te worden aangemaakt waarin activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen worden vastgelegd. Deze logbestanden behoren gedurende een overeengekomen periode te worden bewaard, ten behoeve van toekomstig onderzoek en toegangscontrole.
Opmerkingen Praktijkhouder van praktijk 0	Er worden voor inlogpogingen logbestanden op werkplek en server bijgehouden. Deze worden echter niet actief beheerd en vervallen zodra het logboek vol raakt (oud eerst)

Maatregel	10.10.2.: Controle van systeemgebruik
Uitleg uit normdocument	Er behoren procedures te worden vastgesteld om het gebruik van IT-voorzieningen te controleren. Het resultaat van de controleactiviteiten behoort regelmatig te worden beoordeeld.
Opmerkingen Praktijkhouder van praktijk 0	Er is geen actieve controle op systeemgebruik.

Maatregel	10.10.3.: Bescherming van informatie in logbestanden
Uitleg uit normdocument	(a) Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen inbreuk en onbevoegde toegang. (b) De logging van informatiesystemen voor het verwerken van patiëntgegevens behoort te zijn beveiligd en niet te manipuleren.
Opmerkingen Praktijkhouder van praktijk 0	Er is geen actief beheer op de logbestanden.

Maatregel	10.10.4.: Logbestanden van administrators en operators
Uitleg uit normdocument	Activiteiten van systeemadministrators en systeemoperators behoren in logbestanden te worden vastgelegd.
Opmerkingen Praktijkhouder van praktijk 0	Er zijn geen aparte logbestanden voor systeemadministrators.

Maatregel	10.10.5.: Registratie van storingen

Uitleg uit normdocument	Storingen behoren in logbestanden te worden vastgelegd en te worden geanalyseerd en er behoren geschikte maatregelen te worden genomen.
Opmerkingen Praktijkhouder van praktijk 0	Er is geen actief beheer op storingen.

Maatregel	10.10.6.: Synchronisatie van systeemklokken
Uitleg uit normdocument	(a) De klokken van alle relevante informatiesystemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met een overeengekomen nauwkeurige tijdsbron. (b) Zorginformatiesystemen die tijdkritische zorgactiviteiten ondersteunen, behoren te voorzien in synchronisatie om mogelijke tijdverschillen tussen verschillende registraties van activiteiten te signaleren en daarvoor te corrigeren.
Opmerkingen Praktijkhouder van praktijk 0	Alle systeemklokken synchroniseren met een externe tijdbron.

H11 - Toegangsbeveiliging

Maatregel	11.1.1.: Toegangsbeleid
Uitleg uit normdocument	(a) Er behoort toegangsbeleid te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfseisen en beveiligingseisen voor toegang. (b) Een organisatie die patiëntgegevens verwerkt, behoort een toegangsbeleid ten aanzien van deze gegevens te hanteren. Het toegangsbeleid behoort te voldoen aan professionele, ethische, wettelijke en patiëntgerelateerde eisen en tevens tegemoet te komen aan de eisen die het werk van zorgprofessionals stelt en speciale aandacht te besteden aan de beschikbaarheid van gegevens bij het verlenen van acute zorg.
Opmerkingen Praktijkhouder van praktijk 0	Er is met de vaste medewerkers en schoonmaak afgesproken hoe om te gaan met sleutels. Verder is er geen beleid op omdat dit al jaren niet nodig is geweest.

Maatregel	11.2.1.: Registratie voor gebruikers
Uitleg uit normdocument	(a) Er behoren formele procedures voor het registreren en afmelden van gebruikers te zijn vastgesteld, voor het verlenen en intrekken van toegangsrechten tot alle informatiesystemen en -diensten. (b) Een organisatie die patiëntgegevens verwerkt, behoort te waarborgen dat toegang tot systemen die patiëntgegevens verwerken deel uitmaakt van een formele gebruikersregistratieprocedure. Deze procedure behoort te waarborgen dat de mate van vereiste authenticatie bij een gebruiker in overeenstemming is met het resulterende niveau van toegang.
Opmerkingen Praktijkhouder van praktijk 0	Dit wordt niet centraal geregistreerd.

Maatregel	11.2.2.: Beheer van speciale bevoegdheden
Uitleg uit normdocument	De toewijzing en het gebruik van speciale bevoegdheden behoren te worden beperkt en beheerst
Opmerkingen	Er wordt geen actief beheer op speciale bevoegdheden gedaan.

Praktijkhouder van praktijk 0	

Maatregel	11.2.3.: Beheer van gebruikerswachtwoorden
Uitleg uit normdocument	De toewijzing van wachtwoorden behoort met een formeel beheerproces te worden beheerst.
Opmerkingen Praktijkhouder van praktijk 0	Er is geen formeel beheerproces. Gebruikers krijgen bij in dienst (wat al een hele tijd dezelfde medewerkers zijn) een eigen wachtwoord toegewezen.

Maatregel	11.2.4.: Beoordeling van toegangsrechten van gebruikers
Uitleg uit normdocument	De organisatie behoort de toegangsrechten van gebruikers, met inbegrip van de gebruikersregistraties en details daarbinnen, regelmatig te beoordelen in een formeel proces om zich te vergewissen dat ze compleet en nauwkeurig zijn en dat toegang nog steeds is gewenst.
Opmerkingen Praktijkhouder van praktijk 0	Dit wordt bij indienst en applicatiemigraties gedaan. Verder is er geen beheer op.

Maatregel	11.3.1.: Gebruik van wachtwoorden
Uitleg uit normdocument	Gebruikers behoren goede beveiligingsgewoontes in acht te nemen bij het kiezen en gebruiken van wachtwoorden.
Opmerkingen Praktijkhouder van praktijk 0	Gebruikers krijgen ieder een eigen wachtwoord die ze niet behoren te delen met anderen.

Maatregel	11.3.2.: Onbeheerde gebruikersapparatuur
Uitleg uit normdocument	Gebruikers behoren te bewerkstelligen dat onbeheerde apparatuur passend is beschermd.
Opmerkingen Praktijkhouder van praktijk 0	Er zijn geen onbeheerde gebruikersapparaten aanwezig.

Maatregel	11.3.3.: ‘Clear desk’- en ‘clear screen’-beleid
Uitleg uit normdocument	Er behoort een ‘clear desk’-beleid en een ‘clear screen’-beleid voor IT-voorzieningen te worden ingesteld
Opmerkingen Praktijkhouder van praktijk 0	Er wordt gevraagd het bureau opgeruimd te houden. Aangezien alle ruimten worden afgesloten wordt er niet gevraagd ze leeg te houden. Hetzelfde geldt voor het beeldscherm. Dat wordt afgesloten na vertrek.

Maatregel	11.4.1.: Beleid ten aanzien van het gebruik van netwerkdiensten
Uitleg uit normdocument	Gebruikers behoort alleen toegang te worden verleend tot diensten waarvoor ze specifiek bevoegd zijn.
Opmerkingen Praktijkhouder van praktijk 0	Gebruikers hebben alleen via de vaste werkplekken toegang tot het netwerk. Hier is verder geen beheer of andere toegang tot.

Maatregel	11.4.2.: Authenticatie van gebruikers bij externe verbindingen
Uitleg uit normdocument	Er behoren geschikte authenticatiemethoden te worden gebruikt om toegang van gebruikers op afstand te beheersen.

Opmerkingen Praktijkhouder van praktijk 0	Niet van toepassing in de praktijk.

Maatregel	11.4.3.: Identificatie van netwerkapparatuur
Uitleg uit normdocument	Automatische identificatie van apparatuur behoort te worden overwogen als methode om verbindingen vanaf specifieke locaties en apparatuur te authenticeren
Opmerkingen Praktijkhouder van praktijk 0	Dit wordt niet toegepast in de praktijk.

Maatregel	11.4.4.: Bescherming op afstand van poorten voor diagnose en configuratie
Uitleg uit normdocument	De fysieke en logische toegang tot poorten voor diagnose en configuratie behoort te worden beheerst.
Opmerkingen Praktijkhouder van praktijk 0	Dit wordt niet toegepast in de praktijk.

Maatregel	11.4.5.: Scheiding van netwerken
Uitleg uit normdocument	Groepen informatiediensten, gebruikers en informatiesystemen behoren op netwerken te worden gescheiden.
Opmerkingen Praktijkhouder van praktijk 0	Diensten van mede-gebouwgebruikers worden zo goed mogelijk gescheiden. Verder is er geen interne scheiding in de praktijk van netwerkdiensten.

Maatregel	11.4.6.: Beheersmaatregelen voor netwerkverbindingen
Uitleg uit normdocument	Voor gemeenschappelijke netwerken, vooral waar deze de grenzen van de organisatie overschrijden, behoren de toegangsmogelijkheden voor gebruikers te worden beperkt overeenkomstig het toegangsbeleid en de eisen van bedrijfstoepassingen (zie paragraaf 11.1).
Opmerkingen Praktijkhouder van praktijk 0	Dit is niet van toepassing in de praktijk.

Maatregel	11.4.7.: Beheersmaatregelen voor netwerkroutering
Uitleg uit normdocument	Netwerken behoren te zijn voorzien van beheersmaatregelen voor netwerkroutering om te bewerkstelligen dat computerverbindingen en informatiestromen niet in strijd zijn met het toegangsbeleid voor de bedrijfstoepassingen.
Opmerkingen Praktijkhouder van praktijk 0	Er is een beveiligde internetverbinding, verder is er geen routering.

Maatregel	11.5.1.: Beveiligde inlogprocedures
Uitleg uit normdocument	Toegang tot besturingssystemen behoort te worden beheerst met een beveiligde inlogprocedure
Opmerkingen Praktijkhouder van praktijk 0	Alle werkplekken vereisen een eigen wachtwoord. De HIS-applicatie vereist een wachtwoord per medewerker.

Maatregel	11.5.2.: Gebruikersidentificatie en -authenticatie
Uitleg uit normdocument	(a) Elke gebruiker behoort over een unieke identificatiecode te beschikken (gebruikers-ID) voor persoonlijk gebruik en er behoort een geschikte authenticatietechniek te worden gekozen om de geclaimde identiteit van de gebruiker te bewijzen. (b) Informatiesystemen die patiëntgegevens verwerken, behoren authenticatie toe te passen op basis van ten minste twee afzonderlijke kenmerken.
Opmerkingen Praktijkhouder van praktijk 0	De HIS-applicatie heeft een unieke inlog voor elke gebruiker. Er is geen tweede kenmerk (zoals UZI-pas) wat wordt gebruikt omdat de applicatie dit niet goed ondersteunt.

Maatregel	11.5.3.: Systemen voor wachtwoordbeheer
Uitleg uit normdocument	Systemen voor wachtwoordbeheer behoren interactief te zijn en te bewerkstelligen dat wachtwoorden van geschikte kwaliteit worden gekozen.
Opmerkingen Praktijkhouder van praktijk 0	Dit is niet het geval.

Maatregel	11.5.4.: Gebruik van systeemhulpmiddelen
Uitleg uit normdocument	Het gebruik van hulpprogrammatuur waarmee systeem- en toepassingsbeheersmaatregelen zouden kunnen worden gepasseerd, behoort te worden beperkt en strikt te worden beheerst.
Opmerkingen Praktijkhouder van praktijk 0	Werkplekken zijn standaard ingericht, er zijn geen hulpmiddelen die deze beperkte functionaliteit kunnen omzeilen.

Maatregel	11.5.5.: Time-out van sessies
Uitleg uit normdocument	Interactieve sessies behoren na een vastgestelde periode van inactiviteit automatisch ontoegankelijk te worden gemaakt.
Opmerkingen Praktijkhouder van praktijk 0	Schermen worden na een vaste tijd automatisch vergrendeld.

Maatregel	11.5.6.: Beperking van verbindingstijd
Uitleg uit normdocument	De verbindingstijd behoort te worden beperkt als aanvullende beveiliging voor toepassingen met een verhoogd risico.
Opmerkingen Praktijkhouder van praktijk 0	Hier is geen beperking op.

Maatregel	11.6.1.: Beheersen van toegang tot informatie
Uitleg uit normdocument	Toegang tot informatie en functies van toepassingssystemen door gebruikers en ondersteunend personeel behoort te worden beheerst overeenkomstig het vastgestelde toegangsbeleid.
Opmerkingen Praktijkhouder van praktijk 0	Er is geen beleid op toegang.

Maatregel	11.6.2.: Isoleren van gevoelige systemen

Uitleg uit normdocument	Systemen met een bijzonder hoge gevoeligheid waar het gaat om vertrouwelijkheid en/of om beschikbaarheid en/of om integriteit behoren een eigen, vast toegewezen (geïsoleerde) computeromgeving te hebben.
Opmerkingen Praktijkhouder van praktijk 0	Alle gevoelige gegevens zijn centraal opgeslagen in de HIS-applicaties die op een aparte server staat. Er zijn voorzieningen voor stroomuitval genomen en uitval van schijven of andere serveronderdelen.

Maatregel	11.7.1.: Draagbare computers en communicatievoorzieningen
Uitleg uit normdocument	Er behoort formeel beleid te zijn vastgesteld en er behoren geschikte beveiligingsmaatregelen te zijn getroffen ter bescherming tegen risico's van het gebruik van draagbare computers en communicatiefaciliteiten.
Opmerkingen Praktijkhouder van praktijk 0	Er is geen formeel beleid voor. Wel worden alle computers eens in de zoveel tijd gecontroleerd op aanwezigheid van laatste virusdefinities en updates.

Maatregel	11.7.2.: Telewerken
Uitleg uit normdocument	Er behoren beleid, operationele plannen en procedures voor telewerken te worden ontwikkeld en geïmplementeerd.
Opmerkingen Praktijkhouder van praktijk 0	Dit is niet van toepassing.

H12 - Verwerving, ontwikkeling en onderhoud van informatiesystemen

Maatregel	12.1.1.: Analyse en specificatie van beveiligingseisen
Uitleg uit normdocument	In bedrijfseisen voor nieuwe informatiesystemen of uitbreidingen van bestaande informatiesystemen behoren ook eisen voor beveiligingsmaatregelen te worden opgenomen.
Opmerkingen Praktijkhouder van praktijk 0	Dit wordt per geval beoordeeld om nieuwe beveiligingstechnieken altijd in deze nieuwe onderdelen op te nemen.

Maatregel	12.2.1.: Validatie van invoergegevens
Uitleg uit normdocument	(a) Gegevens die worden ingevoerd in toepassingen, behoren te worden gevalideerd om te bewerkstelligen dat deze gegevens juist en geschikt zijn. (b) Informatiesystemen die patiëntgegevens verwerken, moeten alle patiëntgegevens gecontroleerd van de juiste patiëntidentificatie voorzien.
Opmerkingen Praktijkhouder van praktijk 0	Er wordt in de HIS-applicatie met ICPC-codering gewerkt. Verder valideert het programma zelf of alle velden zijn voorzien van informatie die valt binnen de grenzen van de vereiste invoer.

Maatregel	12.2.2.: Beheersing van interne gegevensverwerking
Uitleg uit normdocument	Er behoren validatiecontroles te worden opgenomen in toepassingen om eventueel corrumperen van informatie door verwerkingsfouten of opzettelijke handelingen te ontdekken
Opmerkingen Praktijkhouder van praktijk 0	Bij updates van de applicatie wordt een controle over de inhoud uitgevoerd.

Maatregel	12.2.3.: Integriteit van berichten
Uitleg uit normdocument	Er behoren eisen te worden vastgesteld en geschikte beheersmaatregelen te worden vastgesteld en geïmplementeerd voor het bewerkstelligen van authenticiteit en het beschermen van integriteit van berichten in toepassingen.
Opmerkingen Praktijkhouder van praktijk 0	Deze zijn vanuit de applicatie vastgesteld, daar heeft de praktijk zelf geen eis voor.

Maatregel	12.2.4.: Validatie van uitvoergegevens
Uitleg uit normdocument	(a) Gegevensuitvoer uit een toepassing behoort te worden gevalideerd, om te bewerkstelligen dat de verwerking van opgeslagen gegevens op de juiste manier plaatsvindt en geschikt is gezien de omstandigheden. (b) Informatiesystemen behoren bij het presenteren van patiëntgegevens altijd voldoende identificerende gegevens te tonen om het de zorgverlener mogelijk te maken vast te stellen dat de patiëntgegevens de patiënt in kwestie betreffen.
Opmerkingen Praktijkhouder van praktijk 0	De HIS-applicatie vereiste een aantal gegevens om patiënt identificatie mogelijk te maken. Denk aan ID-nummer of foto.

Maatregel	12.3.1.: Beleid voor het gebruik van cryptografische beheersmaatregelen
Uitleg uit normdocument	Er behoort beleid te worden ontwikkeld en geïmplementeerd voor het gebruik van cryptografische beheersmaatregelen voor de bescherming van informatie.
Opmerkingen Praktijkhouder van praktijk 0	Er is geen beleid voor.

Maatregel	12.3.2.: Sleutelbeheer
Uitleg uit normdocument	Er behoort sleutelbeheer te zijn vastgesteld ter ondersteuning van het gebruik van cryptografische technieken binnen de organisatie.
Opmerkingen Praktijkhouder van praktijk 0	Er is geen beleid voor.

Maatregel	12.4.1.: Beheersing van operationele programmatuur
Uitleg uit normdocument	Er behoren procedures te zijn vastgesteld om de installatie van programmatuur op productiesystemen te beheersen.
Opmerkingen Praktijkhouder van praktijk 0	Installatiehandleidingen van leveranciers worden altijd gevolgd.

Maatregel	12.4.2.: Bescherming van testdata
Uitleg uit normdocument	(a) Testgegevens behoren zorgvuldig te worden gekozen, beschermd en beheerst. (b) Er behoren geen tot personen herleidbare patiëntgegevens te worden gebruikt als testgegevens.
Opmerkingen Praktijkhouder van praktijk 0	Er is geen testomgeving.

Maatregel	12.4.3.: Toegangsbeheersing voor broncode van programmatuur

Uitleg uit normdocument	De toegang tot broncode van programmatuur behoort te worden beperkt.
Opmerkingen Praktijkhouder van praktijk 0	Er is geen toegang tot broncode.

Maatregel	12.5.1.: Procedures voor wijzigingsbeheer
Uitleg uit normdocument	De implementatie van wijzigingen behoort te worden beheerst door middel van formele procedures voor wijzigingsbeheer.
Opmerkingen Praktijkhouder van praktijk 0	Er is geen formeel proces voor wijzigingen.

Maatregel	12.5.2.: Technische beoordeling van toepassingen na wijzigingen in het besturingssysteem
Uitleg uit normdocument	Bij wijzigingen in besturingssystemen behoren bedrijfskritische toepassingen te worden beoordeeld en getest om te bewerkstelligen dat er geen nadelige gevolgen zijn voor de activiteiten of beveiliging van de organisatie.
Opmerkingen Praktijkhouder van praktijk 0	Na updates en andere wijzigingen voer ik altijd een controle van de werking van het HIS-pakket uit omdat ik op dat moment nog terug kan draaien. Na een werkdag gaat dit lastiger.

Maatregel	12.5.3.: Restricties op wijzigingen in programmatuurpakketten
Uitleg uit normdocument	Wijzigingen in programmatuurpakketten behoren te worden ontmoedigd, te worden beperkt tot noodzakelijke wijzigingen, en alle wijzigingen behoren strikt te worden beheerst.
Opmerkingen Praktijkhouder van praktijk 0	Dit is niet van toepassing op de praktijk.

Maatregel	12.5.4.: Informatielekken
Uitleg uit normdocument	Er behoort te worden voorkomen dat informatielekken ontstaan.
Opmerkingen Praktijkhouder van praktijk 0	Dit wordt gedaan door het onderwerp bespreekbaar te maken tijdens praktijk overleggen.

Maatregel	12.5.5.: Uitbestede ontwikkeling van programmatuur
Uitleg uit normdocument	Bij uitbestede ontwikkeling van programmatuur behoort de organisatie maatregelen te treffen ter waarborging van de kwaliteit van de ontwikkelde programmatuur.
Opmerkingen Praktijkhouder van praktijk 0	Dit is niet van toepassing. Programmatuur wordt as-is aangekocht.

Maatregel	12.6.1.: Beheersing van technische kwetsbaarheden
Uitleg uit normdocument	Er behoort tijdig informatie te worden verkregen over technische kwetsbaarheden van de gebruikte informatiesystemen. De mate waarin de organisatie blootstaat aan dergelijke kwetsbaarheden, behoort te worden geëvalueerd en er behoren geschikte maatregelen te worden genomen voor behandeling van daarmee samenhangende risico's.

Opmerkingen Praktijkhouder van praktijk 0	Dit wordt niet actief gedaan in de praktijk.

H13 - Beheer van informatiebeveiligingsincidenten

Maatregel	13.1.1.: Rapportage van informatiebeveiligingsgebeurtenissen
Uitleg uit normdocument	Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.
Opmerkingen Praktijkhouder van praktijk 0	Hier worden geen items van vastgelegd. Wel worden gebeurtenissen besproken met de medewerkers zodat iedereen er zijn voordeel mee kan doen.

Maatregel	13.1.2.: Rapportage van zwakke plekken in de beveiliging
Uitleg uit normdocument	Van alle werknemers, ingehuurd personeel en externe gebruikers van informatiesystemen en -diensten behoort te worden geëist dat zij alle waargenomen of verdachte zwakke plekken in systemen of diensten registreren en rapporteren.
Opmerkingen Praktijkhouder van praktijk 0	Alle medewerkers wordt eens in de tijd gevraagd om oplettend te blijven naar afwijkingen in systemen en applicatie en deze te melden bij mij.

Maatregel	13.2.1.: Verantwoordelijkheden en procedures
Uitleg uit normdocument	Er behoren verantwoordelijkheden en procedures te worden vastgesteld om een snelle, doeltreffende en ordelijke reactie op informatiebeveiligingsincidenten te bewerkstelligen.
Opmerkingen Praktijkhouder van praktijk 0	Dit is niet het geval, we reageren per geval.

Maatregel	13.2.2.: Leren van informatiebeveiligingsincidenten
Uitleg uit normdocument	Er behoren mechanismen te zijn ingesteld waarmee de aard, omvang en kosten van informatiebeveiligingsincidenten kunnen worden gekwantificeerd en gevolgd.
Opmerkingen Praktijkhouder van praktijk 0	Aangezien de gebeurtenissen besproken worden trachten we er zo ook van te leren.

Maatregel	13.2.3.: Verzamelen van bewijsmateriaal
Uitleg uit normdocument	Waar een vervolgprocedure tegen een persoon of organisatie na een informatiebeveiligingsincident juridische maatregelen omvat (civiel of strafrechtelijk), behoort bewijsmateriaal te worden verzameld, bewaard en gepresenteerd overeenkomstig de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd.
Opmerkingen Praktijkhouder van praktijk 0	Dit is nog nooit van toepassing geweest. Dit zal per geval behandeld worden als dat wel het geval wordt.

H14 - Bedrijfscontinuïteitsbeheer

Maatregel	14.1.1.: Informatiebeveiliging opnemen in het proces van bedrijfscontinuïteitsbeheer
Uitleg uit normdocument	Er behoort een beheerd proces voor bedrijfscontinuïteit in de gehele organisatie te worden ontwikkeld en bijgehouden waarbinnen de eisen voor informatiebeveiliging worden meegenomen die nodig zijn voor de continuïteit van de bedrijfsvoering.
Opmerkingen Praktijkhouder van praktijk 0	Er is geen proces van bedrijfscontinuïteitsbeheer.

Maatregel	14.1.2.: Bedrijfscontinuïteit en risicobeoordeling
Uitleg uit normdocument	(a) Gebeurtenissen die tot onderbreking van bedrijfsprocessen kunnen leiden, behoren te worden geïdentificeerd, tezamen met de waarschijnlijkheid en de gevolgen van dergelijke onderbrekingen en hun gevolgen voor informatiebeveiliging. (b) Organisaties die patiëntgegevens verwerken, behoren een continuïteitsstrategie vast te stellen, te documenteren, in te voeren en te onderhouden. Hierin behoort voor ieder bedrijfsproces een maximaal toegelaten uitvalduur (MUD) en een maximaal toelaatbaar verlies aan gegevens (MGV) te worden vastgesteld.
Opmerkingen Praktijkhouder van praktijk 0	Er is gekeken naar kwetsbaarheden in pandbeveiliging en netwerkbeveiliging. Dit wordt eens in de tijd besproken met de andere pand-gebruikers.

Maatregel	14.1.3.: Continuïteitsplannen en informatievoorziening
Uitleg uit normdocument	Er behoren plannen te worden ontwikkeld en geïmplementeerd om de bedrijfsactiviteiten te handhaven of te herstellen en om de beschikbaarheid van informatie op het vereiste niveau en in de vereiste tijdspanne te bewerkstelligen na onderbreking of uitval van kritische bedrijfsprocessen
Opmerkingen Praktijkhouder van praktijk 0	Er is geen plan, in het geval van uitval zal op dat moment bekeken worden wat nodig is voor doorgang van de werkzaamheden.

Maatregel	14.1.4.: Kader voor de bedrijfscontinuïteitsplanning
Uitleg uit normdocument	Er behoort een enkelvoudig kader voor bedrijfscontinuïteitsplannen te worden gehandhaafd om te bewerkstelligen dat alle plannen consistent zijn, om eisen voor informatiebeveiliging op consistente wijze te behandelen en om prioriteiten vast te stellen voor testen en onderhoud.
Opmerkingen Praktijkhouder van praktijk 0	Dit is niet het geval.

Maatregel	14.1.5.: Testen, onderhouden en herbeoordelen van bedrijfscontinuïteitsplannen
Uitleg uit normdocument	Bedrijfscontinuïteitsplannen behoren regelmatig te worden getest en geactualiseerd, om te bewerkstelligen dat ze actueel en doeltreffend blijven.
Opmerkingen Praktijkhouder van praktijk 0	Dit is niet het geval.

H15 - Naleving

Maatregel	15.1.1.: Identificatie van toepasselijke wetgeving
Uitleg uit normdocument	Alle relevante wettelijke en regelgevende eisen en contractuele verplichtingen en de benadering van de organisatie in de naleving van deze eisen, behoren expliciet te worden vastgesteld, gedocumenteerd en actueel te worden gehouden voor elk informatiesysteem en voor de organisatie.
Opmerkingen Praktijkhouder van praktijk 0	Dit wordt niet gedaan in de praktijk.

Maatregel	15.1.2.: Intellectuele eigendomsrechten
Uitleg uit normdocument	Er behoren geschikte procedures te worden geïmplementeerd om te bewerkstelligen dat wordt voldaan aan de wettelijke en regelgevende eisen en contractuele verplichtingen voor het gebruik van materiaal waarop intellectuele eigendomsrechten kunnen berusten en het gebruik van programmatuur waarop intellectuele eigendomsrechten berusten.
Opmerkingen Praktijkhouder van praktijk 0	Dit is niet van toepassing in de praktijk.

Maatregel	15.1.3.: Bescherming van bedrijfsdocumenten
Uitleg uit normdocument	(a) Belangrijke registraties behoren te worden beschermd tegen verlies, vernietiging en vervalsing, overeenkomstig wettelijke en regelgevende eisen, contractuele verplichtingen en bedrijfsmatige eisen. (b) Organisaties die patiëntgegevens verwerken, behoren ervoor te zorgen dat tot een persoon herleidbare gegevens niet langer worden bewaard dan noodzakelijk en dat het risico van onbedoelde openbaarmaking van persoonsgegevens waar mogelijk wordt beperkt door vernietigen van de gegevens, dan wel door anonimiseren of pseudonimiseren. Zie ISO/TS 25237
Opmerkingen Praktijkhouder van praktijk 0	Dit wordt gedaan middels beveiliging van de HIS-applicatie en serveromgeving tegen toegang en uitval. Tevens worden papieren documenten beveiligd door gesloten deuren en continu toezicht/aanwezig personeel.

Maatregel	15.1.4.: Bescherming van gegevens en geheimhouding van persoonsgegevens
Uitleg uit normdocument	(a) De bescherming van gegevens en privacy behoort te worden bewerkstelligd overeenkomstig relevante wetgeving, voorschriften en indien van toepassing contractuele bepalingen. (b) Behoudens wettelijke uitzonderingen, behoort een zorginstelling toestemming te hebben van de patiënt voor het uitwisselen van zijn gegevens.
Opmerkingen Praktijkhouder van praktijk 0	Ik, samen met de medewerkers hebben allen de eed afgelegd. Wij proberen allen zo goed mogelijk patiëntinformatie te beschermen.

Maatregel	15.1.5.: Voorkomen van misbruik van IT-voorzieningen
Uitleg uit normdocument	Gebruikers behoren ervan te worden weerhouden IT-voorzieningen te gebruiken voor onbevoegde doeleinden.
Opmerkingen Praktijkhouder van praktijk 0	Gebruikers worden gevraagd niet te veel te internetten. Verder zijn er geen restricties.

Maatregel	15.1.6.: Voorschriften voor het gebruik van cryptografische beheersmaatregelen
Uitleg uit normdocument	Cryptografische beheersmaatregelen behoren overeenkomstig alle relevante overeenkomsten, wetten en voorschriften te worden gebruikt.
Opmerkingen Praktijkhouder van praktijk 0	Er zijn hiervoor geen voorschriften.

Maatregel	15.2.1.: Naleving van beveiligingsbeleid en -normen
Uitleg uit normdocument	Managers behoren te bewerkstelligen dat alle beveiligingsprocedures die binnen hun verantwoordelijkheid vallen, correct worden uitgevoerd om naleving te bereiken van beveiligingsbeleid en -normen.
Opmerkingen Praktijkhouder van praktijk 0	Veilig werken wordt in de praktijkoverleggen besproken. Verder is er geen controle of handhaving nodig geweest.

Maatregel	15.2.2.: Controle op technische naleving
Uitleg uit normdocument	Informatiesystemen behoren regelmatig te worden gecontroleerd op naleving van implementatie van technische beveiligingsnormen.
Opmerkingen Praktijkhouder van praktijk 0	Updates en antivirus definities worden eens in de tijd gecontroleerd.

Maatregel	15.3.1.: Beheersmaatregelen voor audits van informatiesystemen
Uitleg uit normdocument	Eisen voor audits en andere activiteiten waarbij controles worden uitgevoerd op productiesystemen, behoren zorgvuldig te worden gepland en goedgekeurd om het risico van verstoring van bedrijfsprocessen tot een minimum te beperken.
Opmerkingen Praktijkhouder van praktijk 0	Hier wordt per geval naar gekeken hoe dit de werkzaamheden zo min mogelijk verstoort.

Maatregel	15.3.2.: Bescherming van audithulpmiddelen voor audits van informatiesystemen
Uitleg uit normdocument	Toegang tot hulpmiddelen voor audits van informatiesystemen behoort te worden beschermd om mogelijk misbruik of compromittering te voorkomen.
Opmerkingen Praktijkhouder van praktijk 0	Er zijn bij de praktijk geen hulpmiddelen voor aanwezig, deze moeten door een externe auditor worden aangeleverd en worden niet binnen de praktijk bewaard.

Praktijk 1 – Geïnterviewde: Huisarts (interviewtijd +- 1,5 uur)
Locatie praktijk: Rijswijk

Welke functie vervult u: Huisarts, Praktijkhouder
Welke functies en werkzaamheden vervullen de andere medewerkers in de praktijk?

- Artsen/praktijkhouder (1x):
    - Aansturing praktijk
    - HR
    - Facilitaire zaken regelen
    - Declaraties versturen naar externe verwerker
    - Behandelen patiënten
    - Overleggen met specialisten
    - Overleggen met andere arts en assistenten
- Arts (1x)
    - Behandelen patiënten
    - Overleggen met specialisten
    - Overleggen met andere arts en assistenten
- Assistenten (2x):
    - Ondersteuning artsen
    - Patiëntbezoeken inplannen
    - Patiëntinformatie verwerken
    - Patiëntvragen beantwoorden
    - Klaarzetten behandelapparatuur
    - Op orde houden behandelapparatuur en -werktuigen
    - Overleggen met artsen
- POH (praktijk ondersteunende huisarts)
    - Behandeling psychische klachten van patiënten
- Longverpleegkundige
    - Begeleiding mensen met longklachten/ stoppen met roken
    - Begeleiding in optimalisatie van de longfunctie
- Diabetesverpleegkundige
    - Begeleiding diabetespatiënten door voorlichting en voorschrijven medicatie.

Tot welke vertrouwelijke informatie heeft u toegang tijdens het uitvoeren van uw functie?
Belangrijkste is natuurlijk patiëntinformatie. Daarnaast heb ik ook toegang tot personeelsgegevens van de praktijkmedewerkers.

Waar denkt u aan bij Informatiebeveiliging?
Bij informatiebeveiliging denk ik aan de computer en alle updates die daarvoor nodig zijn om alles veilig te houden.

Houd u zichzelf bezig met Informatiebeveiliging binnen of buiten uw praktijk?
Weinig, een andere praktijkhouder in het gebouw houdt zich hier erg mee bezig en ik luister zo af en toe geïnteresseerd mee.

Worden er in de praktijk audits uitgevoerd op informatiebeveiliging?
Nee, in ieder geval niet waarvan ik weet.

Heeft de praktijk een accreditering waarbij Informatiebeveiliging getoetst wordt?
Nee. Er is geen praktijkaccreditering aanwezig.

Kunt u een beschrijving geven van uw werkzaamheden en activiteiten op een reguliere werkdag?

- Post-, lab uitslagen en andere actiepunten verwerken
- Spreekuur starten en houden
- Declaraties en verrichtingen bijhouden
- Terugbellen patiënten
- Visites verrichten vooral in de middag.
- Verwijsbrieven maken
- Communicatie met zorginstanties voor starten externe zorg

Zijn er buiten de reguliere werkzaamheden nu nog activiteiten die u niet genoemd heeft?
We hebben regelmatig overleg met de medewerkers van de praktijk of andere gebouwgebruikers.

Met welke mensen hebt u op een reguliere werkdag te maken?
Mijn patiënten, mijn directe collega's en specialisten van andere zorginstellingen.

Welke systemen en applicaties zijn in de praktijk aanwezig?
We maken gebruik van MicroHIS en diverse webportalen voor toegang tot medische gegevens. Voor MicroHIS is een contract met de applicatieleverancier. De webportalen worden extern onderhouden omdat wij hier alleen gebruiker zijn kunnen we daar verder niks over zeggen.

Beheert uzelf of een van de praktijkmedewerkers dit systeem zelf?
De gebruikers in de applicatie beheer ik zelf. Updates worden voor ons verzorgd door de applicatieleverancier.

Hoe worden deze onderhouden?
Dat doet de applicatieleverancier. Ik weet niet hoe zij dat hebben geregeld.

Wordt er regelmatig onderhoud uitgevoerd (back-ups, updates)?
Updates worden regelmatig gedaan, hier krijgen we vooraf bericht van dat ze er even uit liggen. Volgens mij doen ze dit maandelijks. Back-ups weet ik eigenlijk niet.

Is er contact of een overeenkomst met een leverancier voor onderhoud?
Ja.

Is er een systeem/applicatiebeheerder voor deze applicatie?
Nee.

Is de toegang tot het systeem of applicatie beperkt tot specifieke medewerkers?
Ja, alleen mensen die in bepaalde applicaties mogen hebben daar een account voor.

Hoe zorgt u dat patiëntgegevens tijdens de contactmomenten privé blijven
We sluiten altijd de deur voordat we een consult of telefoongesprek beginnen. De kamer is aardig geluidsdicht dus gesprekken kunnen niet zomaar gehoord worden.

Hoe zorgt u dat relevante data goed opgeslagen worden?
Ik gebruik in de HIS-applicatie ICPC-codes. Daarnaast noteer ik ook in eigen woorden wat extra toelichting behoeft.

Weet u hoe de systemen van opslag beschermd zijn tegen bedreigingen en fouten?
Voor zover ik weet worden virussen tegen gehouden door de antivirus die op alle systemen aanwezig is. Verder zijn er alleen gebruikersfouten die zo veel als mogelijk voorkomen worden door werkinstructies en natuurlijk de ICPC-codes.

Staat Informatiebeveiliging op de agenda bij overleggen (zoals werkoverleggen en met collega's)?
Ja.

Wordt Informatiebeveiliging buiten de vooraf geplande overleggen besproken?
Ja, voornamelijk door de andere praktijkhouder geïnitieerd.

Zo ja, wat wordt er zoal besproken?
Voornamelijk de herinnering dat bij afsluiten de systemen geüpdatet moeten worden en dat antivirus zo af en toe gecheckt moet worden dat die alles nog goed bijwerkt.
Mocht er iets gebeuren in de wereld wat ook interessant is voor ons en wat in het nieuws komt wordt dat meestal ook onder de aandacht gebracht.
Ook worden deze overleggen als ideeënbusje gebruikt voor verbeterpunten.

Bij overleggen binnen de eigen praktijk wordt ook besproken:
- Continu herinnering: Geen gegevens aan derden zonder toestemming van de patiënt zelf (ook in het geval van bijvoorbeeld de partner)

Is er een personeelsbeleid?
Er zijn wat losse werkinstructies, maar geen heel HR-document o.i.d.

Worden nieuwe en bestaande medewerkers gescreend?
Er is geen complete screening, wel kijken we na of alle artsen en assistenten hun diploma bezitten.

Is er voor de medewerkers een functie- en toegangsbeleid?
Voor de HIS-applicatie krijgt elke medewerker die toegang nodig heeft voor zijn werkzaamheden een eigen inlogsysteem. Voor algemene praktijkapplicaties is een gedeelde gebruikersnaam beschikbaar.

Worden accounts uitgeschakeld of wachtwoorden gewijzigd bij medewerkers die uit dienst gaan?
Ja.

Is er een handboek of schriftelijke uitleg van de procedures in de praktijk?
Ja, er is een protocol beschikbaar voor startende assistenten. Wisseling van arts is nog maar weinig voorgekomen en daarvoor hebben we deze nog niet nodig gehad. In deze documenten staan procedures m.b.t. inloggen, voorschriften voor notities en andere werkinstructies.

Worden moeilijke wachtwoorden afgedwongen?
Nee.

Vervallen wachtwoorden periodiek?
Nee.

Wachtwoorden vervangen bij uitdienst medewerkers?
Ik verwijder de gebruiker altijd, dus dat lijkt me niet nodig.

Heeft iedere gebruiker een eigen gebruikersnaam en wachtwoord?
Ja.

Bent u op de hoogte van wachtwoorden van andere medewerkers?
Nee, als beheerder van MicroHIS kan ik ze wel inzien maar ik weet ze op dit moment niet.

Zijn andere medewerkers op de hoogte van wachtwoorden van u?
Nee.

Is er antivirus bescherming aanwezig op alle werkplekken?
Ja.

Is veilige e-mailcommunicatie mogelijk met artsen en patiënten?
Ja, we gebruiken zorgmail hiervoor.

Wordt gebruik gemaakt van een veilige internetverbinding?
Ja, de praktijken in het gebouw maken gebruik van een eZorg internetverbinding.

Hoe gaat u om met het verwijderen van vertrouwelijke data en datadragers?
We hebben bij alle bureaus een shredder staan. Daarnaast worden patiëntendossiers ingezameld en eens in de tijd opgehaald door een bedrijf die dit vernietigt.

Is er beleid voor aanschaf van nieuwe systemen of applicaties?
Nee.

Is er een aangewezen persoon verantwoordelijk voor Informatiebeveiliging?
Nee.

Hoe wordt omgegaan met IB-incidenten (Wegvallen verbinding/systeem)
Als internet wegvalt dan hebben we even geen uitslagen meer van het lab, maar we hebben onze HIS-applicatie lokaal staan dus we kunnen eigenlijk gewoon doorwerken.
Als de server zou uitvallen zouden we even geen agenda hebben. Dat is wat meer gedoe maar we kunnen alsnog gewoon doorwerken. Diagnoses kunnen met de patiënt gewoon gesteld worden, maar moeten dan later verwerkt worden in het systeem. Natuurlijk moet het systeem wel tijdig gemaakt worden.

Hoe wordt omgegaan met IB-incidenten (Wegvallen gegevens bij brand/virus/systeemcrash/etc.)
We hebben een back-up van alle gegevens buiten het pand, dus in principe is dit hetzelfde als wegvallen van een verbinding of systeem. We kunnen op een andere locatie gewoon doorwerken.

Inzage door onbevoegden (hack/nieuwsgierige patiënt/etc.)
Dit zou heel vervelend zijn. Ik zou eigenlijk nu niet weten hoe we dan moeten reageren. Ik denk dat we dat per geval bekijken.

Hoeveel uren werkt u gemiddeld?
Maandag, dinsdag, woensdag en vrijdag

Tijdsbesteding aan patiëntcontacten (spreekuur, visites, brieven, post invoeren)
Maandag (halve dag), woensdag en vrijdag.
Daarnaast dinsdag als overloop

Tijdsbesteding aan niet-patiëntgebonden uren (Denk aan financiële administratie, bestellingen, onderhoud praktijk apparatuur, personeelsbeleid en -overleg, nascholing/overleggen)
Maandag (middag).

Zijn er activiteiten die u door de werkdruk niet binnen de reguliere werkweek gedaan krijgt?
Soms is het erg druk en is onderling dagelijks overleg niet mogelijk.
Sommige andere activiteiten blijven ook liggen.

Hoe lost u dit op?
We houden in de HIS-applicatie een vragenlijst bij. Deze vragenlijst is op iedere computer te openen en daarmee kan het overleg dus wel plaatsvinden al neemt niet iedereen op hetzelfde tijdstip deel. Er zijn dan twee statussen: W is voor een vraag richting arts vanuit assistent, S voor gezien en een antwoord gegeven.

Daarnaast doe ik de volgende activiteiten buiten werktijden:
- Alle declaraties
- Post verwerken waar dit nog niet af is
- Overige administratie

De volgende activiteiten worden in de pauze momenten gedaan:
- Telefoontjes met specialisten en maken van verwijzingen
- Maand- en werkoverleg

Denkt u dat informatiebeveiliging u meer tijd zal kosten of u tijd zal opleveren? Waarom?
Ik denk dat het voornamelijk tijd kost. We zitten er nu niet lekker in maar worden er ook niet voor opgeleid. Ik denk echter wel dat het nodig is om de patiënt goed te beschermen.

Vind u dat u voldoende tijd beschikbaar heeft om onderhoud op uw systemen en applicaties uit te voeren?
Nee, alle tijd gaat richting de patiënt en overige werkzaamheden worden nu al buiten werktijd gedaan.

Vind u dat u voldoende tijd beschikbaar hebt om uzelf op de hoogte te houden op het gebied van informatiebeveiliging?
Nee, bijscholing is vooral gericht op kennis van het vak. Daar hoort kennis over informatiebeveiliging niet bij en zal dus op een ander moment bijgehouden moeten worden. Hier is zeker onvoldoende tijd voor.

Zijn er punten waar jullie weleens discussie over hebben als het gaat om informatiebeveiliging? Worden deze opgelost? Denk bijvoorbeeld aan vraagstukken rondom privacy/ patiëntgegevens
We hebben enige tijd terug met de huisartsen in de regio overlegd hoe we het beste informatie over patiënten kunnen overdragen. Hier is zowel gekeken naar wat mag en wat wij nuttig achten. Hierbij werd gezegd dat delen via bijvoorbeeld WhatsApp niet mag, maar delen op een soortgelijke eenvoudige manier wordt wel nuttig geacht voor snelle second opinion of visueel overleg. Hier hebben wij de SILO-applicatie voor in gebruik die speciaal voor dergelijke doeleinden ontwikkeld is.

Waar we continu op de situatie moeten letten:

- Communicatie met niet-Nederlands sprekenden (is de tolk betrouwbaar en bekwaam)
- Hoe wordt omgegaan met informatievragen van partner namens echtgenoot?
- Instanties proberen ook af en toe gegevens te verkrijgen (denk aan UWV en Gemeenten)
    - Deze krijgen alléén antwoord als de patiënt zelf toestemming aan ons heeft gegeven

Vind u dat uw praktijk voldoende op de hoogte is van informatiebeveiliging?
Nee, dit kan zeker beter.

Vind u dat uw praktijk voldoende beschermd?
Ja, ik heb vertrouwen in de controles en werkzaamheden van onze IT-partij.

Op welke vlakken ziet u zelf verbetermogelijkheden?
Soms zijn we voor patiënten in het telefonisch spreekuur minder goed bereikbaar omdat het gewoon erg druk is. We zijn hiervoor een terugbelspreekuur aan het inrichten zodat alle telefoontjes aangenomen worden maar mogelijkerwijs niet direct behandeld worden.

We ontvangen regelmatig post over patiënten die geen patiënt zijn van de praktijk. Indien bekend is waar het heen (of terug) moet dan wordt het doorgestuurd. Indien ontvanger of verzender onbekend zijn wordt het vernietigd.

Wat zijn volgens u de mogelijke gevolgen als vertrouwelijke informatie op straat komt?
Kan veel zijn. In het beste geval gebeurt er niks mee en wordt de slordigheid zonder schade voor de patiënt gecorrigeerd. In het ergste geval kunnen we de praktijk wel sluiten.

Praktijk 2 - Geïnterviewde: huisarts (interviewtijd +- 1,5 uur)
Locatie praktijk: Rijswijk

Welke functie vervult u: Huisarts, Praktijkhouder
Welke functies en werkzaamheden vervullen de andere medewerkers in de praktijk?

- Artsen/praktijkhouder (1x):
    - Behandelen patiënten
    - Overleg met assistenten
    - Patiëntvragen beantwoorden
    - Visites maken bij patiënten
- Assistenten (2x, samen als 1 fulltime medewerker):
    - Ondersteuning artsen
    - Patiëntbezoeken inplannen
    - Patiëntinformatie verwerken
    - Patiëntvragen beantwoorden
    - Klaarzetten behandelapparatuur
    - Op orde houden behandelapparatuur en -werktuigen
    - Overleggen met artsen
- POH somatisch (praktijk ondersteunende huisarts)
    - Gedeeld met twee andere praktijken, ieder één dag
    - Behandeling psychische klachten van patiënten

Tot welke vertrouwelijke informatie heeft u toegang tijdens het uitvoeren van uw functie?
Ik heb zelf toegang tot alle informatie in de praktijk. Dat is dus alle financiële- en patiëntinformatie.

Waar denkt u aan bij Informatiebeveiliging?
Ik denk eraan dat bijvoorbeeld de brieven die hier liggen niet onbeheerd achter moeten blijven. Mijn systeem veilig genoeg moet zijn dat niet zomaar iemand erin kan kijken. Gegevens door de IT-beheerder goed beheerd worden en voorzien van een back-up.

Houd u zichzelf bezig met Informatiebeveiliging binnen of buiten uw praktijk?
Ja, ik zit bijvoorbeeld niet op het LSP want ik heb nooit een goed gevoel gekregen over de bescherming van gegevens. De SMASH kan hier dus niet bij. De andere praktijken (waarneemgroep) kunnen wel in mijn systeem.
Verder zorg ik dat systemen zijn uitgelogd zodra mensen weggaan van hun plek en aan het einde van de dag.

Worden er in de praktijk audits uitgevoerd op informatiebeveiliging?
Er zit in ieder geval een privacy aspect in, echter weet ik niet zeker of informatiebeveiliging apart benoemd is.

Heeft de praktijk een accreditering waarbij Informatiebeveiliging getoetst wordt?
NHG-accreditering sinds eind juni van dit jaar, waarbij protocollen voor privacy horen.

Kunt u een beschrijving geven van uw werkzaamheden en activiteiten op een reguliere werkdag?

- Begin met vol spreekuur (tot 10.30u á 11.00u)
- Daarna overleg assistenten; bespreken recepten, telefonische consulten en visiteaanvragen.
- Terugbellen patiënten n.a.v. uitslagen en problemen oplossen
- Daarna visites
- Om 13.30u begint spreekuur tot 16.00u met uitloop
- Dag eindigt om 17.00u (begin nachtdienst)
- Daarna nog enkele visites
- Rond 19.30u ben ik meestal thuis, daar doe ik dan nog de administratieve werkzaamheden

Zijn er buiten de reguliere werkzaamheden nu nog activiteiten die u niet genoemd heeft?
Vaak schrijf ik thuis nog verwijsbrieven en doe ik alle andere administratieve werkzaamheden waar ik doordeweeks niet aan toekom.

Met welke mensen hebt u op een reguliere werkdag te maken?
Mijn directe collega's, natuurlijk de patiënten, specialisten van buiten waarmee ik moet overleggen en andere gebruikers van het gebouw.

Welke systemen en applicaties zijn in de praktijk aanwezig?
ASP-applicatie voor toegang tot patiëntendossiers. In deze applicatie worden alle werkzaamheden gedaan. In dit systeem zit ook e-mailfunctie voor verwijzingen e.d. Daarnaast nog MS Office voor kleine werkzaamheden, maar niet voor patiënt verwerking.

Beheert uzelf of een van de praktijkmedewerkers dit systeem zelf?
Nee, dit wordt beheerd door de ASP-leverancier

Hoe worden deze onderhouden?
De leverancier beheert het systeem

Wordt er regelmatig onderhoud uitgevoerd (back-ups, updates)?
Ik neem aan dat zij regelmatig back-ups maken.

Is er contact of een overeenkomst met een leverancier voor onderhoud?
Vast wel. Ik krijg een rekening van ze. Ik krijg geen overzicht van wat ze allemaal doen voor onderhoud van het systeem.

Is er een systeem/applicatiebeheerder voor deze applicatie?
Ja, de IT partij die deze ASP-applicatie levert beheert hem ook.

Is de toegang tot het systeem of applicatie beperkt tot specifieke medewerkers?
Ja, er is per medewerker autorisatie ingesteld tot specifieke gegevens.

Hoe zorgt u dat patiëntgegevens tijdens de contactmomenten privé blijven
Veilige communicatie voor e-mail en muziek in de wachtkamer. Enige reden hiervoor is afleiding van gesprekken, zodat er geen stilte is waardoor woorden opgevangen kunnen worden. Ik wil dat gesprekken gemaskeerd worden door muziek.

Hoe zorgt u dat relevante data goed opgeslagen worden?
Plaatsen van gegevens gebeurd vaak door assistentes (denk aan post) onder een ICPC-code. Afwijkende waardes worden op takenlijst gezet bij mij zodat ik hier extra op kan letten. Alles wordt verder via één standaard in het systeem gezet. Niet relevante informatie wordt er wel uit gelaten om te zorgen dat alles overzichtelijk blijft.

Weet u hoe de systemen van opslag beschermd zijn tegen bedreigingen en fouten?
Het systeem controleert geplaatste data, daarnaast probeer ik zelf ook alle nieuwe informatie wel te lezen om te controleren of alles er goed in is gezet.

Staat Informatiebeveiliging op de agenda bij overleggen (zoals werkoverleggen en met collega's)?
Maandelijkse vergadering met alle medewerkers en samenwerkende praktijken waar privacy en andere "dingen die niet helemaal goed gaan" worden besproken. Zo blijf je met elkaar scherp. Het terugkijken naar structurele gebeurtenissen gebeurt echter nog niet. Verslag en todo lijst van de vergadering wordt na de vergadering nagestuurd.

Wordt Informatiebeveiliging buiten de vooraf geplande overleggen besproken?
Ja, dit wordt elke dag om 11.00u tussen arts en assistenten besproken indien er een punt is om te bespreken. Dit is bij het reguliere assistentenoverleg.

Zo ja, wat wordt er zoal besproken?
Er worden voornamelijk de aandachtspunten en dingen die fout gingen besproken.

Is er een personeelsbeleid?
Met de NHG-accreditering hebben we alle medewerker specifieke afspraken, bevoegdheden en ook de diploma's en nascholingsverantwoording van iedereen in mappen gezet zodat het makkelijk terug is te vinden.

Worden nieuwe en bestaande medewerkers gescreend?
Mijn assistenten heb ik vanaf 1994, ik heb hier gewoon nog niet mee te maken gekregen.
We hebben wel een gedetacheerde. Hier hebben we een sollicitatiegesprek mee gevoerd.
We hebben we de cv, diploma's en nascholingen bekeken.

Is er voor de medewerkers een functie- en toegangsbeleid?
Ja, er is voor iedere functie beschreven wat ze mogen binnen de ASP-applicatie en binnen de praktijk. Dit wijkt dus af voor assistentes, mijzelf en PoH-arts.

Worden accounts uitgeschakeld of wachtwoorden gewijzigd bij medewerkers die uit dienst gaan?
Er is een inlog voor de eigen medewerkers, daar is al heel lang niks in gewijzigd.
Daarnaast is er een inlog voor de vakantiewaarneming. Deze wordt niet uitgeschakeld en is bekend bij de waarnemers.

Is er een handboek of schriftelijke uitleg van de procedures in de praktijk?
Voor de NHG-accreditering moesten we alle procedures en werkzaamheden op papier vastleggen. Voor de audit moet alles worden vastgelegd en wordt met alle praktijkmedewerkers de procedures doorgesproken en wordt gecontroleerd a.h.v. de documentatie. Dit is allemaal opgesteld a.h.v. de NHG-accreditering handleiding/handboek. Ook staan er werkinstructies voor reguliere taken. Er zijn ook handouts voor waarnemers. Denk hierbij aan hoe je in het systeem komt en waar je op moet letten.

Worden moeilijke wachtwoorden afgedwongen?
Van de applicatie weet ik niet hoe “moeilijk” de wachtwoorden moeten zijn. Het is al een lange tijd geleden dat ik deze heb ingevoerd. Wachtwoorden van de werkplekken zijn redelijk eenvoudig, van minimaal 8 cijfers maar hoeven geen speciale tekens te hebben ofzo.

Voor de toegang tot bijvoorbeeld uitslagen bij Reinier de Graaf (website) kan ik alleen de UZI-pas gebruiken met bijbehorende Pincode.

Vervallen wachtwoorden periodiek?
Nee, deze hoeven volgens mij niet gewijzigd te worden. Windows op de werkplekken moet wel gewijzigd worden. De ASP-applicatie daarachter vraagt dat niet en logt automatisch in, maar kan alleen gestart worden als Windows inlogt. Ik word overigens wel gek van het zo vaak moeten wijzigen van het wachtwoord.

Wachtwoorden vervangen bij uitdienst medewerkers?
Dit is tot nu toe niet van toepassing geweest.

Heeft iedere gebruiker een eigen gebruikersnaam en wachtwoord?
Ja, iedere gebruiker heeft zijn eigen inloggegevens. Er zitten in het systeem ook autorisatie niveaus, dus ik kan dingen afschermen van andere medewerkers als het gevoeliger wordt dan voor hun ogen bestemd is.

Bent u op de hoogte van wachtwoorden van andere medewerkers?
Nee

Zijn andere medewerkers op de hoogte van wachtwoorden van u?
Nee

Worden er updates uitgevoerd op systemen en applicaties? (vr. 8c)
Op de werkplekken wordt om de haverklap gevraagd om updates, dit doe ik aan het einde van de dag. In de ASP-omgeving verwacht ik dat de leverancier dit doet.

Hoe vaak wordt dit gedaan?
Op de werkplekken “om de haverklap”. In de ASP-omgeving weet ik het niet.

Is er antivirus bescherming aanwezig op alle werkplekken?
Op de lokale werkplekken is Panda antivirussoftware (gratis versie) aanwezig. Op de ASP-omgeving weet ik het niet. Ik neem aan dat de ASP-leverancier dit geregeld heeft.

Is veilige e-mailcommunicatie mogelijk met artsen en patiënten?
Vanuit de ASP-applicatie worden verwijsbrieven naar de patiënt verstuurd. Gedetailleerde informatie wordt echter niet per e-mail verstuurd. De uitwisseling met andere artsen gaat ook via beveiligde e-mail, waar de patiëntinformatie zelf via zorgdomein (beveiligde omgeving) uitgewisseld wordt.

Wordt gebruik gemaakt van een veilige internetverbinding?
Nee, er is een reguliere internetverbinding waarover de connectie met de ASP-applicatie gemaakt wordt.

Hoe gaat u om met het verwijderen van vertrouwelijke data en datadragers?
Van oude archieven weet ik niet of het verplicht is dit na 15 jaar weg te gooien. We hebben we een aparte map van overleden mensen. Die ruimen we zo af en toe op. Alles wat weg moet gaat door de shredder en dat wordt eens in de zoveel tijd opgehaald.

Is er beleid voor aanschaf van nieuwe systemen of applicaties?
Nee, deze worden aangeschaft als ze nodig zijn. Meestal op basis van aanraden van de ASP-leverancier.

Is er een aangewezen persoon verantwoordelijk voor Informatiebeveiliging?
Nee, ik regel vooral de dingen rondom de systemen.

Hoe wordt omgegaan met IB-incidenten (Wegvallen verbinding/systeem)
Zo af en toe worden we uit het systeem gegooid. Dat schijnt een bug te zijn. Dan is het beeld "geblokkeerd". De leverancier moet de gebruikers er dan uitgooien en daarna kan je weer inloggen.

Hoe wordt omgegaan met IB-incidenten (Wegvallen gegevens bij brand/virus/systeemcrash/etc.)
Ik zal in het geval van brand op mijn iPad doorwerken met de verbinding naar de ASP-leverancier. Bij virussen, systeemcrash en andere dingen ga ik ervan uit dat de ASP-leverancier deze goed oplost. In de tussentijd kunnen wij gewoon met de patiënt doorwerken en alles op papier noteren. De systemen om te registreren zijn voor mijn patiëntenzorg niet op elk moment nodig.

Inzage door onbevoegden (hack/nieuwsgierige patiënt/etc.)
Niet is onmogelijk, maar we proberen hier aandacht aan te besteden tijdens overleggen, zodat het niet of zo weinig mogelijk voorkomt. Neem bijvoorbeeld aan het sluiten van deuren bij telefoongesprekken.
We zijn wel een keer geschrokken van iemand die het loket had geopend omdat hij zijn eigen briefje zag liggen en deze had meegenomen. Dit hebben we besproken en vanaf nu wordt het loket continu afgesloten (slot met cijfercode).

Hoeveel uren werkt u gemiddeld?
Ongeveer 12 uur op een dag, dit is altijd al geweest van vroeg af aan. De vrijdag is uitbesteed aan een andere arts, om een dag rust te kunnen houden. Wel gebruik ik deze dag vaak als overloop van de rest van de week.

Tijdsbesteding aan patiëntcontacten (spreekuur, visites, brieven, post invoeren)
Eigenlijk is de gehele dag plus een groot deel daarna aan patiëntencontacten besteed.

Tijdsbesteding aan niet-patiëntgebonden uren (Denk aan financiële administratie, bestellingen, onderhoud praktijk apparatuur, personeelsbeleid en -overleg, nascholing/overleggen)
Onderhoud van gebouw doet de verhuurder. Financiële administratie doet mijn vrouw.

Zijn er activiteiten die u door de werkdruk niet binnen de reguliere werkweek gedaan krijgt?
Vooral het administratief werk doe ik vaak op zondag. Eigenlijk alles wat niet past binnen het patiëntcontact gaat automatisch buiten de werkdag.

Hoe lost u dit op?
Eigenlijk niet, dit is al jaren mijn werkritme en er is gewoon veel te doen.

Denkt u dat informatiebeveiliging u meer tijd zal kosten of u tijd zal opleveren? Waarom?
Het kost tijd. Zoiets levert nooit tijd op. De dingen die je selecteert als belangrijk geef je extra aandacht, maar dat kost tijd om te onderhouden. Je krijgt er wel kwaliteit voor terug.
Vroeger was het bijna 100% patiëntenzorg met patiëntinformatie op de (kwetsbare) groene kaart, tegenwoordig zitten er veel meer administratieve handelingen omheen. Dat betekent wel dat je preciezer noteert in de HIS-applicatie. Kwaliteit van de informatie gaat dus wel omhoog, echter wil je wel overdag nog patiënten blijven verzorgen, dus kost het vaak daarbuiten extra tijd voor alle administratie.
Neem ook bijvoorbeeld de praktijkaccreditatie. Hiervoor heb je veel tijd nodig om het goed op papier te krijgen. Echter krijg je er wel kwaliteit voor terug omdat je de aandachtspunten met elkaar kan overleggen. Het was een hoop werk om alle protocollen op papier te krijgen, maar nu weet iedereen hoe het werkt. Ook is het voor andere artsen makkelijker om te begrijpen hoe het hier werkt.

Vind u dat u voldoende tijd beschikbaar heeft om onderhoud op uw systemen en applicaties uit te voeren?
Ik doe de eigen updates aan het einde van de dag. Verder hoef ik er niet veel aan te doen.

Vind u dat u voldoende tijd beschikbaar hebt om uzelf op de hoogte te houden op het gebied van informatiebeveiliging?
Ik krijg van de beroepsgroep (via LHV) wel af en toe informatie. Ik zoek echter niet proactief naar nieuwe informatie. Daar heb ik gewoon te weinig tijd voor.

Zijn er punten waar jullie weleens discussie over hebben als het gaat om informatiebeveiliging? Worden deze opgelost? Denk bijvoorbeeld aan vraagstukken rondom privacy/ patiëntgegevens
We hebben bijvoorbeeld de uitslagen die moeders over kinderen vragen. Tot op zekere leeftijd geef je deze, daarna niet meer. Ander voorbeeld is overdracht van dossiers. Je kan wel een kopie of afschrift aan de patiënt geven, echter gaat het origineel altijd aangetekend (en na toestemming van de patiënt) naar de nieuwe huisarts.
Bij bijvoorbeeld een onder toezicht stelling, waarbij ouders niet meer de dagelijkse verzorging hebben, hebben ouders wel recht op informatie en soms niet.
Ik bel zo af en toe wel met de juridische afdeling van de LHV om na te vragen of iets wel/niet mag.

Vind u dat uw praktijk voldoende op de hoogte is van informatiebeveiliging?
Ik houd wel de highlights van verschillende mailings bij. Uit de mail van de LHV lees ik dan de highlights. Bij de mails van Huisarts Vandaag bijvoorbeeld ook.

Vind u dat uw praktijk voldoende beschermd?
In principe wel, maar ik vind wel dat er dagelijks grote bedreigingen voorbijkomen en dus heel precies moet zijn in de omgang met gegevens. Zowel voor mijzelf als de assistenten behoeft het dus continu alertheid.

Er is in het pand een alarminstallatie die brand en andere dingen ook registreert. Wij worden bericht als die afgaat. Er zitten extra deuren en sloten voor toegang tot het analoge archief.

Op welke vlakken ziet u zelf verbetermogelijkheden?
Alles vergt vooral continu aandacht. Als je ergens even niet op let dan kan het meteen grote gevolgen hebben. Dat is lastig om te verbeteren, maar we proberen er gewoon alert op te zijn.

Er worden vaak “herinneringen” gevraagd door externen. Deze zet ik als taken in de toekomst in de applicatie. Zo is soms een extra controle nodig een half jaar van nu (voor de patiënt uiteraard van belang). Dan maak ik dus een extra taak aan die dan zichtbaar wordt. Hiermee probeer ik alles zo veel mogelijk bij te houden, maar het is wel erg veel. Ik heb wel het gevoel dat ik met dit systeem alles redelijk op orde heb.

Wat zijn volgens u de mogelijke gevolgen als vertrouwelijke informatie op straat komt?
Klacht over de praktijk dat de gegevens niet veilig zijn. Daar proberen we dus alert op te zijn omdat het écht belangrijk is.

Praktijk 3 - Geïnterviewde: huisarts (interviewtijd +- 1,5 uur)
Locatie praktijk: Den Haag

Welke functie vervult u: Huisarts, Praktijkhouder
Welke functies en werkzaamheden vervullen de andere medewerkers in de praktijk?

- Artsen/praktijkhouder (1x):
    - Behandelen patiënten, zoals kleine chirurgische ingrepen, COPD-spreekuur
    - Overleg met assistenten
    - Patiëntvragen beantwoorden
    - Visites maken bij patiënten
    - Managen van personeel
    - Beheer van financiële zaken voor de praktijk
- HIDHA - Arts (1x)
    - Behandelen patiënten
    - Overleggen met specialisten
    - Overleggen met andere arts en assistenten
- Assistenten (2x):
    - Ondersteuning artsen
    - Patiëntbezoeken inplannen
    - Patiëntinformatie verwerken
    - Patiëntvragen beantwoorden
    - Klaarzetten behandelapparatuur
    - Op orde houden behandelapparatuur en -werktuigen
    - Overleggen met artsen
- POH GGZ (praktijk ondersteunende huisarts, niet in dienst)
    -
    - Behandeling psychische klachten van patiënten

Tot welke vertrouwelijke informatie heeft u toegang tijdens het uitvoeren van uw functie?
Alle informatie die we van de specialist krijgen. Alle informatie die we van artsenorganisaties krijgen. Alle informatie die wij van patiënten krijgen of die we doorgeven aan patiënten.

Waar denkt u aan bij Informatiebeveiliging?
Dat informatie niet kan lekken naar derden toe die er niks mee te maken hebben. De softwareleverancier zegt dat alles via veilige systemen staat en dit garandeert. Bijvoorbeeld receptuur die je verstuurt via een beveiligd systeem of telefonie via beveiligde kanalen.

Houd u zichzelf bezig met Informatiebeveiliging binnen of buiten uw praktijk?
Ik ben er binnen mijn praktijk mee bezig en breng wat ik leer ook mee naar de SMASH waar ik ook werk.

Worden er in de praktijk audits uitgevoerd op informatiebeveiliging?
Er worden jaarlijks tussentijdse audits uitgevoerd, waarbij ook naar de systeembeveiliging gekeken wordt. Om de drie jaar krijg je een volledige audit met enquêtes voor de patiënten.

Heeft de praktijk een accreditering waarbij Informatiebeveiliging getoetst wordt?
In de accreditatie is gekeken of de praktijk beveiligd is. Zo is gekeken of elke computer van een wachtwoord is voorzien en HIS-systeem alleen met UZI-pas toegankelijk is.

Kunt u een beschrijving geven van uw werkzaamheden en activiteiten op een reguliere werkdag?
Ik werk drie dagen in de week. Die zijn uitsluitend met patiëntencontacten gevuld.
Op de “vrije” dagen doe ik het administratieve gedeelte van de praktijk. Hieronder valt vooral de controle van financiële en gebeurtenis administratie.

Zijn er buiten de reguliere werkzaamheden nu nog activiteiten die u niet genoemd heeft?
Daarnaast gaat ook de nascholing natuurlijk buiten werkdagen. Dit houd ik goed bij, want vind ik leuk. Dit is vooral gericht op nieuwe behandeltechnieken en opfrissing van bestaande kennis, niet echt op privacy of beveiliging.

Met welke mensen hebt u op een reguliere werkdag te maken?
Voornamelijk met mijn patiënten en assistenten.

Welke systemen en applicaties zijn in de praktijk aanwezig?
We hebben een aantal websites waar we op kijken voor het verkrijgen van informatie. Verder hebben we eigenlijk alleen de HIS-applicatie waarin we werken.

Beheert uzelf of een van de praktijkmedewerkers dit systeem zelf?
De ASP-leverancier doet het onderhoud en hosting. Zij testen zo af en toe het systeem en leveren hier eens in de tijd rapportjes over op.

Hoe worden deze onderhouden?
De HIS-applicatie doet de ASP-leverancier, hoe weet ik niet.
Lokale systemen worden door mijzelf bijgehouden als het gaat om updates en antivirus.

Wordt er regelmatig onderhoud uitgevoerd (back-ups, updates)?
Weet ik eigenlijk niet. Ze melden in ieder geval maandelijks dat er onderhoud is waardoor het systeem even niet beschikbaar is. Dit zijn volgens mij de updates. Deze worden wel buiten kantoortijden gepland.
Om de maand kijk ik even in de rapporten van updates en antivirus of alles nog goed gaat.

Is er contact of een overeenkomst met een leverancier voor onderhoud?
Ja, er is een overeenkomst met de leverancier.

Is er een systeem/applicatiebeheerder voor deze applicatie?
Niet vanuit de praktijk, maar de ASP-leverancier heeft er waarschijnlijk diversen.

Is de toegang tot het systeem of applicatie beperkt tot specifieke medewerkers?
Alleen de mensen met een UZI-pas kunnen in de HIS-applicatie.

Hoe zorgt u dat patiëntgegevens tijdens de contactmomenten privé blijven
We hebben hier allemaal afgesloten ruimten, waarbij de deuren altijd dicht zijn tijdens gesprekken. Daarnaast hebben we ook een kleine ruimte om tijdens besprekingen met gezinnen ook gesprekken te kunnen houden met individuen.
Als ik wegloop van mijn scherm zorg ik altijd dat deze afgesloten is zodat patiënten niet even kunnen kijken als ik ergens anders bezig ben.

Buiten deze kamer hebben we ook nog de balie van de assistenten afgesloten met een schuifdeur, zodat telefoongesprekken niet gehoord kunnen worden in de wachtkamer. Daarnaast is achtergrondmuziek aanwezig in de wachtkamer om geen gesprekken te kunnen opvangen als het daar stil is.

Hoe zorgt u dat relevante data goed opgeslagen worden?
Wat we heel veel hebben gedaan is om alles ICPC te coderen (duidelijkheid). Daarmee komt het goed in het systeem. Bij verhuizing komen de codes dan ook goed over.

Weet u hoe de systemen van opslag beschermd zijn tegen bedreigingen en fouten?
Nee, dit wordt door de ASP-leverancier geregeld.

Staat Informatiebeveiliging op de agenda bij overleggen (zoals werkoverleggen en met collega's)?
Ja, echter wordt het niet elk overleg besproken. Iedere medewerker wordt uitgenodigd om punten in te brengen. Daarnaast worden incidenten altijd besproken. Actiepunten en dingen door patiënten ingebracht worden ook de volgende vergadering besproken om te de opvolging te kunnen zien.

Wordt Informatiebeveiliging buiten de vooraf geplande overleggen besproken?
Ja, ik breng zo af en toe punten in voor de besprekingen met de andere praktijken in het gebouw. Verder bespreken we losse punten die naar voren komen.

Zo ja, wat wordt er zoal besproken?
Wat bijvoorbeeld besproken worden is hoe om te gaan met klachten en hoe (voornamelijk de frontdesk assistenten) kunnen zorgen dat meeluisteren niet mogelijk is.

Is er een personeelsbeleid?
Voor het in dienst komen van een arts in opleiding is er een instructie, zodat accounts en alle overige materialen geregeld worden en de arts weet hoe hij bij ons aan de slag kan gaan en wat hij allemaal mag.

Worden nieuwe en bestaande medewerkers gescreend?
Onze medewerkers zijn al jaren in dienst. Hiervoor is de vraag dus niet relevant. De artsen in opleiding worden door Leiden gescreend dus dit hoeven we niet zelf te doen.

Is er voor de medewerkers een functie- en toegangsbeleid?
We hebben een procedure document waarin staat wat van medewerkers verwacht wordt. Je zou dit kunnen zien als een functieprofiel. Toegang in de omgeving wordt op basis daarvan geregeld.

Worden accounts uitgeschakeld of wachtwoorden gewijzigd bij medewerkers die uit dienst gaan?
Het verwijderen van gebruikers doe ik in de ASP-applicatie. De leverancier maakt een gebruiker om toegang te krijgen tot dit systeem.

Is er een handboek of schriftelijke uitleg van de procedures in de praktijk?
We hebben intern een protocol voor uitwisseling en gebruik van data, zodat iedereen weet hoe we moeten werken. Ditzelfde geldt voor de andere werkinstructies. Daarnaast zijn er diverse protocollen voor het werk en communicatie. Er is ook informatie over onze privacyregeling op onze website beschikbaar zodat patiënten kunnen lezen hoe wij werken.

Worden moeilijke wachtwoorden afgedwongen?
Nee, toegang kan alleen met de eigen UZI-pas in combinatie met PIN-code. Dit is de enige optie. Toegang tot andere applicaties worden gedaan met moeilijke wachtwoorden. Dit wordt afgedwongen door de leverancier.

Vervallen wachtwoorden periodiek?
Ik verander eens in de zoveel tijd het wachtwoord van de algemene mailbox, verder heeft iedereen een eigen wachtwoord voor de applicaties en die moeten eens in de tijd veranderd worden.

Wachtwoorden vervangen bij uitdienst medewerkers?
Dit is niet van toepassing.

Heeft iedere gebruiker een eigen gebruikersnaam en wachtwoord?
Ja, omdat iedere medewerker zijn eigen UZI-pas heeft.
Er is wel een gedeeld wachtwoord voor de mailbox van de praktijk die iedere medewerker kent.

Bent u op de hoogte van wachtwoorden van andere medewerkers?
Nee, wachtwoorden gebruiken we niet. Daarnaast ben ik niet op de hoogte van de PIN-codes van anderen.

Zijn andere medewerkers op de hoogte van wachtwoorden van u?
Nee.

Worden er updates uitgevoerd op systemen en applicaties?
Ja, de ASP-leverancier doet dit voor de applicatie. Ik doe dit zelf voor de lokale systemen.

Hoe vaak wordt dit gedaan?
Ten minste maandelijks.

Is er antivirus bescherming aanwezig op alle werkplekken?
Ja, dit onderhoud ik zelf.

Is veilige e-mailcommunicatie mogelijk met artsen en patiënten?
We hebben in het kader van de bedrijfsaccreditatie als een van de verbeterpunten staan om alle actuele e-mailadressen van de patiënten te verzamelen. Dit zorgt ervoor dat kleine punten bij de juiste personen terecht komt.
We gebruiken zorgdomein voor veilige communicatie met specialisten en collega huisartsen.

Wordt gebruik gemaakt van een veilige internetverbinding?
Er is een lijn voor zowel ons internetverkeer als onze telefonie. Er moet voor toegang tot de HIS-applicatie wel eerst een beveiligde verbinding met de omgeving gemaakt worden.

Hoe gaat u om met het verwijderen van vertrouwelijke data en datadragers?
Papieren dossiers worden vernietigd. Verder staan alle data bij de ASP-leverancier in de HIS-applicatie. Deze worden verwijderd met het verwijderen van oude dossiers. USB-schijven gebruiken we niet.

Is er beleid voor aanschaf van nieuwe systemen of applicaties?
Nee.

Is er een aangewezen persoon verantwoordelijk voor Informatiebeveiliging?
Nee.

Hoe wordt omgegaan met IB-incidenten (Wegvallen verbinding/systeem)
Internet wil nog weleens uitvallen. Ik gebruik dan mijn mobiele hotspot als alternatief.

Hoe wordt omgegaan met IB-incidenten (Wegvallen gegevens bij brand/virus/systeemcrash/etc.)
Dit moet de ASP-leverancier regelen.

Inzage door onbevoegden (hack/nieuwsgierige patiënt/etc.)
Jaren geleden zijn er wat klachten binnengekomen over de gehorigheid van de balie, aan de hand daarvan hebben we destijds de schuifdeur aangebracht. Muziek was reeds aanwezig maar nog niet voldoende. Verder bekijken we dit per geval/klacht, maar dit is de laatste jaren niet meer voorgekomen.
Daarnaast hebben verzekeraars nog wel een handje om “alles” op te vragen, zoals “gaarne dossieroverzicht”. Ik laat hun dan eerst weten hun vraag zo specifiek mogelijk te stellen en maximaal 5 vragen. Dan lever ik in ieder geval alleen relevante data aan. Voorafgaande vraag ik altijd toestemming aan de patiënt. Telefonische aanvragen worden niet gehonoreerd, alleen schriftelijke.

Hoeveel uren werkt u gemiddeld?
Drie dagen, de andere twee dagen ben ik meestal met de artsen in opleiding en administratie bezig.

Tijdsbesteding aan patiëntcontacten (spreekuur, visites, brieven, post invoeren)
Dit is eigenlijk de complete werktijd van de drie dagen.

Tijdsbesteding aan niet-patiëntgebonden uren (Denk aan financiële administratie, bestellingen, onderhoud praktijk apparatuur, personeelsbeleid en -overleg, nascholing/overleggen)
Twee dagen maximaal, meestal is dit rond de 8 á 10 uur. Soms ook wat meer.
Daarnaast heb je nog wat avonden voor nascholing die verplicht is voor je accreditering als huisarts.

Zijn er activiteiten die u door de werkdruk niet binnen de reguliere werkweek gedaan krijgt?
Vooral de administratie. Daarnaast opgevraagde documenten van bijvoorbeeld verzekeraars.

Hoe lost u dit op?
Ik doe de administratie en opgevraagde stukken meestal wat later (1 á 2 weken later).

Denkt u dat informatiebeveiliging u meer tijd zal kosten of u tijd zal opleveren? Waarom?
Ik denk dat er na het insteken van tijd voor het invoeren van goede processen, dat het inmiddels wel tijd oplevert. De storingen aan apparatuur en vertragingen door onduidelijkheden en extra overleg komen steeds minder voor.

Vind u dat u voldoende tijd beschikbaar heeft om onderhoud op uw systemen en applicaties uit te voeren?
Dit wordt door de leverancier gedaan. Ik neem aan dat ze hiervoor voldoende tijd inplannen.

Vind u dat u voldoende tijd beschikbaar hebt om uzelf op de hoogte te houden op het gebied van informatiebeveiliging?
Ja, ik ben niet de enige die op de hoogte moet blijven voor veilig maken van de praktijk.

Zijn er punten waar jullie weleens discussie over hebben als het gaat om informatiebeveiliging? Worden deze opgelost? Denk bijvoorbeeld aan vraagstukken rondom privacy/ patiëntgegevens
Bijvoorbeeld als ouder wat voor kind wil aanvragen, waardoor informatie gevraagd wordt die niet per se gedeeld mag worden. Ook voor dit soort situaties is een protocol aanwezig. VIM-registratie (Veiligheids Incident Melden) wordt dan besproken als er toch wat fout gaat zodat dat in het vervolg niet meer gebeurd.
We hebben hier veel expats, daarom spreken alle medewerkers van de praktijk in ieder geval ook goed Engels. Andere talen hebben we hier eigenlijk niet.

Vind u dat uw praktijk voldoende op de hoogte is van informatiebeveiliging?
Ik probeer vooral de collega's rond mij verder in te lichten, dat kan wel beter.

Vind u dat uw praktijk voldoende beschermd?
Ja, al vind ik het leuk om me op de hoogte te houden en verder te verbeteren.

Op welke vlakken ziet u zelf verbetermogelijkheden?
Op dit moment worden receptaanvragen van de telefooncentrale naar een "normale" mailbox verstuurd. De telefonie leverancier is hiervoor momenteel aan het kijken hoe dit veiliger kan. Verder zijn we nog met verbeteringen bezig voor aankomend jaar. Dit wil ik niet alleen doen zodat de anderen ook meer op de hoogte zijn van alle keuzes die zijn gemaakt.

Wat zijn volgens u de mogelijke gevolgen als vertrouwelijke informatie op straat komt?
Ik denk dat voornamelijk een slechter patiëntvertrouwen de praktijk zal schaden. Er zal vast ook een boete zijn, echter vind ik het vervelender als patiënten benadeeld worden.

Praktijk 4 - Geïnterviewde: huisarts (interviewtijd +- 1,5 uur)
Locatie praktijk: Rijswijk

Welke functie vervult u: Huisarts, Praktijkhouder
Welke functies en werkzaamheden vervullen de andere medewerkers in de praktijk?

- Artsen/praktijkhouder (2x):
    - Behandelen patiënten (gesprekken, verrichtingen, klein chirurgie)
    - Overleg met assistenten
    - Patiëntvragen beantwoorden
    - Maken van verwijsbrieven en recepten
    - Visites maken bij patiënten
    - Beantwoorden vragen verzekeringsmaatschappijen
    - Invoeren en bijhouden administratie
    - Contact met leveranciers en collega's onderhouden
    - Declaraties uitvoeren en contact met verzekeraars en boekhouder onderhouden
- Assistenten (3x):
    - Ondersteuning artsen
    - Patiënten behandelen (bloeddruk, oren uitspuiten, injecties, wratten aanstippen)
    - Patiëntbezoeken inplannen
    - Patiëntinformatie verwerken
    - Recepten maken o.b.t. aanvraag receptenlijn.
    - Patiëntvragen beantwoorden (telefonisch)
    - Klaarzetten behandelapparatuur
    - Op orde houden behandelapparatuur en -werktuigen
    - Overleggen met artsen
- POH somatisch (praktijk ondersteunende huisarts)
    - Dit is een van de assistentes, dus géén extra persoon
    - Behandeling psychische klachten van patiënten

Tot welke vertrouwelijke informatie heeft u toegang tijdens het uitvoeren van uw functie?
De volledige historie van al mijn patiënten.

Waar denkt u aan bij Informatiebeveiliging?
Wat bij ons vooral speelt is dat niet zomaar iedereen in de dossiers kan inloggen of lezen. Dit zowel van buitenaf (iemand die er niet in hoort) en daarnaast ook dat je onderling niet alles hoeft te zien. Verder dat je discreet met informatie omgaat.

Houd u zichzelf bezig met Informatiebeveiliging binnen of buiten uw praktijk?
Ik houd me hier een beetje mee bezig maar kan zelf weinig oplossen. Hiervoor vraag ik de ICT-leverancier om mij bij te staan voor onderhoud en verbeteren van beveiliging.

Worden er in de praktijk audits uitgevoerd op informatiebeveiliging?
Nee.

Heeft de praktijk een accreditering waarbij Informatiebeveiliging getoetst wordt?
Nee, we willen hier volgend jaar wel aan beginnen.

Kunt u een beschrijving geven van uw werkzaamheden en activiteiten op een reguliere werkdag?
Je hebt je spreekuren, huisbezoeken, telefoontjes met patiënten en specialisten.
Daarnaast maken van brieven voor verwijzingen en verzekeraars. Bij het spreekuur zit dan ook kleine chirurgie.
Ik doe ook de administratie, waar dit overdag kan. Ik zorg dat declaraties gedaan worden en contact met diverse partijen (verzekeraars, boekhouder, etc.) gehouden wordt.

Zijn er buiten de reguliere werkzaamheden nu nog activiteiten die u niet genoemd heeft?
Nee.

Met welke mensen hebt u op een reguliere werkdag te maken?
Mijn assistenten, collega's in de wijk en specialisten die onze patiënten behandelen.

Welke systemen en applicaties zijn in de praktijk aanwezig?
OmniHIS is onze HIS-applicatie.
Daarnaast gebruiken we de webbrowser voor toegang tot mail en andere informatie.

Beheert uzelf of een van de praktijkmedewerkers dit systeem zelf?
Nee, dit doet onze ICT-leverancier.

Hoe worden deze onderhouden?
Eens in de 12 weken is deze op locatie. Dan worden updates uitgevoerd. Ook worden oude bestanden opgeschoond en andere onderhoudswerkzaamheden gedaan als deze nodig zijn.

Wordt er regelmatig onderhoud uitgevoerd (back-ups, updates)?
Ja, eens in de 12 weken dus op locatie. Daarnaast wordt het HIS-systeem constant op afstand bijgewerkt. Deze staat bij een externe ASP-leverancier.
Back-ups worden door de ASP-leverancier gemaakt. Deze geeft zo af en toe een mededeling wanneer er werkzaamheden zijn.

Is er contact of een overeenkomst met een leverancier voor onderhoud?
Met de OmniHIS leverancier heb ik een overeenkomst.

Is er een systeem/applicatiebeheerder voor deze applicatie?
Nee, we gebruiken onze ICT-leverancier hiervoor. Deze heeft ook met de HIS-leverancier contact als dit nodig is.

Is de toegang tot het systeem of applicatie beperkt tot specifieke medewerkers?
Ja, ik heb bijvoorbeeld meer rechten dan de assistenten. Daarnaast kunnen we onderdelen ook van een slotje voorzien zodat de specifieke medewerker er alleen bij kan. Dit is vooral handig als er familieleden of collega's e.d. in de praktijk zitten.

Hoe zorgt u dat patiëntgegevens tijdens de contactmomenten privé blijven
De ruimte zelf is afgesloten, dus buiten de kamer kan niemand het horen. Soms wordt je gebeld tijdens het spreekuur. Dan voorkom je in ieder geval dat je namen en gedetailleerde gegevens noemt. Bijna altijd loop ik dan even naar een andere ruimte. De assistentes zitten in een afgesloten ruimte zodat patiënten in de wachtkamer hun gesprekken in ieder geval niet kunnen horen.

In contactmomenten met ziekenhuizen proberen we eerst te achterhalen of we echt de persoon aan de lijn hebben die we willen bereiken. Andersom gebeurt het ook, dat we worden teruggebeld als we informatie bij een ziekenhuis proberen op te vragen.

Hoe zorgt u dat relevante data goed opgeslagen worden?
Dit is een lastig punt. Alles moet tegenwoordig ICPC gecodeerd worden. Maar met name bij patiënten die vaak komen krijg je dan een hele waslijst aan episodes. Daar het goede uitfilteren kan werken want elke klacht coderen werkt verstorend. Je wordt er echter wel op afgerekend als je het niet doet. Sommige punten wil ik niet in het HIS hebben omdat het erg gevoelig ligt maar wellicht een loze melding is. Dit zou dan op een verwijsbrief terecht kunnen komen zonder dat dit gegrond hoeft te zijn. Dit soort “mogelijk loze” items houd ik dan ook apart van de HIS. Dit raadpleeg ik wel voorafgaande aan het consult.

Weet u hoe de systemen van opslag beschermd zijn tegen bedreigingen en fouten?
Dit regelt de ASP-leverancier.

Staat Informatiebeveiliging op de agenda bij overleggen (zoals werkoverleggen en met collega’s)?
We hebben maandelijks overleg met de medewerkers. Hier wordt het gebruik van internet (openen van sites) en de PC besproken om dit onder de aandacht te houden.

Daarnaast willen we de praktijkaccreditatie ook bespreken in het eerstvolgende wijkoverleg. Dit omdat de omringende praktijken ook niet geaccrediteerd zijn en een gezamenlijke effort wellicht veel nut kan hebben en per praktijk ook extra voordeel heeft.

Wat we ook bespreken is aansluiting bij het LSP. Hier had ik geen goed gevoel bij. Omdat ik echter wel druk voelde om hierbij aan te sluiten vanuit de LSP-organisatie heb ik dit wel gedaan. Patiënten includeren hiervoor heb ik echter nooit gedaan.

Wordt Informatiebeveiliging buiten de vooraf geplande overleggen besproken?
Ja, met wijkcollega’s bespreken we vaak actuele onderwerpen. Er zitten een aantal artsen tussen die dit fanatiek bijhouden.

Zo ja, wat wordt er zoal besproken?
Neem bijvoorbeeld de bedreigingen op websites of het klikken op linkjes in de e-mail. Dat neem ik vervolgens mee naar de praktijk overleggen zodat de andere arts en assistenten ook op de hoogte zijn.

Is er een personeelsbeleid?
Er is wel een vaste procedure, maar dat is wel lang geleden want er wisselt niet zo veel.

Worden nieuwe en bestaande medewerkers gescreend?
Bij de assistenten kijk je de sollicitatie en cv goed na en vraagt referenties op. Bij de artsen controleer je de BIG-registratie. Waarnemers moeten ook altijd even op gesprek komen en een btw-verklaring aanleveren zodat een BIG-registratie gecontroleerd kan worden.

Is er voor de medewerkers een functie- en toegangsbeleid?
Nee.

Worden accounts uitgeschakeld of wachtwoorden gewijzigd bij medewerkers die uit dienst gaan?
Ja, dit doe ik zelf.

Is er een handboek of schriftelijke uitleg van de procedures in de praktijk?
Ja, ik heb diverse mappen met instructies voor het gebruik van de diverse websites (LSP, ZorgDomein, UZI) en applicaties. Deze bewaar ik zodra ik deze van de leverancier of specialist binnenkrijg.

Worden moeilijke wachtwoorden afgedwongen?
Nee.

Vervallen wachtwoorden periodiek?
Nee. Bedoeling was om met UZI passen te gaan werken. Dit werd lang geroepen dat dit verplicht zou worden. Dus destijds had ik ze aangevraagd en bij het postkantoor afgehaald. Echter liet de implementatie in de software zo lang op zich wachten dat de eerste passen alweer verlopen waren. Ik had daarna geen zin meer om weer geld uit te geven voor een systeem wat nog niet werkte dus heb deze uiteindelijk niet aangeschaft.

Wachtwoorden vervangen bij uitdienst medewerkers?
Ja, de accounts worden meteen uitgezet door mij. Kom ik er niet uit omdat ik het te lang niet meer heb gedaan dan vraag ik de ICT-leverancier om hulp.

Heeft iedere gebruiker een eigen gebruikersnaam en wachtwoord?
Ja, iedereen heeft een eigen gebruikersnaam met eigen rechten.

Bent u op de hoogte van wachtwoorden van andere medewerkers?
Heel soms als een waarnemer kort komt. Na afloop wordt het wachtwoord van het gebruikte account dan wel gewijzigd.

Zijn andere medewerkers op de hoogte van wachtwoorden van u?
Nee.

Worden er updates uitgevoerd op systemen en applicaties?
Dit wordt gedaan door de ICT-leverancier. Kleine updates van de werkplekken doen we zelf, deze gebeuren aan het einde van de dag.

Hoe vaak wordt dit gedaan?
Eens in de 6 weken hebben we een afspraak. Dit is 1x telefonisch en 1x hier in de praktijk. Dus om de 12 weken worden alle systemen nagelopen op afwijkingen en worden updates, waar deze nog nodig zijn, geïnstalleerd.

Is er antivirus bescherming aanwezig op alle werkplekken?
Ja, dit is aanwezig en houd ik bij.

Is veilige e-mailcommunicatie mogelijk met artsen en patiënten?
Ja, dit gaat via ZorgDomein. Overdracht van dossiers gaat via post. Bijvoorbeeld de verwijzingen via Zorgdomein op een beveiligde website.

Wordt gebruik gemaakt van een veilige internetverbinding?
Ja, deze verbinding wordt geleverd door eZorg. Daarnaast letten we op de slotjes van alle sites. Daarnaast bieden diverse organisaties beveiligde sites aan om bijvoorbeeld uitslagen van het ziekenhuis te kunnen inzien. Een verdere integratie met het HIS moet nog komen.

Hoe gaat u om met het verwijderen van vertrouwelijke data en datadragers?
Soms heb ik een USB om dingen op te slaan van belangrijke documenten. De ICT-leverancier zorgt dat alles veilig verwijderd wordt. Papieren dossiers van voor 1994 worden vernietigd in een versnipperaar. Oude dossiers van overleden patiënten die verwijderd mogen worden (na 15 jaar) worden verbrand in de open haard.

Is er beleid voor aanschaf van nieuwe systemen of applicaties?
Nee, als ik deze nodig heb vraag ik dit aan de ICT-leverancier. Specifieke eisen heb ik hier niet voor.

Is er een aangewezen persoon verantwoordelijk voor Informatiebeveiliging?
Nee.

Hoe wordt omgegaan met IB-incidenten (Wegvallen verbinding/systeem)
Dit is nog niet voorgekomen, maar in principe kunnen we gewoon doorwerken zonder de systemen dus mag de ASP-leverancier dat herstellen terwijl wij doorwerken.

Hoe wordt omgegaan met IB-incidenten (Wegvallen gegevens bij brand/virus/systeemcrash/etc.)
We sluiten alles netjes af en het gebouw is van een alarm voorzien. Er is bij een collega weleens een laptop gestolen. Gelukkig stond daar geen patiëntinformatie op omdat hij alleen de ASP-applicatie gebruikte. Maar we hebben hier niet mappen of instructies voor liggen hoe we met dit soort dingen om moeten gaan.

Inzage door onbevoegden (hack/nieuwsgierige patiënt/etc.)
Ik probeer tegen bijvoorbeeld verzekeraars zo summier mogelijk te zijn. Vaak vraagt de verzekering veel gegevens. Je kan natuurlijk niet liegen, maar ze zomaar alles geven ga ik ook zeker niet doen. Daarnaast zorg ik dat de machtiging van de patiënt altijd precies weergeeft wat doorgegeven mag worden. Een “ik machtig <<verzekeraar>> om alles te communiceren” zal ik dus niet accepteren. Telefonisch zal ik ook niks doorgeven. Dit is te veel aan eigen interpretatie onderhevig.

In een ander geval gaan bijvoorbeeld ouders zich met kinderen bemoeien of andersom, terwijl dit niet gewenst of toegestaan is. In dit geval zetten we een memoveld bij de patiënt zodat hier extra op gelet wordt.

Hoeveel uren werkt u gemiddeld?
Ik werk vier dagen in de praktijk en mijn collega eigenlijk ook.
Daarnaast hebben we nog een waarnemer voor een halve dag.

Tijdsbesteding aan patiëntcontacten (spreekuur, visites, brieven, post invoeren)
Ik denk dat ik ongeveer 85% patiëntgebonden taken heb in de tijd dat ik bezig ben. Dit is wel 100% van de vier dagen dat ik bezig ben. Dit is ongeveer 11 uur per dag.

Tijdsbesteding aan niet-patiëntgebonden uren (Denk aan financiële administratie, bestellingen, onderhoud praktijk apparatuur, personeelsbeleid en -overleg, nascholing/overleggen)
De resterende tijd is ongeveer 15%, dit past echter niet in mijn vier werkdagen. Dit doe ik dan ook in de avonden of het weekend. Dit zijn zeker nog 6 á 8 uur aan andere taken.

Zijn er activiteiten die u door de werkdruk niet binnen de reguliere werkweek gedaan krijgt?
Zoals gezegd zijn alle niet-patiëntgebonden taken buiten mijn werktijd. Dit is wel afhankelijk van hoeveel tijd ik ook privé over heb.

Hoe lost u dit op?
Ik werk dus veel thuis om wel bij te blijven.

Denkt u dat informatiebeveiliging u meer tijd zal kosten of u tijd zal opleveren? Waarom?
Het kost tijd van mij en de ICT-leverancier. Ik ga er wel vanuit dat dit bijhouden van mijn praktijk tijd oplevert t.a.v. de problemen die kunnen optreden en de andere vertragende factoren zoals tragere systemen gedurende de loop van de tijd. Ik kan dit alleen niet met hele harde cijfers laten zien.
Ik vind wel dat het registreren van informatie een steeds groter deel van de tijd in je dagelijks werk beslaat. De tijd die je daadwerkelijk met de patiënt tegenover je spendeert, dat neemt sterk af. Op dit moment maken we daardoor langere werkdagen omdat wij vinden dat deze extra administratieve tijd niet ten koste moet gaan van de patiëntenzorg. Er staat geen juiste vergoeding tegenover. De prijs per consult blijft namelijk hetzelfde terwijl je door de extra administratie minder patiënten kan ontvangen binnen een standaard werkdag.

Vind u dat u voldoende tijd beschikbaar heeft om onderhoud op uw systemen en applicaties uit te voeren?
Ik denk het wel. Maar dat komt ook omdat ik dit veel buiten werktijd doe.

Vind u dat u voldoende tijd beschikbaar hebt om uzelf op de hoogte te houden op het gebied van informatiebeveiliging?
Je hebt hiervoor onder andere de nascholing. Hier komt privacy soms in voor, maar dat is dan wel sporadisch. Vaak gaat het over medisch inhoudelijke dingen.

Zijn er punten waar jullie weleens discussie over hebben als het gaat om informatiebeveiliging? Worden deze opgelost? Denk bijvoorbeeld aan vraagstukken rondom privacy/ patiëntgegevens
Wat ik heel gevaarlijk vind is dat een dossier 100% moet kloppen als deze op LSP wordt aangesloten. Als het niet klopt is dit namelijk veel gevaarlijker dan een afwezig dossier. Hierom heb ik ook geen patiënten geïncludeerd op het LSP. Vragen die ik gesteld heb aan de ICT-leverancier m.b.t. juridische verantwoordelijkheid van gebruik van verkeerde of verkeerd geïnterpreteerde gegevens zijn naar mij nooit beantwoord. Zo lang dat niet duidelijk is ga ik geen patiënten op het LSP aansluiten. Andersom kan het ook. Als patiënten vragen om bij het LSP aangesloten te zijn zal ik eerst het hele dossier controleren (in overleg met de patiënt) om zeker te zijn dat het klopt en medicatie en behandelingen van externe partijen ook voorkomen, wat nu vaak niet zo is maar voor een behandeling zeker relevant is.

Wat we soms ook hebben is dat bijvoorbeeld de vrouw geen Nederlands spreekt maar de man wel. In dat geval vraag je je weleens af of alles goed overkomt. In dat geval vraag je weleens aan de vrouw om alleen te komen en schakel je een vertaler in zodat je zekerder bent dat wat je bespreekt ook zo overkomt.

Zo af en toe krijgen we overzichten van verzekeraars omdat we vergoeding krijgen over ons voorschrijfgedrag. Als je voorkeursmiddelen (van de verzekeraar) voorschrijft en je doet dat op een bepaald percentage van je patiënten krijg je een beloning. Wij krijgen hiervan een overzicht, maar ik vraag mij af waar ze die cijfers vandaan halen. Daarnaast klopte het laatste overzicht ook nog niet, waarop alle huisartsen een correctie kregen. Ik vind het dus een heel onzorgvuldig geheel van hoe met deze cijfers omgegaan wordt. Als je daar vragen over stelt kan niemand eigenlijk antwoord geven. Ook dit geeft geen vertrouwen in hoe gedeelde gegevens gebruikt worden, waardoor ik ook hierom niet graag op het LSP aansluit.

Vind u dat uw praktijk voldoende op de hoogte is van informatiebeveiliging?
Ik word voornamelijk op de hoogte gehouden door wat fanatieke collega's uit de wijk. Echter vind ik wel dat mijn praktijk zelf nog niet voldoende op de hoogte is. We zouden het nog niet zelfstandig kunnen denk ik. De onderwerpen die naar voren kwamen hebben we wel goed kunnen afhandelen.

Vind u dat uw praktijk voldoende beschermd?
Ik denk van wel, we houden het op orde en denken na over wat anderen van ons krijgen, met name bij verzekeraars.

Op welke vlakken ziet u zelf verbetermogelijkheden?
Ik heb aan de ICT-leverancier gevraagd of het mogelijk is om een verzekering tegen ICT-beveiliging of hacken af te sluiten. Ik heb hierop nog geen antwoord maar verwacht dat daarbij ook enkele eisen zitten die onze praktijk nog verder beveiligen.

Daarnaast vragen we de ICT-leverancier soms om advies wat we nog kunnen verbeteren. Als die zegt dat we goed werken zie ik niet zo veel verbeterpunten verder.

Wat zijn volgens u de mogelijke gevolgen als vertrouwelijke informatie op straat komt?
Ik heb hier geen idee van, dat moet ik uitzoeken als het voorkomt. Ik heb het wel gevraagd bij de ICT-leverancier. Hier was nog geen goed beeld van. Mijn angst is om voor de tuchtraad te moeten komen als je niet goed met gegevens omgaat.

Praktijk 5 - Geïnterviewde: huisarts (interviewtijd +- 1,5 uur)
Locatie praktijk: Rijswijk

Welke functie vervult u: Huisarts, Praktijkhouder
Welke functies en werkzaamheden vervullen de andere medewerkers in de praktijk?

- Artsen/praktijkhouder (1x):
    - Behandelen patiënten/ consulten uitvoeren
    - Overleg met assistent(en)
    - Patiëntvragen beantwoorden
    - Visites maken bij patiënten
    - Personeelscontracten opstellen
    - Financiële administratie bijhouden
- Assistent administratief
    - Bijwerken dossiers
    - Invoeren formulieren en post
- Assistenten (2x Geneeskunde studenten):
    - Ondersteuning artsen
    - Patiëntbezoeken inplannen
    - Patiëntinformatie verwerken
    - Patiëntvragen beantwoorden
    - Klaarzetten behandelapparatuur
    - Op orde houden behandelapparatuur en -werktuigen
    - Overleggen met artsen
- Praktijkondersteuner vanuit GGZ (praktijk ondersteunende huisarts)
    - Behandeling psychische klachten van patiënten
- POH-somatisch (praktijk ondersteunende huisarts)
    - Patiënten met diabetisch verzorgen
    - Patiënten verzorgen m.b.t. longfunctie

Tot welke vertrouwelijke informatie heeft u toegang tijdens het uitvoeren van uw functie?
Belangrijkste zijn de dossiers van patiënten. Daarnaast heb ik mappen met inschrijfformulieren. Alle overige patiëntinformatie staat in de HIS-webapplicatie. Daarnaast krijgen we via ZorgTransfer bestanden doorgestuurd. Er staan dus ook bestanden op de lokale computer die geüpload zijn of moeten worden naar de webapplicatie, deze bevatten dossiers van patiënten die naar deze praktijk toekomen.
Daarnaast heb ik toegang tot financiële administratie.

Waar denkt u aan bij Informatiebeveiliging?
Stress dat je niet aan de regels kan voldoen. Technisch kan je eigenlijk niet doen wat je zou moeten doen. Je zou dus eigenlijk je best moeten doen en vinden dat dat goed genoeg is.
Wat de definitie inhoud is zorgen dat mensen niet van andere mensen gevoelige informatie kunnen inzien. Waar dit vaak om gaat, wat aandacht krijgt, is psychische dingen of dingen waar een taboe op rust. Dit zijn de grote dingen.

Houd u zichzelf bezig met Informatiebeveiliging binnen of buiten uw praktijk?
Ja, zowel binnen als buiten. Ik heb dit vooral van vroeger meegekregen. Vooral vervelende momenten zoals het horen van receptinhoud bij apotheek die ik zelf heb meegemaakt wil ik voorkomen bij mijn patiënten.

Worden er in de praktijk audits uitgevoerd op informatiebeveiliging?
Nee.

Heeft de praktijk een accreditering waarbij Informatiebeveiliging getoetst wordt?
Nee.

Kunt u een beschrijving geven van uw werkzaamheden en activiteiten op een reguliere werkdag?
Ik ben voornamelijk met administratieve taken en patiëntcontacten bezig. Daarnaast probeer ik zo veel mogelijk te delegeren en wat ik tegenkom (lean principe) invulling te geven in de organisatie.

Zijn er buiten de reguliere werkzaamheden nu nog activiteiten die u niet genoemd heeft?
Wetenschappelijk onderzoek doe ik ook nog buiten de reguliere werkzaamheden.

Met welke mensen hebt u op een reguliere werkdag te maken?
Mijn patiënten en collega's natuurlijk. Verder met specialisten. Ook met andere bedrijven die nodig zijn rondom de praktijk zoals apotheken in de buurt en schoonmakers.

Welke systemen en applicaties zijn in de praktijk aanwezig?
Ik heb zelf een nieuwe laptop, ook om te kunnen meenemen naar visites en thuiswerk. Ik heb er wel anti-virus en een code opgezet zodat hij niet zomaar gestart kan worden.
Zorgmail filetransfer. Dit gaat met een Vecozo certificaat.
We hebben voor interne bestanden een beveiligde netwerkschijf die zichzelf back-upt. Dat is voor tijdelijke opslag van bestanden die nog in de HIS-applicatie geüpload moeten worden.

Beheert uzelf of een van de praktijkmedewerkers dit systeem zelf?
Alles op de praktijk beheer ik zelf. De HIS-applicatie wordt door de leverancier onderhouden.

Hoe worden deze onderhouden?
Ik houd zelf de updates bij, voor de HIS-applicatie heb ik een contract en krijg van de leverancier soms onderhoudsmeldingen. In dat geval zijn ze 's avonds even niet beschikbaar.
Ik weet dat de systemen van deze HIS-applicatie in ieder geval in twee aparte datacenters staan, verder weet ik er eigenlijk weinig vanaf.

Wordt er regelmatig onderhoud uitgevoerd (back-ups, updates)?
Ik krijg regelmatig meldingen van onderhoud en verstoringen. De onderhoudsmeldingen vind ik zelf dan minder belangrijk, maar vooral de meldingen bij vertragingen en andere verstoringen zou ik graag wat meer krijgen zodat ik daar meer op kan anticiperen en kan zien of mijn eigen data beïnvloed zijn.

Is er contact of een overeenkomst met een leverancier voor onderhoud?
Ja

Is er een systeem/applicatiebeheerder voor deze applicatie?
Ik neem aan dat er een team aan deze applicatie werkt. Betaal er natuurlijk voldoende geld voor.

Is de toegang tot het systeem of applicatie beperkt tot specifieke medewerkers?
Ja, je kan per gebruiker vinkjes aan zetten voor toegang tot delen van de HIS-applicatie.

Hoe zorgt u dat patiëntgegevens tijdens de contactmomenten privé blijven
Ik zorg wel altijd dat de ruimten afgesloten zijn voordat ik gesprekken aanga. Dit zowel met de persoon als per telefoon. Ook mijn collega's vertel ik dat deuren dicht moeten zijn voordat dit soort informatie besproken wordt. Ook bij de assistenten zorg ik dat de gesprekken niet gehoord kunnen worden in de wachtruimte. We hebben bij de Gemeente gevraagd om dikkere muren wat we hebben gekregen.

Hoe zorgt u dat relevante data goed opgeslagen worden?
In het systeem kan je verschillende labels aan informatie geven. Hiermee kan je aangeven hoe belangrijk bepaalde informatie is. Zo zorg je dat belangrijke dingen in ieder geval altijd zichtbaar worden. Verder is het heel belangrijk om alle informatie goed te koppelen. Dan kan het namelijk ook makkelijker teruggevonden worden als er andere klachten spelen.
Ik gebruik wel de ICPC-codes maar vul deze meestal wel aan om zo specifiek mogelijk de problemen te beschrijven. Dit is vooral voor waarnemers erg belangrijk omdat ICPC-codes meestal net niet specifiek genoeg zijn.

Weet u hoe de systemen van opslag beschermd zijn tegen bedreigingen en fouten?
De leverancier maakt van de applicatie back-ups.
Verder zorg ik dat ikzelf en mijn medewerkers op de hoogte zijn hoe ze gegevens goed op kunnen slaan in het systeem zodat iedereen hetzelfde werkt.

Staat Informatiebeveiliging op de agenda bij overleggen (zoals werkoverleggen en met collega's)?
Niet als zodanig. Wat ik wel probeer is dit bespreekbaar te maken. Tevens staat er wel een vast punt voor werkoverdracht van oudere medewerkers naar jongere krachten zodat ook routine kennis en werkmethodes besproken kunnen worden en waar mogelijk verbeterd.

Wordt Informatiebeveiliging buiten de vooraf geplande overleggen besproken?
Ja, alles waar ik of mijn collega's tegenaan lopen bespreken we even met elkaar. Dit hoeft niet per se tijdens een werkoverleg te zijn.

Zo ja, wat wordt er zoal besproken?
Het laatste wat we hebben besproken is het sluiten van de deur van de assistenten bij een telefoongesprek. Dit moet gedaan worden bij telefonische gesprekken maar hij mag daarna weer open omdat het best een kleine ruimte is.

Is er een personeelsbeleid?
Ik heb een aparte map achter slot waar alle contracten met medewerkers en bijvoorbeeld schoonmakers in zitten. Hier zitten o.a. VOG en paspoort in.
Daarnaast houd ik bij wat allemaal nodig is bij nieuwe medewerkers. Zo vul ik aan wat er nog niet is bij elke mutatie.
Wat ik wel expliciet zoek bij nieuwe medewerkers is dat de patiënten hulp op de eerste plaats komt en geld ondergeschikt is.

Worden nieuwe en bestaande medewerkers gescreend?
Volgens mij zijn we dit zelfs verplicht. Dit doe ik wel. De vraag is alleen wel of je dit soort gegevens (paspoort of VOG-afgifte bijvoorbeeld) mag bewaren. Verder vraag ik altijd wel een CV en heb een persoonlijk gesprek met sollicitanten.

Is er voor de medewerkers een functie- en toegangsbeleid?
Toegang wordt per medewerker geregeld. Dit zijn vrij standaard rollen dus makkelijk te beheren door mijzelf.

Worden accounts uitgeschakeld of wachtwoorden gewijzigd bij medewerkers die uit dienst gaan?
Als medewerkers uit dienst gaat wordt het account uitgeschakeld.

Is er een handboek of schriftelijke uitleg van de procedures in de praktijk?
Er is een handboek. Dit is compleet voor alles wat ik al een keer gedaan heb. Per medewerker en andere activiteit vul ik deze aan waar ik verwacht dezelfde instructie nog een keer nodig te hebben. Ik vraag ook aan de andere medewerkers om op te schrijven waar ze tegenaan lopen zodat we samen kunnen kijken wat nog mist of wat beter kan.

Worden moeilijke wachtwoorden afgedwongen?
We hebben voor de praktijk identifiers voor inloggen. Zo heeft elke gebruiker zijn eigen kastje en wachtwoord. Dit lijkt me moeilijk genoeg.
Ik heb nog een UZI pas, echter die gebruik ik niet. Het was een heel gedoe en kostte veel geld om dit te regelen maar dat was te veel om ook het gebruik nog eens te gaan uitzoeken.

Vervallen wachtwoorden periodiek?
Op dit moment niet. De identifier code is wel beperkt houdbaar.

Wachtwoorden vervangen bij uitdienst medewerkers?
Dit is eigenlijk niet nodig, want het hele account staat dicht dus het wachtwoord is ook niet meer te gebruiken.

Heeft iedere gebruiker een eigen gebruikersnaam en wachtwoord?
Ja, iedere medewerker heeft een eigen account.

Bent u op de hoogte van wachtwoorden van andere medewerkers?
Nee.

Zijn andere medewerkers op de hoogte van wachtwoorden van u?
Nee.

Worden er updates uitgevoerd op systemen en applicaties?
Ja

Hoe vaak wordt dit gedaan?
Ik krijg zo af en toe (maandelijks ofzo) mailtjes van onderhoud, dus denk in ieder geval maandelijks.

Is er antivirus bescherming aanwezig op alle werkplekken?
Ja.

Is veilige e-mailcommunicatie mogelijk met artsen en patiënten?
Ja, dit gaat via Zorgmail.
Het gebeurt wel een enkele keer dat patiënten iets willen delen via bijvoorbeeld WhatsApp, dit is voor hun dan vooral praktisch. Bijvoorbeeld als patiënten op vakantie zijn en snel wat willen sturen. Maar richting de patiënt is dit niet de bedoeling.

Wordt gebruik gemaakt van een veilige internetverbinding?
We hebben een dubbele glasvezelverbinding voor eZorg. Dit is zowel voor veilig internet als voor uitval van een van de twee.

Hoe gaat u om met het verwijderen van vertrouwelijke data en datadragers?
Ik heb voor papieren dossiers een grote afgesloten container die 1x per half jaar geleegd wordt. Daar krijg je dan een certificaat van dat de inhoud volledig vernietigd is.
Ik heb nog een laptop thuisliggen die niet meer gebruikt wordt. Verder heb ik harde schijven geprobeerd zo goed mogelijk kapot te maken voordat ik ze wegdeed. Dat was nog wel een behoorlijke klus.

Is er beleid voor aanschaf van nieuwe systemen of applicaties?
Nee, ik let vooral op de eisen van de applicaties en voor de rest moet het systeem gewoon goed reageren op gebruik. Dus ik denk dat ik wel sterkere systemen koop dan nodig. Waar ik wel voor zorg is dat antivirus er altijd op aanwezig is.

Is er een aangewezen persoon verantwoordelijk voor Informatiebeveiliging?
Dit ben ik zelf, omdat ik enige praktijkhouder ben en voor alles in de praktijk verantwoordelijk ben.

Hoe wordt omgegaan met IB-incidenten (Wegvallen verbinding/systeem)
Soms is het systeem erg traag, dan meld ik dit de leverancier ook. Echter is dit dan wel vervelend. Ze proberen dit dan op te lossen, maar dit duurt zo af en toe ook een paar dagen.
We zijn als praktijk wel later opengegaan omdat er geen internet geleverd kon worden. Als het nu zal uitvallen dan kunnen we echter wel open. Bellen werkt alleen niet meer als internet weg valt.

Hoe wordt omgegaan met IB-incidenten (Wegvallen gegevens bij brand/virus/systeemcrash/etc.)
Als gegevens helemaal weg zijn moet ik er wel wat mee, maar wat zou ik op dit moment niet weten. Ik zou het in ieder geval even met de collega's bespreken hoe verder te handelen. Ik denk dat het in ieder geval gemeld moet worden als datalek. Hoe verder zal ik dan op dat moment moeten zien.

Inzage door onbevoegden (hack/nieuwsgierige patiënt/etc.)
Ik heb bij de Gemeente gevraagd om dikkere muren omdat gesprekken nog hoorbaar waren. Verder behandel ik nieuwe inzichten.

Hoeveel uren werkt u gemiddeld?
Ongeveer 40 á 50 uren per week.

Tijdsbesteding aan patiëntcontacten (spreekuur, visites, brieven, post invoeren)
Overdag doe ik alle patiëntcontacten. Omdat de praktijk nog niet heel erg groot is past dit prima in de dag. Ik denk dat ik ongeveer 20 uur per week hieraan besteed.

Tijdsbesteding aan niet-patiëntgebonden uren (Denk aan financiële administratie, bestellingen, onderhoud praktijk apparatuur, personeelsbeleid en -overleg, nascholing/overleggen)
Alle taken die niet onder patiëntcontact vallen doe ik tussendoor. Er moeten daarnaast dossiers worden bijgewerkt en contact met de accountants gehouden worden. Ik heb nu ongeveer 20 tot 30 uur per week aan overige werkzaamheden, maar dat is meer omdat ik er zelf voor kies om in dit tempo de dossiers te verwerken. Scholing doe ik in eigen tijd, dit is ook een uitgebouwde hobby geworden.

Zijn er activiteiten die u door de werkdruk niet binnen de reguliere werkweek gedaan krijgt?
Nee, omdat de praktijk nog vrij klein is heb je op dit moment voor alles nog voldoende tijd beschikbaar.
Wat wel vaak blijft liggen zijn vragen van verzekeringen voor informatie over patiënten. Die wil ik altijd goed uitzoeken dus dit moet vaak thuis. Dan moet eerst gekeken worden welke informatie ze nu echt nodig hebben en mogen hebben. De verzekeraar vraagt vaak om alles of meer dan ze mogen. Aangezien je niet bent opgeleid om juridisch alles goed te kunnen beoordelen heb je meestal wel tijd nodig om zo'n aanvraag goed te beoordelen.
Daarnaast los ik fouten in het importeren van de EDI-bestanden op buiten de werktijd. Soms moet er een zinnetje aangepast worden en dan werkt een import wel. Blijkbaar zitten er soms tekens of letters in die het bestand kapot maken. Deze weet ik meestal wel te vinden. Voor de rest moet de import dan handmatig gedaan worden maar dat is maar heel zelden.

Hoe lost u dit op?
Niet van toepassing, alles wat ik buiten werktijd doe heeft gewoon extra tijd nodig.
Als het voorkomt dat er dingen van werk blijven liggen zoals invoeren van administratie dan doe ik dat meestal de volgende dag wel omdat daar voldoende tijd voor is.

Denkt u dat informatiebeveiliging u meer tijd zal kosten of u tijd zal opleveren? Waarom?
Vooral alles wat we doen die de betrouwbaarheid van de gegevens verbeteren levert mij tijd op.

Vind u dat u voldoende tijd beschikbaar heeft om onderhoud op uw systemen en applicaties uit te voeren?
Nee.

Vind u dat u voldoende tijd beschikbaar hebt om uzelf op de hoogte te houden op het gebied van informatiebeveiliging?
Nee. Ik zit er net niet genoeg in om goed te weten hoe te handelen. Zou wel fijn zijn als er hier wat meer specifieke bijscholing over is.

Zijn er punten waar jullie weleens discussie over hebben als het gaat om informatiebeveiliging? Worden deze opgelost? Denk bijvoorbeeld aan vraagstukken rondom privacy/ patiëntgegevens
Wat soms speelt is dat je graag van een van de ouders wil achterhalen of weten of er iets speelt zoals een ernstige ziekte die grote invloed kan hebben op de leefsituatie van jouw patiënt. Dit is soms lastig te beoordelen. Hoe ik hiermee omga: Je moet hier erg mee opletten en proberen na te gaan wat mag en het goede is voor de behandeling. We doen individuele gezondheidszorg en moeten alles goed beoordelen maar ook goede zorg leveren.

In de praktijk komt het soms ook voor dat partner of kind meekomt voor het vertalen van het gesprek. In het geval van een kind wil je soms bepaalde dingen niet bespreken. Ook in het geval van bijvoorbeeld de partner moet je opletten. Dit kan lastig zijn bv. bij abortus. Bij grotere onderwerpen gebruik ik de tolktelefoon hiervoor om elke vorm van verkeerde vertaling of machtsverschil uit te sluiten.
Wat daarnaast nog speelt is dat bij vermeldingen van contact met meldpunt kindermishandeling in het systeem waar uiteindelijk na onderzoek niks aan de hand blijft te zijn dat deze regels wel "makkelijk of automatisch meekomen" bij verwijsbrieven naar de specialist. Daar kunnen mensen wel van schrikken en eigenlijk hoeven specialisten dit niet per se te weten in sommige gevallen. Dat is wel lastig in het huidige systeem want het hoort wel in de gegevens terug te komen omdat het nuttig kan zijn voor de behandeling.

Vind u dat uw praktijk voldoende op de hoogte is van informatiebeveiliging?
Nog niet, dit verbetert wel naarmate we gebeurtenissen met elkaar bespreken.

Vind u dat uw praktijk voldoende beschermd?
Niet helemaal, maar het wordt wel beter.

Op welke vlakken ziet u zelf verbetermogelijkheden?
Ik wil vooral dat dossiers zo kort mogelijk op harde schijf staan en al helemaal niet meer op de computer.

Wat zijn volgens u de mogelijke gevolgen als vertrouwelijke informatie op straat komt?
Ik denk vooral dat er een onderzoek zal komen. Verder zal dit natuurlijk niet goed zijn voor de praktijk.

Bijlage 6 - Resultaten enquête

Er zijn in totaal 79 volledige reacties binnengekomen. Hieronder per vraag de resultaten op de vragen. De dataset is aangeboden aan de Open Universiteit in een aparte bijlage en zullen alléén voor de examencommissie inzichtelijk worden gemaakt. Een beperkte en geanonimiseerde dataset is voor onderzoeksdoeleinden op te vragen bij de onderzoeker (mail: services@bjbakker.nl).

Bij de invulvelden zijn de data "schoongemaakt" zodat functie- en plaatsnamen eenduidig zijn opgeslagen en wiskundige opdrachten erop mogelijk worden.
Voorbeeld bij vraag 3: "Rdam" is herschreven naar "Rotterdam".

Verder zijn de resultaten (behalve vraag 3 en 4) als volgt weergegeven:
- Reacties in aantal en percentage van de gehele dataset (aangeduid als Hele dataset)
- Reacties in aantal en percentage van de dataset "praktijken met NHG-accreditering"
- Reacties in aantal en percentage van de dataset "praktijken zonder NHG-accreditering"

Bij vragen 1 en 3 zijn de beschikbare cijfers opgenomen uit de Landelijke Peiling:
https://www.nivel.nl/sites/default/files/cijfers-uit-de-registratie-van-huisartsen-peiling-jan-2015.pdf

Vraag 1: Wat is de praktijkvorm van uw huisartsenpraktijk?

Antwoordkeuze	Hele dataset	Met NHG	Zonder NHG	Huisartsen in praktijk (landelijk 2015)
Solopraktijk	17 (21,52%)	10 (16,13%)	7 (41,18%)	2072 (22%)
Duopraktijk	21 (26,58%)	14 (22,58%)	7 (41,18%)	3767 (40%)
Groepspraktijk	41 (51,90%)	38 (61,29%)	3 (17,65%)	3673 (39%)

Vraag 2: Welke functie vervult u binnen de praktijk?

Antwoordkeuze	Hele dataset	Met NHG	Zonder NHG
Arts (praktijk houdend)	59 (74,68%)	45 (72,58%)	14 (82,35%)
Arts (niet-praktijk houdend)	13 (16,46%)	10 (16,13%)	3 (17,65%)
Assistent	2 (2,53%)	2 (3,23%)	-
Anders, namelijk:	5 (6,33%)	5 (8,06%)	-

Onder "Anders, namelijk:" werd door alle 5 de respondenten "praktijkmanager" ingevuld.

Vraag 3: Heeft de praktijk een NHG-Praktijkaccreditering?

Antwoordkeuze	Reacties (%)	Reacties (#)
Ja	78,48%	62
Nee	21,52%	17

"Anno 2014 werkt volgens de NPA 55% van alle huisartsen in een praktijk die deelneemt aan de NHG-praktijkaccreditering."
https://www.nivel.nl/sites/default/files/bestanden/Kennissynthese_Toekomstvisie_Huisartsenzor_2022.pdf

Vraag 4: Wat is de vestigingsplaats van de huisartsenpraktijk?

* Steden met meer dan twee reacties zijn hieronder individueel weergegeven. Alle steden met één reactie zijn samengevoegd in “Anders”.

Antwoordkeuze	Reacties (%)	Reacties (#)
Den Haag	30,19%	16
Rijswijk	22,64%	12
Zoetermeer	9,43%	5
Ridderkerk	7,55%	4
Amsterdam	7,55%	4
Utrecht	7,55%	4
Rotterdam	5,66%	3
Almere	5,66%	3
Maassluis	3,77%	2
Anders	49,06%	26

Vraag 5: Hoeveel patiënten heeft de praktijk (ongeveer)?

	Hele dataset	Met NHG	Zonder NHG
Minimale waarde:	1200	1200	1300
Maximale waarde:	15000	15000	10000
Gemiddeld:	4945	5382	3349
Standaardafwijking:	3245	3390	1939

Onderverdeeld in drie groepen:

Antwoordkeuze	Hele dataset	Met NHG	Zonder NHG
1200 t/m 5833	55 (70,51%)	39 (62,90%)	16 (94,12%)
5834 t/m 10417	18 (23,08%)	17(27,42%)	1 (5,88%)
10418 t/m 15000	5 (6,41%)	5 (8,06%)	-

Vraag 6: Hoeveel medewerkers heeft de praktijk?

	Hele dataset	Met NHG	Zonder NHG
Minimale waarde:	2	2	3
Maximale waarde:	50	50	25
Gemiddeld:	12,14	13,56	6,94
Standaardafwijking:	8,77	9,00	5,23

Vraag 7: Hoeveel uren werkt u gemiddeld op een werkdag?

	Hele dataset	Met NHG	Zonder NHG
Minimale waarde:	5	5	9
Maximale waarde:	12	12	11
Gemiddeld:	9,44	9,35	9,74
Standaardafwijking:	1,54	1,70	0,55

Vraag 8: Hoeveel uren hiervan zijn voor patiëntencontacten?

	Hele dataset	Met NHG	Zonder NHG
Minimale waarde:	0	0	4
Maximale waarde:	11	11	9
Gemiddeld:	6,47	6,38	6,79
Standaardafwijking:	2,10	2,29	1,13

Vraag 9: Hoeveel uren hiervan zijn voor overige werkzaamheden voor de praktijk?

	Hele dataset	Met NHG	Zonder NHG
Minimale waarde:	0	0	1
Maximale waarde:	12	12	6
Gemiddeld:	2,77	2,77	2,76
Standaardafwijking:	1,73	1,86	1,16

Vraag 10: Is er binnen de praktijk voldoende tijd beschikbaar voor:

Hele dataset	**Altijd**	**Meestal**	**Soms**	**Bijna nooit**	**Nooit**	**n.v.t.**
Patiënten	15 (18,99%)	55 (69,62%)	7 (8,86%)	2 (2,53%)	-	-
Administratieve taken	7 (8,86%)	35 (44,30%)	27 (34,18%)	8 (10,13%)	2 (2,53%)	-
Onderhoud van informatiesystemen	5 (6,33%)	25 (31,65%)	23 (29,11%)	13 (16,46%)	3 (3,80%)	10 (12,66%)

Met NHG	**Altijd**	**Meestal**	**Soms**	**Bijna nooit**	**Nooit**	**n.v.t.**
Patiënten	13 (20,97%)	41 (66,13%)	6 (9,86%)	2 (3,23%)	-	-
Administratieve taken	7 (11,29%)	24 (38,71%)	23 (37,10%)	6 (9,68%)	2 (3,23%)	-
Onderhoud van informatiesystemen	2 (3,23%)	22 (35,48%)	17 (27,42%)	12 (19,35%)	1 (1,61%)	8 (12,90%)

Zonder NHG	**Altijd**	**Meestal**	**Soms**	**Bijna nooit**	**Nooit**	**n.v.t.**
Patiënten	2 (11,76%)	14 (82,35%)	1 (5,88%)	-	-	-
Administratieve taken	-	11 (64,71%)	4 (23,53%)	2 (11,76%)	-	-
Onderhoud van informatiesystemen	3 (17,65%)	3 (17,65%)	6 (35,29%)	1 (5,88%)	2 (11,76%)	2 (11,76%)

Vraag 11: Heeft Informatiebeveiliging een vaste plek op de agenda bij overleggen?

Antwoordkeuze	**Hele dataset**	**Met NHG**	**Zonder NHG**
Ja	21 (26,58%)	19 (30,65%)	2 (11,76%)
Nee	58 (73,42%)	43 (69,35%)	15 (88,24%)

Vraag 12: Is er een aangewezen medewerker verantwoordelijk voor informatiebeveiliging binnen de organisatie?

Antwoordkeuze	Hele dataset	Met NHG	Zonder NHG
Ja	41 (51,90%)	37 (59,68%)	4 (23,53%)
Nee	27 (34,18%)	16 (25,81%)	11 (64,71%)
Weet niet	11 (13,92%)	9 (14,52%)	2 (11,76%)

Vraag 13: Hoe wordt omgegaan met informatiebeveiligingsincidenten?

Antwoordkeuze	Hele dataset	Met NHG	Zonder NHG
Er is beleid	36 (45,57%)	33 (53,23%)	3 (17,65%)
Er is geen beleid	34 (43,04%)	23 (37,10%)	11 (64,71%)
Weet niet	9 (11,39%)	6 (9,69%)	3 (17,65%)

Vraag 14: Wordt informatiebeveiliging meegenomen in de beslissing voor aanschaf van nieuwe applicaties en medische apparatuur?

Antwoordkeuze	Hele dataset	Met NHG	Zonder NHG
Ja	62 (78,48%)	50 (80,65%)	12 (70,59%)
Nee	10 (12,66%)	6 (9,68%)	4 (23,53%)
Weet niet	7 (8,86%)	6 (9,68%)	1 (5,88%)

Vraag 15: Wie voorziet de HIS-applicatie van uw praktijk van (beveiligings)updates?

Antwoordkeuze	Hele dataset	Met NHG	Zonder NHG
Ikzelf	4 (5,06%)	2 (3,23%)	2 (11,76%)
Andere praktijkmedewerker	4 (5,06%)	4 (6,45%)	-
Ingehuurde (IT-)partij	51 (64,56%)	40 (64,52%)	11 (64,71%)
Niemand	-	-	-
Weet niet	1 (1,27%)	1 (1,61%)	-
Anders, namelijk	19 (24,05%)	15 (24,19%)	4 (23,53%)

Onder “anders, namelijk:” werden de volgende antwoorden gegeven:

- HIS-leverancier: 12x
- Andere interne afdeling: 4x
- Huisarts uit andere praktijk: 1x
- Combinatie van “ikzelf” en IT-partij: 2x

Vraag 16: Hoe vaak worden er updates op de HIS-applicatie geïnstalleerd?

Antwoordkeuze	Hele dataset	Met NHG	Zonder NHG
Dagelijks	3 (3,80%)	2 (3,23%)	1 (5,88%)
Wekelijks	4 (5,06%)	3 (4,84%)	1 (5,88%)
Maandelijks	14 (17,72%)	11 (17,74%)	3 (17,65%)
Jaarlijks	2 (2,53%)	2 (3,23%)	-
Nooit	-	-	-
Automatisch (via IT-partij)	34 (43,04%)	25 (40,32%)	9 (52,94%)
Weet niet	22 (27,85%)	19 (30,65%)	3 (41,18%)

Vraag 17: Hoe vaak wordt er een back-up gemaakt van de HIS-applicatie?

Antwoordkeuze	Hele dataset	Met NHG	Zonder NHG
Dagelijks	26 (32,91%)	19 (30,65%)	7 (41,18%)
Wekelijks	-	-	-
Maandelijks	1 (1,27%)	-	1 (5,88%)
Jaarlijks	-	-	-
Nooit	1 (1,27%)	1 (0,00%)	-
Automatisch (via IT-partij)	33 (41,77%)	26 (41,94%)	7 (41,18%)
Weet niet	18 (22,78%)	16 (25,81%)	2 (11,76%)

Vraag 18: Hoe vaak worden er updates op de werkplekken geïnstalleerd?

Antwoordkeuze	Hele dataset	Met NHG	Zonder NHG
Dagelijks	1 (1,27%)	1 (1,61%)	-
Wekelijks	4 (5,06%)	2 (3,23%)	2 (11,76%)
Maandelijks	2 (2,53%)	-	2 (11,76%)
Jaarlijks	4 (5,06%)	4 (6,45%)	-
Nooit	4 (5,06%)	3 (4,84%)	1 (5,88%)
Automatisch (via IT-partij)	37 (46,84%)	28 (45,16%)	9 (52,94%)
Weet niet	27 (34,18%)	24 (38,71%)	3 (17,65%)

Vraag 19: Is er een overeenkomst met de leverancier van de HIS-applicatie voor onderhoud?

Antwoordkeuze	Hele dataset	Met NHG	Zonder NHG
Ja	69 (87,34%)	54 (87,10%)	15 (88,24%)
Nee	3 (3,80%)	3 (4,84%)	-
Weet niet	7 (8,86%)	5 (8,06%)	2 (11,76%)

Vraag 20: Op hoeveel werkplekken is antivirus bescherming aanwezig in de praktijk?

Antwoordkeuze	Hele dataset	Met NHG	Zonder NHG
Op geen enkele	1 (1,27%)	1 (1,61%)	-
Op een deel	1 (1,27%)	1 (1,61%)	-
Op alle	68 (86,08%)	54 (87,10%)	14 (82,35%)
Weet niet	9 (11,39%)	6 (9,68%)	3 (17,65%)

Vraag 21: Wordt er gebruik gemaakt van veilige e-mailcommunicatie voor overleg van patiëntinformatie met collegae?

Antwoordkeuze	Hele dataset	Met NHG	Zonder NHG
Altijd	41 (51,90%)	31 (50,00%)	10 (58,82%)
Meestal	29 (36,71%)	23 (37,10%)	6 (35,29%)
Soms	4 (5,06%)	3 (4,84%)	1 (5,88%)
Bijna nooit	3 (3,80%)	3 (4,84%)	-
Nooit	2 (2,53%)	2 (3,23%)	-

Vraag 22: Wordt bij telefonisch overleg de identiteit van de andere partij (bv. specialist) geverifieerd voordat patiëntinformatie gedeeld wordt?

Antwoordkeuze	Hele dataset	Met NHG	Zonder NHG
Altijd	20 (25,32%)	18 (29,03%)	2 (11,76%)
Meestal	22 (27,85%)	19 (30,65%)	3 (17,65%)
Soms	10 (12,66%)	10 (16,13%)	-
Bijna nooit	17 (21,52%)	10 (16,13%)	7 (41,18%)
Nooit	10 (12,66%)	5 (8,06%)	5 (29,41%)

Vraag 23: Wie mag er bij systemen of applicaties met patiëntgegevens? (Meerdere antwoorden mogelijk)

Antwoordkeuze	Hele dataset	Met NHG	Zonder NHG
(IT-)leverancier	46 (58,23%)	35 (56,45%)	11 (64,71%)
Specifieke medewerkers op grond van functie	74 (93,67%)	58 (93,55%)	16 (94,12%)
Specifieke medewerkers zonder grond van functie	2 (2,53%)	2 (3,23%)	-
Weet niet	2 (2,53%)	1 (1,61%)	1 (5,88%)
Anders, namelijk	-	-	-

Vraag 24: Hoe wordt uw computer vergrendeld als u de ruimte verlaat?

Antwoordkeuze	Hele dataset	Met NHG	Zonder NHG
Automatisch	34 (43,04%)	26 (41,94%)	8 (47,06%)
Zelf	33 (41,77%)	30 (48,39%)	3 (17,65%)
Niet	12 (15,19%)	6 (9,68%)	6 (35,29%)

Vraag 25: Worden wachtwoorden gedeeld met andere medewerkers?

Antwoordkeuze	Hele dataset	Met NHG	Zonder NHG
Ja, iedereen kent elkaars wachtwoord	3 (3,80%)	2 (3,23%)	1 (5,88%)
Ja, er is één wachtwoord voor iedereen	1 (1,27%)	-	1 (5,88%
Ja, gebeurt vaak	8 (10,13%)	6 (9,68%)	2 (11,76%)
Ja, gebeurt soms	19 (24,05%)	16 (25,81%)	3 (17,65%)
Nee	48 (60,76%)	38 (61,29%)	10 (58,82%)
Weet niet	-	-	-

Vraag 26: Wanneer wordt de toegang tot systemen uitgeschakeld als een medewerker uit dienst gaat?

Antwoordkeuze	Hele dataset	Met NHG	Zonder NHG
Direct	31 (39,24%)	22 (35,48%)	9 (52,94%)
Binnen een vastgestelde tijd	20 (25,32%)	18 (29,03%)	2 (11,76%)
Op individuele basis	12 (15,19%)	9 (14,52%)	3 (17,65%)
Nooit	1 (1,27%)	1 (1,61%)	-
Weet niet	15 (18,99%)	12 (19,35%)	3 (17,65%)

Vraag 27: Wanneer worden algemeen bekende wachtwoorden vervangen als een medewerker de organisatie verlaat?

Antwoordkeuze	Hele dataset	Met NHG	Zonder NHG
Direct	16 (20,25%)	14 (22,58%)	2 (11,76%)
Binnen een vastgestelde tijd	15 (18,99%)	10 (16,13%)	5 (29,41%)
Op individuele basis	13 (16,46%)	10 (16,13%)	3 (17,65%)
Nooit	17 (21,52%)	14 (22,58%)	3 (17,65%)
Weet niet	18 (22,78%)	14 (22,58%)	4 (23,53%)

Vraag 28: Welke controles worden gedaan bij het aanstellen van nieuwe medewerkers? (Meerdere antwoorden mogelijk)

Antwoordkeuze	Hele dataset	Met NHG	Zonder NHG
Inschrijving in het BIG-Register	61 (77,22%)	48 (77,42%)	13 (76,47%)
Controle van de cv	51 (64,56%)	40 (64,52%)	11 (64,71%)
Vereiste VOG-verklaring	19 (24,05%)	16 (25,81%)	3 (17,65%)
Controle van diploma(s)	56 (70,89%)	45 (72,58%)	11 (64,71%)
Nabellen van referenties	48 (60,76%)	38 (61,29%)	10 (58,82%)
Anders, namelijk	4 (5,06%)	3 (4,84%)	1 (5,88%)

Onder “anders, namelijk:” werden de volgende antwoorden gegeven:

- Weet niet: 3x
- Nog nooit nieuwe medewerkers aangenomen: 1x

Vraag 29: Word patiëntinformatie op papier versnipperd of via een gecertificeerd bedrijf vernietigd?

Antwoordkeuze	Hele dataset	Met NHG	Zonder NHG
Ja	78 (98,73%)	61 (98,39%)	17 (100,00%)
Nee	1 (1,27%)	1 (1,61%)	-
Weet niet	-	-	-

Vraag 30: Hoe wordt met afgedankte USB-schijven en -sticks omgegaan?

Antwoordkeuze	Hele dataset	Met NHG	Zonder NHG
Vernietigd door gecertificeerd bedrijf	6 (7,59%)	5 (8,06%)	1 (5,88%)
Leeggehaald en in prullenbak	6 (7,59%)	3 (4,84%)	3 (17,65%)
Direct in prullenbak	1 (1,27%)	1 (1,61%)	-
Zelf fysiek vernietigd	12 (15,19%)	9 (14,52%)	3 (17,65%)
Schijven/sticks worden niet gebruikt	36 (45,57%)	27 (43,55%)	9 (52,94%)
Weet niet	12 (15,19%)	11 (17,74%)	1 (5,88%)
Anders, namelijk	6 (7,59%)	6 (9,68%)	-

Onder “anders, namelijk:” werden de volgende antwoorden gegeven:
- Via IT-verantwoordelijke: 5x
- Nog nooit nodig geweest: 1x

Vraag 31: Welke maatregelen zijn genomen om binnen de praktijk gesprekken met patiënten privé te houden? (Meerdere antwoorden mogelijk)

Antwoordkeuze	Hele dataset	Met NHG	Zonder NHG
Deuren van spreek- en behandelkamers zijn altijd gesloten	76 (96,20%)	60 (96,77%)	16 (94,12%)
De wachtruimte is een gesloten ruimte	28 (35,44%)	24 (38,71%)	4 (23,53%)
De wachtruimte heeft muziek om gesprekken te maskeren	28 (35,44%)	21 (33,87%)	7 (41,18%)
Muren zijn voorzien van extra geluidsisolatie	38 (48,10%)	30 (48,39%)	8 (47,06%)
Assistentenbalie is afgeschermd met deur of ruit	46 (58,23%)	40 (64,52%)	6 (35,29%)
Er zijn geen maatregelen getroffen	-	-	-
Weet niet	-	-	-
Anders, namelijk	3 (3,80%)	2 (3,23%)	1 (5,88%)

Onder “anders, namelijk:” werden de volgende antwoorden gegeven:
- Geluidisolatie in deuren: 1x
- Valdorpels: 1x
- Aparte ruimte voor telefoonverkeer/ afspraken maken, etc: 1x

Vraag 32: Vindt u dat uw praktijk voldoende op de hoogte is van informatiebeveiliging?

Antwoordkeuze	Hele dataset	Met NHG	Zonder NHG
Ja	50 (63,29%)	42 (67,74%)	8 (47,06%)
Nee	29 (36,71%)	20 (32,26%)	9 (42,94%)

Vraag 33: Is het toepassen van informatiebeveiliging (IB) binnen de praktijk de investering waard?

Antwoordkeuze	Hele dataset	Met NHG	Zonder NHG
Nee, IB kost te veel tijd	2 (2,53%)	2 (3,23%)	-
Nee, IB kost te veel geld	1 (1,27%)	-	1 (5,88%)
Nee, IB kost te veel tijd én geld	14 (17,72%)	11 (17,74%)	3 (17,65%)
Ja, IB levert geld op	2 (2,53%)	1 (1,61%)	1 (5,88%)
Ja, IB bespaart geld	3 (3,80%)	2 (3,23%)	1 (5,88%)
Ja, IB levert tijd op én bespaart geld	3 (3,80%)	3 (4,84%)	-
Weet niet	23 (29,11%)	15 (24,19%)	8 (47,06%)
Anders, namelijk	31 (39,45%)	28 (45,16%)	3 (17,65%)

Onder “anders, namelijk:” werden de volgende antwoorden gegeven:
- Het is belangrijker dan geld/tijd: 21x
- Het moet (wettelijk): 6x
- Ik wil geen datalekken: 1x
- Kost geld als het niet op orde is: 2x
- Betaald/geregeld door derden: 1x

Vraag 34: Hoe belangrijk is informatiebeveiliging voor uw praktijk?

Antwoordkeuze	Hele dataset	Met NHG	Zonder NHG
Heel belangrijk	53 (67,09%)	42 (67,74%)	11 (64,71%)
Enigszins belangrijk	20 (25,32%)	16 (25,81%)	4 (23,53%)
Niet erg belangrijk	6 (7,59%)	4 (6,45%)	2 (11,76%)
Onbelangrijk	-	-	-

Vraag 35: Hoe groot zijn volgens u de gevolgen voor de praktijk als vertrouwelijke informatie op straat komt?

Antwoordkeuze	Hele dataset	Met NHG	Zonder NHG
Groot	16 (20,25%)	10 (16,13%)	6 (35,29%)
Middel	45 (56,96%)	36 (58,06%)	9 (52,94%)
Klein	14 (17,72%)	12 (19,35%)	2 (11,76%)
Anders, namelijk	4 (5,06%)	4 (6,45%)	-

Onder “anders, namelijk:” werden de volgende antwoorden gegeven:
- Weet niet: 3x
- Hangt van de situatie af: 1x

Vraag 36: Gaat u naar aanleiding van deze enquête aanpassingen maken in uw praktijk (op het gebied van informatiebeveiliging)?

Antwoordkeuze	Hele dataset	Met NHG	Zonder NHG
Ja	21 (26,58%)	13 (20,97%)	8 (47,06%)
Nee	58 (73,42%)	49 (79,03%)	9 (52,94%)

Bijlage 7 - Resultaten enquête – Analyse SPSS T-test

In deze bijlage staat een statistische analyse opgenomen van de resultaten van de enquête. Hierbij is een Independent Sample T-test uitgevoerd met hypothese H0 “Er is geen verschil tussen de niet- en wel geaccrediteerde praktijken op basis van de gestelde vraag” en HA “Er is verschil tussen de niet- en wel geaccrediteerde praktijken op basis van de gestelde vraag”.

In de tabel hieronder worden de statistieken van deze twee groepen (groep 1 wel- en groep 2 niet-geaccrediteerde praktijken) weergegeven. Dit geeft details over de verdeling van deze groepen.

Group Statistics

	accreditatie	N	Mean	Std. Deviation	Std. Error Mean
Vraag 5	Ja	62	5382,4032	3418,08376	434,09707
	Nee	17	3348,8235	1998,90871	484,80657
Vraag 6	Ja	62	13,5645	9,07459	1,15247
	Nee	17	6,9412	5,39062	1,30742
Vraag 7	Ja	62	9,3548	1,71872	,21828
	Nee	17	9,7353	,56230	,13638
Vraag 8	Ja	62	6,3790	2,30943	,29330
	Nee	17	6,7941	1,15999	,28134
Vraag 9	Ja	62	2,7661	1,87021	,23752
	Nee	17	2,7647	1,20049	,29116
Vraag 10 (patiënten)	Ja	62	1,9516	,66351	,08427
	Nee	17	1,9412	,42875	,10399
Vraag 10 (administratieve werkzaamheden)	Ja	62	2,5484	,93524	,11878
	Nee	17	2,4706	,71743	,17400
Vraag 10 (onderhoud van informatiesystemen)	Ja	62	3,1935	1,37708	,17489
	Nee	17	3,1176	1,61564	,39185
Vraag 11	Ja	62	1,6935	,46478	,05903
	Nee	17	1,8824	,33211	,08055
Vraag 12	Ja	62	1,5484	,73946	,09391
	Nee	17	1,8824	,60025	,14558
Vraag 13	Ja	62	1,5645	,66827	,08487
	Nee	17	2,0000	,61237	,14852
Vraag 14	Ja	62	1,2903	,63729	,08094
	Nee	17	1,3529	,60634	,14706
Vraag 15	Ja	62	3,6290	1,43988	,18286
	Nee	17	3,4706	1,58578	,38461
Vraag 16	Ja	62	5,3548	1,80252	,22892
	Nee	17	5,1176	1,90008	,46084
Vraag 17	Ja	62	4,7097	2,52455	,32062
	Nee	17	3,8824	2,61922	,63525
Vraag 18	Ja	62	6,0000	1,28037	,16261
	Nee	17	5,2941	1,68689	,40913
Vraag 19	Ja	62	1,2097	,57651	,07322
	Nee	17	1,2353	,66421	,16109
Vraag 20	Ja	62	3,0484	,42184	,05357
	Nee	17	3,1765	,39295	,09531
Vraag 21	Ja	62	1,7419	,99070	,12582
	Nee	17	1,4706	,62426	,15141
Vraag 22	Ja	62	2,4355	1,28829	,16361
	Nee	17	3,5882	1,41681	,34363
Vraag 24	Ja	62	1,6774	,64717	,08219
	Nee	17	1,8824	,92752	,22496
Vraag 25	Ja	62	4,4194	,91523	,11623
	Nee	17	4,1765	1,23669	,29994
Vraag 26	Ja	62	2,4032	1,47615	,18747
	Nee	17	2,1765	1,55062	,37608
Vraag 27	Ja	62	3,0645	1,49174	,18945
	Nee	17	3,1176	1,40900	,34173
Vraag 29	Ja	62	1,0161	,12700	,01613
	Nee	17	1,0000	,00000	,00000
Vraag 30	Ja	62	4,8871	1,68994	,21462
	Nee	17	4,2353	1,60193	,38852
Vraag 32	Ja	62	1,3226	,47128	,05985

	Nee	17	1,5294	,51450	,12478
Vraag 33	Ja	62	7,2742	1,43914	,18277
	Nee	17	6,7647	1,64048	,39787
Vraag 34	Ja	62	1,3871	,61016	,07749
	Nee	17	1,4706	,71743	,17400
Vraag 35	Ja	62	2,2097	,79211	,10060
	Nee	17	1,7647	,66421	,16109
Vraag 36	Ja	62	1,7903	,41040	,05212
	Nee	17	1,5294	,51450	,12478
Aantal “Weet niet” antwoorden	Ja	62	2,3548	2,58683	,32853
	Nee	17	2,0588	2,88250	,69911

Vervolgens wordt hieronder de uitkomst voor de Independent Samples T-test weergegeven en in twee stappen beoordeeld.

In de eerste stap wordt naar de significantie gekeken van de “Levene's Test for Equality of Variances”. Indien deze sig kleiner of gelijk is dan 0,05 bestaat er zeer waarschijnlijk gelijkheid in variantie en zal “equal variances assumed” worden beoordeeld, anders zal “equal variances not assumed” worden beoordeeld.

In stap twee zal Sig. (2-tailed) worden beoordeeld op hetzelfde significantieniveau (95%) voor de aangenomen variantie. Hierbij vertelt de uitkomst of hypothese H0 moet worden aangenomen (> 0,05 = ontoereikende significantie) of HA (<0,06 = significant resultaat) moet worden aangenomen.

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Vraag 5	Equal variances assumed	8,178	,005	2,339	77	,022	2033,57970	869,46023	302,26319	3764,89620
	Equal variances not assumed			3,125	44,447	,003	2033,57970	650,75163	722,44822	3344,71118
Vraag 6	Equal variances assumed	4,997	,028	2,866	77	,005	6,62334	2,31133	2,02089	11,22579
	Equal variances not assumed			3,800	43,617	,000	6,62334	1,74285	3,10998	10,13670
Vraag 7	Equal variances assumed	6,944	,010	-,896	77	,373	-,38046	,42465	-1,22604	,46513
	Equal variances not assumed			-1,478	74,587	,144	-,38046	,25738	-,89323	,13232
Vraag 8	Equal variances assumed	2,573	,113	-,714	77	,477	-,41509	,58108	-1,57215	,74198
	Equal variances not assumed			-1,021	53,196	,312	-,41509	,40642	-1,23019	,40002
Vraag 9	Equal variances assumed	2,274	,136	,003	77	,998	,00142	,47972	-,95382	,95667
	Equal variances not assumed			,004	39,762	,997	,00142	,37575	-,75814	,76099
Vraag 10 (patiënten)	Equal variances assumed	1,698	,196	,061	77	,951	,01044	,17030	-,32868	,34956
	Equal variances not assumed			,078	39,451	,938	,01044	,13384	-,26019	,28106
Vraag 10 (administratieve werkzaamheden)	Equal variances assumed	1,547	,217	,318	77	,752	,07780	,24485	-,40976	,56536
	Equal variances not assumed			,369	32,532	,714	,07780	,21068	-,35106	,50666
Vraag 10 (onderhoud van informatiesystemen)	Equal variances assumed	,302	,584	,194	77	,847	,07590	,39148	-,70363	,85544
	Equal variances not assumed			,177	22,772	,861	,07590	,42911	-,81227	,96407
Vraag 11	Equal variances assumed	16,159	,000	-1,566	77	,122	-,18880	,12060	-,42895	,05134
	Equal variances not assumed			-1,891	35,141	,067	-,18880	,09986	-,39150	,01389
Vraag 12	Equal variances assumed	6,111	,016	-1,711	77	,091	-,33397	,19514	-,72254	,05461
	Equal variances not assumed			-1,928	30,693	,063	-,33397	,17324	-,68744	,01951
Vraag 13	Equal variances assumed	7,234	,009	-2,421	77	,018	-,43548	,17988	-,79368	-,07729
	Equal variances not assumed			-2,546	27,389	,017	-,43548	,17106	-,78624	-,08473
Vraag 14	Equal variances assumed	,072	,789	-,362	77	,718	-,06262	,17275	-,40660	,28136

	Equal variances not assumed			-,373	26,522	,712	-,06262	,16786	-,40733	,28209
Vraag 15	Equal variances assumed	,000	,996	,393	77	,695	,15844	,40283	-,64369	,96058
	Equal variances not assumed			,372	23,733	,713	,15844	,42587	-,72103	1,03791
Vraag 16	Equal variances assumed	,074	,786	,475	77	,636	,23719	,49915	-,75675	1,23113
	Equal variances not assumed			,461	24,480	,649	,23719	,51456	-,82371	1,29810
Vraag 17	Equal variances assumed	,579	,449	1,188	77	,239	,82732	,69662	-,55983	2,21448
	Equal variances not assumed			1,163	24,768	,256	,82732	,71158	-,63889	2,29354
Vraag 18	Equal variances assumed	4,392	,039	1,875	77	,065	,70588	,37638	-,04358	1,45535
	Equal variances not assumed			1,603	21,315	,124	,70588	,44026	-,20887	1,62063
Vraag 19	Equal variances assumed	,159	,691	-,157	77	,876	-,02562	,16311	-,35042	,29919
	Equal variances not assumed			-,145	23,035	,886	-,02562	,17695	-,39164	,34041
Vraag 20	Equal variances assumed	1,190	,279	-1,125	77	,264	-,12808	,11389	-,35487	,09870
	Equal variances not assumed			-1,172	27,002	,252	-,12808	,10933	-,35241	,09624
Vraag 21	Equal variances assumed	1,361	,247	1,070	77	,288	,27135	,25367	-,23377	,77647
	Equal variances not assumed			1,378	40,644	,176	,27135	,19686	-,12633	,66902
Vraag 22	Equal variances assumed	,140	,709	-3,199	77	,002	-1,15275	,36030	-1,87019	-,43531
	Equal variances not assumed			-3,029	23,757	,006	-1,15275	,38059	-1,93868	-,36683
Vraag 24	Equal variances assumed	9,330	,003	-1,048	77	,298	-,20493	,19562	-,59447	,18460
	Equal variances not assumed			-,856	20,461	,402	-,20493	,23950	-,70380	,29394
Vraag 25	Equal variances assumed	2,408	,125	,896	77	,373	,24288	,27122	-,29718	,78294
	Equal variances not assumed			,755	21,042	,459	,24288	,32168	-,42600	,91177
Vraag 26	Equal variances assumed	,068	,795	,555	77	,580	,22676	,40845	-,58658	1,04009
	Equal variances not assumed			,540	24,542	,594	,22676	,42022	-,63951	1,09303

Vraag 27	Equal variances assumed	,261	,611	-,132	77	,896	-,05313	,40380	-,85719	,75093
	Equal variances not assumed			-,136	26,685	,893	-,05313	,39073	-,85530	,74903
Vraag 29	Equal variances assumed	1,123	,293	,521	77	,604	,01613	,03095	-,04549	,07775
	Equal variances not assumed			1,000	61,000	,321	,01613	,01613	-,01612	,04838
Vraag 30	Equal variances assumed	,008	,928	1,424	77	,159	,65180	,45776	-,25971	1,56332
	Equal variances not assumed			1,468	26,605	,154	,65180	,44386	-,25956	1,56317
Vraag 32	Equal variances assumed	2,238	,139	-1,572	77	,120	-,20683	,13157	-,46882	,05516
	Equal variances not assumed			-1,494	23,877	,148	-,20683	,13840	-,49254	,07888
Vraag 33	Equal variances assumed	,343	,560	1,255	77	,213	,50949	,40607	-,29910	1,31808
	Equal variances not assumed			1,164	23,194	,256	,50949	,43785	-,39585	1,41482
Vraag 34	Equal variances assumed	,968	,328	-,481	77	,632	-,08349	,17356	-,42909	,26211
	Equal variances not assumed			-,438	22,741	,665	-,08349	,19048	-,47777	,31079
Vraag 35	Equal variances assumed	,168	,683	2,118	77	,037	,44497	,21007	,02668	,86327
	Equal variances not assumed			2,343	29,726	,026	,44497	,18993	,05694	,83300
Vraag 36	Equal variances assumed	8,221	,005	2,195	77	,031	,26091	,11884	,02426	,49756
	Equal variances not assumed			1,929	21,895	,067	,26091	,13523	-,01962	,54144
Aantal “Weet niet” antwoorden	Equal variances assumed	,001	,978	,408	77	,685	,29602	,72577	-1,14918	1,74121
	Equal variances not assumed			,383	23,546	,705	,29602	,77245	-1,29988	1,89191

Bijlage 8 - Literatuurstudierapport

Informatiebeveiliging in huisartsenpraktijken

(On)mogelijkheden van veilige gegevensuitwisseling tussen huisartsen.

Cursus:	IH060Y Voorbereiding afstuderen
Eerste begeleider:	dr. ir. Hugo Jonker
Tweede begeleider:	dr. ir. Harald Vranken
Student:	B.J. Bakker
Studentennr.:	851415519
Datum:	16-08-2016

Copyright:

“I fear the day when your security requirements kill one of my patient” (Kotz, Fu, Gunter, & Rubin, 2015).

Samenvatting

Doelstelling: In dit artikel wordt een literatuuroverzicht gegeven waarbij de scope ligt op management van informatiebeveiliging bij elektronische gegevensuitwisseling tussen huisartsenpraktijken.
Methode: De zoekresultaten zijn gescand op titel en abstract en gevonden mogelijk relevante artikelen zijn volledig gelezen. Uit de 117 uiteindelijk geselecteerde artikelen is benodigde informatie gehaald en verwerkt in de resultaten.
Bronnen: Er is een zoekstrategie bepaald die gebruik maakt van de OU digitale bibliotheken EBSCHOhost, PubMED, Google Scholar, ScienceDirect en SpringerLink. De zoekresultaten zijn aangevuld met resultaten uit de literatuurlijst en suggesties van huisartsen en ICT-bedrijven waarmee gesproken is gedurende het onderzoek.
Resultaten:
De resultaten zijn in twee onderdelen verwerkt; De metadata, waarbij gekeken zal worden naar wat te zeggen valt over het totaal van gevonden literatuur. De inhoudelijke behandeling van de gevonden literatuur en wat geschreven wordt over management van informatiebeveiliging bij huisartsenpraktijken, wat de voorwaarden zijn voor het goed uitvoeren hiervan en hoe en in welke mate informatiebeveiliging op dit moment wordt beheerst en kan worden verbeterd.
Conclusie:
Gebleken is dat er onvoldoende literatuur beschikbaar is om een goed overzicht te maken wat betreft management van informatiebeveiliging bij huisartsenpraktijken. Vanuit de literatuur is er wel voldoende materiaal beschikbaar om te kunnen stellen dat het waarschijnlijk is dat huisartsenpraktijken niet aan alle eisen kunnen voldoen. Gezien de noodzaak van goede informatiebeveiliging van zorgsystemen, die steeds meer koppelingen hebben met andere systemen, is er zeker meer onderzoek nodig op dit vlak.

Inhoudsopgave

1 Inleiding

Het onderwerp van dit onderzoek “management van informatiebeveiliging bij huisartsenpraktijken” is voortgekomen uit het onderzoeksgebied van de afstudeerbegeleider. Hierbij is aangesloten bij het onderzoeksgebied IT-security.

Er is steeds meer aandacht voor datalekken in de media en de roep naar veiligheid en privacy klinkt sterk onder de burger. Ook de overheid legt hier steeds zichtbaarder nadruk op, zo ook in de Meldplicht Datalekken (College Bescherming Persoonsgegevens, 2015) die op 1 januari 2016 van kracht is geworden. Een van de grootste verzamelingen gevoelige persoonsgegevens, is wellicht ons medisch dossier. Door de Wet op de Geneeskundige Behandelingsovereenkomst (art. 7:454-456 BW) is dossiervorming wettelijk geregeld en bevat een groot deel dan wel niet het complete medisch leven van alle mensen in Nederlandse en is goede informatiebeveiliging van alle toegangspunten tot deze informatie dus erg belangrijk.
Hiertoe is een literatuurstudie gedaan met als scope “management van informatiebeveiliging bij elektronische gegevensuitwisseling tussen huisartsenpraktijken”. In deze scriptie zal de verdere literatuurstudie beschreven worden. De resultaten hiervan zullen uiteengezet worden, waarna een conclusie getrokken zal worden en mogelijke aanbevelingen gedaan zullen worden ten aanzien van de vraagstelling en de antwoorden op deze vragen.

1.1 Achtergrond

Er zijn op het gebied van management van informatiebeveiliging in de zorg veel voorschriften en normen. Zo veel zelfs dat ze niet in een enkele alinea te benoemen zijn. De Stichting IBGZ en NHG bieden op hun sites documenten aan huisartsen aan die een overzicht moeten bieden in het “woud aan regels”. Enkele voorbeelden van normen en regels zijn wel te benoemen. Zo is werken conform de NEN7510 verplicht voor alle zorgverleners, aangezien in de Wet gebruik Burgerservicenummer in de zorg (BWBR0023864) en in de regels voor een Goed Beheerd Zorgsysteem (VZVZ) naar deze norm verwezen wordt. De NEN-normering stelt een kader voor enkele honderden maatregelen die genomen kunnen worden op het gebied van informatiebeveiliging in de zorg. Informatiebeveiliging gaat hier om het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van alle informatie die benodigd is om patiënten verantwoorde zorg te kunnen bieden. Deze informatie wordt tegenwoordig voornamelijk digitaal opgeslagen. Er is hierbij een trend naar digitale gegevensuitwisseling te zien. Dit heeft ook zijn uitwerking op het aantal voorschriften voor het gebruik van digitale uitwissel- en opslagmethoden. Zo zijn er richtlijnen voor gebruik van e-mail (Jongenelen & Ligtvoet, 2015) en geeft de NEN 7510 norm eisen voor de communicatie via een Goed Beheerd Zorgsysteem, afgekort GBZ. Bij invulling van de NEN7510 wordt een managementsysteem ingericht voor het correct implementeren en beheren van informatiebeveiliging in de zorg.

In de zorgsector is de Inspectie voor de Gezondheidszorg het toezichthoudend orgaan. Bij ziekenhuizen is door de Inspectie voor de Gezondheidszorg reeds onderzoek (Inspectie voor de Gezondheidszorg, 2008) gedaan naar de staat van de informatiebeveiliging. Hieruit bleek dat deze in alle gevallen niet aan de gestelde normen voldeed. In andere sectoren van de zorg, zijn dergelijke onderzoeken niet gedaan of niet openbaar beschikbaar, zo blijkt uit een scan van de beschikbare onderzoeken in databanken van Google Scholar, Springer en PubMed en bij navraag bij de IGZ, diverse huisartsenpraktijken, softwareleveranciers van Huisarts Informatie Systemen (HIS) en partijen die de ICT-applicaties en -systemen van zorgverleners beheren. Bij de gesprekken met enkele huisartsen kwam naar voren dat zij wel door de IGZ gecontroleerd worden, maar dat zij geen gestandaardiseerd systeem hebben voor continu verbeteren van de informatiebeveiliging en uitwisseling van best-practices met andere collega’s, maar dit wel wenselijk achten. Ook “eigen koepelorganisaties zoals LHV, NHG en KNMG stellen op het gebied van informatiebeveiliging richtlijnen en handreikingen beschikbaar.

Toch bespreken huisartsen voornamelijk onderling wat ze doen op het gebied van informatiebeveiliging, omdat de beschikbare documentatie weinig inzicht biedt in praktische uitwerkingen". Omdat de NEN7510 normering "ontoegankelijk basismateriaal vormt en moeilijk is aan te geven wat er van belang is in de huisartsenzorg" (Mensink, 2010), is er een praktijkwijzer Informatiebeveiliging in de huisartsenpraktijk (Nederlands Huisartsen Genootschap, 2009b) uitgegeven om binnen huisartsenpraktijken een eerste invulling te geven aan de NEN7510 norm.

Ook met de praktische hulp in de vorm van de praktijkwijzer is het de vraag of huisartsenpraktijken kunnen voldoen aan de gestelde eisen. De impact op de patiënt of grotere groep patiënten bij een verkeerde invulling van informatiebeveiliging binnen huisartsenpraktijken is potentieel groot. Eén huisartsenpraktijk heeft bijvoorbeeld al snel gegevens van duizenden patiënten en een inbreuk op de informatiebeveiliging heeft snel grote gevolgen voor de privacy van grote groepen patiënten. Nu door de digitalisering alle systemen aangesloten zijn (via bijvoorbeeld het Landelijk Schakel Punt) is schaalvergroting toegepast en bestaat een risico voor alle burgers in Nederland, omdat door de koppeling van data deze ook meer waarde heeft gekregen (1 + 1 = 3) (Bonthuis, 2007). Niet meer één enkele huisartsenpraktijk loopt risico bij onvoldoende informatiebeveiliging, maar ook alle aangesloten systemen en gegevens.

1.2 Probleemstelling

Na een vluchtige analyse van het onderzoeksgebied lijkt er een praktijkprobleem te zijn rondom informatiebeveiliging van elektronische gegevensuitwisseling bij huisartsenpraktijken. Het lijkt op dit ogenblik onmogelijk om huisartsenpraktijken te laten voldoen aan de eisen van informatiebeveiliging bij onderlinge gegevensuitwisseling. Daarnaast lijkt er zeer beperkt tot geen onderzoek beschikbaar te zijn die de verschillende managementaspecten van informatiebeveiliging van gegevensuitwisseling bij huisartsenpraktijken bekijkt. We verbreden in dit literatuuronderzoek de scope van de zoektermen naar "management van informatiebeveiliging binnen de gehele zorgsector" omdat de verwachting bestaat dat bij een te specifieke scope onvoldoende literatuur gevonden zal worden. Waar mogelijk zullen de gaten in de literatuur worden aangestipt ten aanzien van de probleemstelling.

De scope van het onderzoek zal zijn; **literatuuronderzoek naar management van informatiebeveiliging bij elektronische gegevensuitwisseling tussen huisartsenpraktijken.**

Probleemstelling; **Is er voldoende managementcapaciteit beschikbaar bij huisartsenpraktijken voor het goed doen van informatiebeveiliging?**
Hypothese; *De vereiste mate van informatiebeveiliging bij huisartsenpraktijken kan niet gehaald worden*

1.2.1 Deelvragen

1. Wat is, volgens de wetenschappelijke literatuur, management van informatiebeveiliging binnen de zorgsector?
2. Wat zegt de literatuur over de eisen die gesteld worden aan informatiebeveiliging binnen de zorg?
3. Wat zegt de literatuur over de eisen aan informatiebeveiliging die gesteld worden bij elektronische gegevensuitwisseling tussen huisartsenpraktijken?
4. Wat zegt de literatuur over de mate en effectiviteit van inrichting van informatiebeveiliging binnen de zorg?
5. Wat zegt de literatuur over de mate waarin de eisen die gesteld worden aan management van informatiebeveiliging bij huisartsenpraktijken gehaald worden?
6. Wat stelt de literatuur voor als aandachts- of verbeterpunten om te voldoen aan de gestelde eisen?

1.3 Leeswijzer

Om de probleemstelling en deelvragen uit paragraaf 1.2 te beantwoorden zal in deze scriptie een literatuurstudie worden uitgevoerd. Aan de hand van de vragen zal in paragraaf 1.5 een zoekstrategie worden neergezet, waarbij de uitvoering van de onderzoeksmethode, gebruikte zoektermen en bronnen in hoofdstuk 2 beschreven zullen worden. Aan de hand van de criteria, zal de literatuur wel of niet worden opgenomen in deze studie. De resultaten zullen worden opgenomen in hoofdstuk 3. In paragraaf 3.1 en 3.2 zullen allereerst de resultaten in termen van statistiek en metadata beschreven worden. Hierbij zal gekeken worden wat te zeggen valt over het totaal van gevonden literatuur. In paragraaf 3.3 komt aan de orde wat de literatuur schrijft over management van informatiebeveiliging in de zorgsector en wat de voorwaarden zijn voor het goed uitvoeren hiervan. Vervolgens kijken we wat de literatuur schrijft over de eisen van management van informatiebeveiliging ten aanzien van elektronische uitwisseling tussen huisartsenpraktijken. Daarnaast is de vraag hoe management van informatiebeveiliging nu wordt uitgevoerd in de praktijk en wat wordt voorgesteld vanuit de literatuur voor verdere verbetering. Er zal na de beantwoording van de vragen in hoofdstuk 4 een conclusie gegeven worden en aanbevelingen gedaan worden op basis van de gevonden resultaten en de antwoorden op de probleemstelling en vragen. Ook zullen in hoofdstuk 5 de beperkingen van dit onderzoek besproken worden.

1.4 Theoretische en praktische relevantie

De bestaande literatuur zal bijdragen aan de beantwoording van de vragen in deze meta-studie door het inzichtelijk maken van de grenzen van de bestaande literatuur en het identificeren van mogelijke gebreken en/of beperkingen aan de bestaande literatuur.
Door het overzichtelijk weergeven van bestaande literatuur en de grenzen hiervan krijgen zorgondernemingen extra houvast op de gestelde eisen aan informatiebeveiliging bij elektronische gegevensuitwisseling tussen huisartsenpraktijken en kan vervolgonderzoek de beperkingen in de literatuur verder verminderen.

1.5 Verantwoording zoekstrategie

Dit onderzoek zal zich richten op de literatuur rondom management van informatiebeveiliging bij huisartsenpraktijken. Daarbij wordt specifiek gekeken naar informatiebeveiliging bij elektronische gegevensuitwisseling tussen huisartsenpraktijken. Hierbij zal een verkennend onderzoek uitgevoerd worden. Zo kan een vertrekpunt bekeken worden van waaruit de mogelijkheden tot verbetering kunnen worden geïdentificeerd.

- Welke gegevens zijn nodig om de vragen te beantwoorden?
- Wat voor soort literatuur zal gebruikt worden?
- Welke criteria bepalen de relevantie van gevonden bronnen?

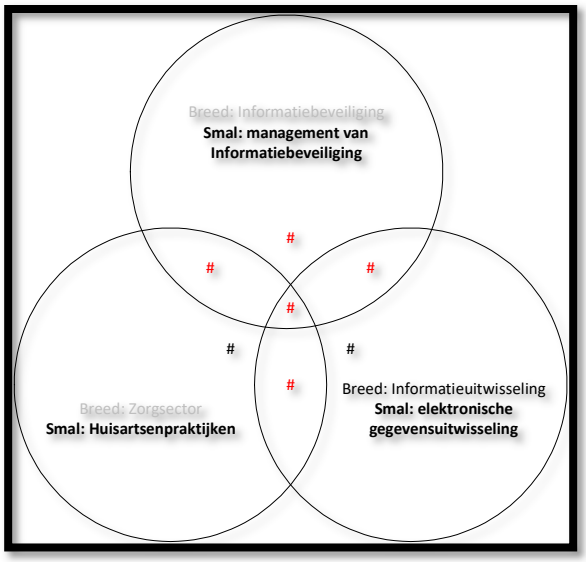
2 Inrichting literatuurstudie (methode)

Er zal in digitale bibliotheken van de OU Bibliotheekcatalogus worden gezocht naar literatuur over informatiebeveiliging bij elektronische gegevensuitwisseling tussen huisartsenpraktijken en literatuur die de vraagstellingen van dit literatuuronderzoek ondersteunen om zo reeds gedaan onderzoek in deze richting te kunnen vinden en aan te kunnen sluiten bij de bestaande literatuur. Deze literatuur zal gezocht worden aan de hand van enkele termen die in dit onderzoeksgebied van toepassing zijn. Hierbij zal zowel in het Nederlands als Engels gezocht worden. Dit omdat Nederlands de standaardtaal van overheidspublicaties, studiemateriaal van de zorgsector en Nederlandse regelgeving en norm-publicaties is. Daarnaast zal Engels gebruikt worden omdat de peer reviewed onderzoeken in deze taal gepubliceerd worden.

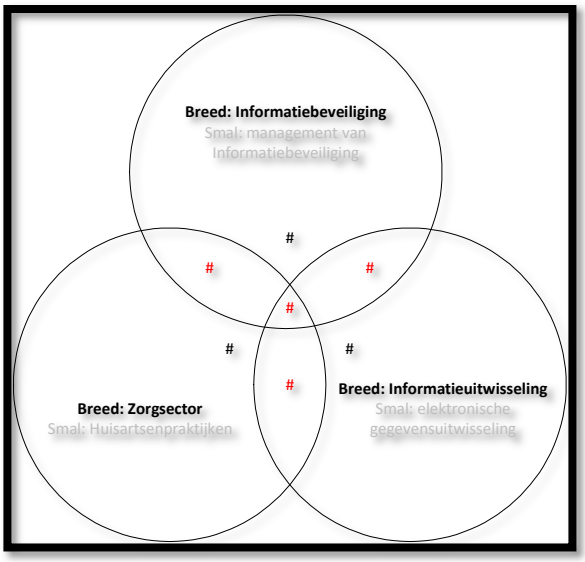
Voor een adequate beantwoording van de gestelde vragen, zullen de zoekresultaten binnen de driehoek van de belangrijkste termen (figuur 1) “management van informatiebeveiliging”, “elektronische gegevensuitwisseling” en “huisartsenpraktijken” worden gezet. Omdat de verwachting is dat weinig tot geen artikelen binnen de driehoek zullen passen, zal een driehoek worden opgesteld waarbinnen de gevonden artikelen worden ingedeeld op basis van drie bredere termen (figuur 2) resp. “informatiebeveiliging”, “informatie-uitwisseling” en “zorgsector”.

In de driehoek worden het aantal (#) gevonden relevante artikelen weergegeven op de positie waar het artikel over gaat, op basis van de inhoud van titel en abstract. Op basis van deze invulling kan gekeken worden of de hoofd- en deelvragen kunnen worden beantwoord of dat er wellicht een gat in de literatuur bestaat. De rode gebieden zullen in de resultaten als relevant worden opgenomen.

Figuur 1: Smalle zoektermen



Figuur 2: Brede zoektermen



De begrippen uit tabel 1 zullen als zoektermen worden gebruikt om relevante artikelen te zoeken. De Nederlandse en Engelse zoektermen zijn hier alfabetisch gesorteerd. Alle zoektermen zullen tussen quotes worden gezet om zo specifiek mogelijk te kunnen zoeken.

Tabel 1: Zoektermen

Engels		**Nederlands**
“eHealth”		“Communicatie in de zorg”
“Electronic Patient record ”		“Elektronisch medisch dossier”
“eScience”		“Elektronisch Patiëntendossier”
“General Practitioner” OR “general practices”		“Elektronische gegevensuitwisseling”
“Healthcare”		“Elektronische informatie-uitwisseling”
“Health Care Organizations”		“Goed Beheerd Zorgsysteem”
“Healthcare Information”		“Huisarts Informatie Systeem”
“Information Exchange”		“Huisartsenpraktijk”
“Information Security”		“ICT in de Zorg”
“Information Technology”		“Informatiebeveiliging”
“National Health Service”		“Landelijk Schakel Punt”
“Private communications Security”		“Patiëntengegevens”
“Secure Private Communications”		“Zorgorganisaties”

Om alle resultaten te kunnen noteren wordt een zoekmatrix gemaakt, waarin de combinaties van zoektermen staan, met lege ruimten om het aantal zoekresultaten te kunnen noteren.
Daarnaast zal worden bijgehouden welk raakvlak er is met de opgezette piramide waar het gaat om de hoofdonderwerpen.

Er zullen, vanwege de beperkte onderzoeksperiode, beperkingen worden opgesteld aan het aantal te doorzoeken zoekresultaten. Van de verkregen zoekresultaten zullen per zoekbron de eerste 20 resultaten bekeken worden, dit komt overeen met de eerste twee resultatenpagina's van zoekmachine Google Scholar. Indien er meer resultaten beschikbaar zijn binnen het zoekresultaat zullen deze niet bekeken worden. Daarnaast zullen de literatuurlijsten van de gevonden publicaties bekeken worden om zo via de sneeuwbalmethode, interessante artikelen te zoeken. Ook zullen voor de hand liggende partijen waaronder overheid, huisartsen en systeembeheerders gevraagd worden naar mogelijk beschikbaar onderzoeksmateriaal. Uit de verkregen literatuur zal een rapportage volgen waaruit de vraagstelling zo goed als mogelijk beantwoord wordt.

Mocht een artikel zich enkel achter een "paywall" bevinden en op geen enkele andere legale manier verkregen kunnen worden (zoals via OU bibliotheek, het aanschrijven van de auteur of elders vindbaar op internet), zal deze niet meegenomen worden in deze literatuurstudie. Bijdrage aan de wetenschappelijke gemeenschap is beperkt door de financiële eis.

Zoektermen zullen bestaan uit de hierboven genoemde begrippen.
Bronnen die hierbij gebruikt zullen worden, zullen bestaan uit diverse literatuurbibliotheken die bij de voorlopige analyse al resultaten hebben opgeleverd. Hierbij zijn alle literatuurbibliotheken van de OU Bibliotheekcatalogus bekeken op een voorlopige set aan relevante artikelen. De volgende literatuurbibliotheken zijn uiteindelijk doorzocht:

- EBSCOhost (alle zoekbronnen) -> alléén Engelse zoektermen
- PubMED -> alléén Engelse zoektermen
- Google Scholar (metazoekmachine, zonder patenten/citaten)-> Engelse/ Nederlandse termen
    a. ScienceDirect (Elsevier) -> alléén Engelse zoektermen
    b. SpringerLink -> alléén Engelse zoektermen

Binnen Google Scholar zijn ook de resultaten uit bronnen van de laatstegenoemde literatuurbibliotheken meegenomen, aangezien de resultaten hiervan overlapten. EBSCOhost en PubMED hadden minder overlap en zijn daarom apart genoemd.
Bij alle zoekmachines, behalve Google Scholar, is alleen naar Engelse zoektermen gezocht omdat deze zoekmachines geen of zeer weinig Nederlandse resultaten heeft geindexeerd.

Ook zal bij het zoeken gebruik gemaakt worden van websites van overheid en organisaties die wetten, regels, normen of andere publicaties hebben over informatiebeveiliging en over de zorgsector. Deze sites zijn niet op één plek te vinden en bijeen gekomen tijdens het maken van de vluchtige analyse en tijdens gesprekken met huisartsen en ICT bedrijven die in de zorg opereren. De gebruikte websites staan hieronder, inclusief de link naar de basissite van de gebruikte publicaties:

- Nictiz.nl, https://www.nictiz.nl/publicaties
- Inspectie voor de Gezondheidszorg (IGZ), http://www.igz.nl/actueel/publicaties/
- Vereniging Zorgaanbieders voor Zorgcommunicatie (VZVZ), https://www.vzvz.nl/
- NEN.nl, https://www.nen.nl/Zoekresultaten.htm?q=informatiebeveiliging
- Overheids websites, https://www.rijksoverheid.nl/documenten
- NHG.org (Nederlands Huisartsen Genootschap), https://www.nhg.org/thema/ict-uw-praktijk
- Zorgvisie (sectie ICT), http://www.zorgvisie.nl/ICT/

Aan de hand van de titel en abstract van de gevonden publicaties zal een eerste selectie gemaakt worden. De artikelen zullen geselecteerd worden als ze ten minste een van de termen uit de eerder gegeven driehoek raken én als ze ingaan op de zorgsector. Alléén relevante resultaten zullen individueel benoemd worden in de resultaten. Het totaal van de zoekresultaten zal benoemd worden bij de resultaten om de reproduceerbaarheid van het onderzoek te bevorderen.
Ook zal een artikel aangemerkt worden als wel- of niet-wetenschappelijk, zo kan een onderscheid gemaakt worden tussen artikelen die iets zeggen over regelgeving of op andere manier een feitelijke toevoeging geven aan de informatievoorziening en peer-reviewed research.

Mochten er geen of weinig relevante artikelen gevonden worden bij een deelvraag, om deze goed te kunnen beantwoorden, dan zal dit gat in de literatuur bij de conclusie aangegeven worden.

Zodra een of meerdere hoofd- of deelvragen beantwoordt kunnen worden via de hierboven genoemde zoekcriteria, dan zal dit gedaan worden in het hoofdstuk Resultaten en zal de beantwoording van deze vraag of vragen waar mogelijk van kritiek en aanvullingen worden voorzien in de hoofdstukken Discussie en Conclusie.

3 Resultaten

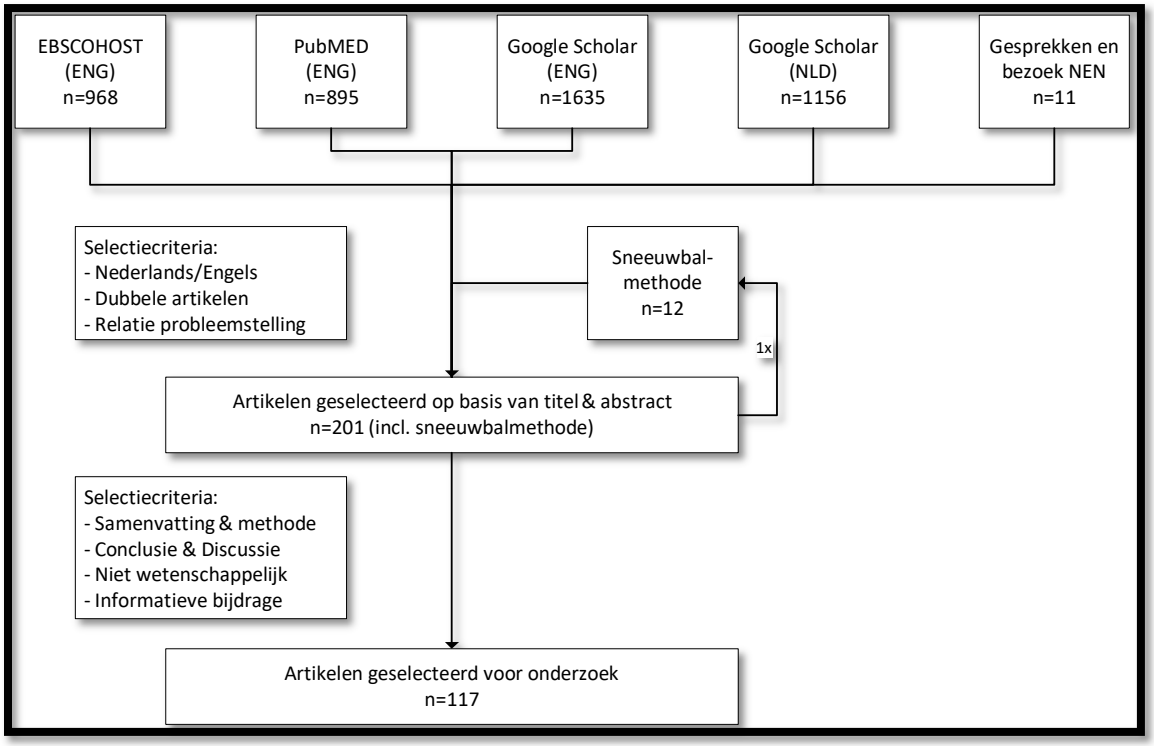
In dit hoofdstuk zullen de resultaten besproken worden van de uitgevoerde literatuurstudie. De volgorde van behandelen zal zo veel als mogelijk gelijk gehouden worden aan de opzet van de zoekmethode. Daarbij zullen eerst globaal het aantal resultaten worden weergegeven en vervolgens zal ingegaan worden op de spreiding van de resultaten over het onderzoeksveld om vervolgens in te gaan op de inhoud van de verkregen zoekresultaten.

Tijdens het zoeken was een “voorkeur” voor zoekresultaten van de zoekmachines terug te zien. Dit kwam doordat de zoekmachine op basis van de eerdere zoekopdrachten voorspellingen ging maken. Dit is ongewenst gedrag omdat zo mogelijk relevante artikelen wegvallen. Dit gedrag van de zoekmachines is uiteindelijk zo veel mogelijk tenietgedaan door tussen zoekresultaten door de browserhistorie ter verwijderen en altijd “privé modus” te gebruiken. De zoekopdrachten zijn uitgevoerd tussen januari 2016 en april 2016.

3.1 Behandeling zoekresultaten in termen van cijfers

Alle resultaten zijn aan de hand van de uitgevoerde zoekopdrachten genoteerd in de zoekmatrix. Daarnaast is bijgehouden welk raakvlak er is met de opgezette piramide waar het gaat om de hoofdonderwerpen. De zoekmethode is verder uitgevoerd zoals in de onderzoekaanpak beschreven. De resultaten van de individuele zoekstappen zijn weergegeven in figuur 3.

Figuur 3: Overzicht van de doorlopen zoekstappen en aantal zoekresultaten



EBSCOHOST

In tabel 2 zijn de gebruikte combinaties van zoekopdrachten (uitgevoerd tussen quotes) weergegeven met op de kruispunten het aantal gevonden resultaten. Groene waarden bevatten relevante artikelen in de eerste 20 resultaten van de betreffende zoekopdracht.

Tabel 2: Zoekmatrix EBSCOHOST

Aantal zoekresultaten bij verschillende zoektermen	<<LEEG>>	"eHealth"	"Electronic Patient record "	"eScience"	"General Practitioner" OR "general practices"	"Healthcare"	"Health Care Organizations"	"Healthcare Information"	"Information Exchange"	"Information Security"	"Information Technology"	"National Health Service"	"Private communications Security"	"Secure Private Communications"
"eHealth"	3385													
"Electronic Patient record "	1110	13												
"eScience"	380	1	3											
"General Practitioner" OR "general pra	32394	36	23	0										
"Healthcare"	803834	975	283	10	971									
"Health Care Organizations"	8108	10	6	0	1	2706								
"Healthcare Information"	5621	53	17	0	0	5621	41							
"Information Exchange"	26854	125	21	2	4	1650	51	159						
"Information Security"	104	4	3	0	1	394	19	75	0					
"Information Technology"	407521	387	133	4	64	13390	364	2158	0	3587				
"National Health Service"	54689	38	76	0	235	12398	85	23	0	21	1206			
"Private communications Security"	83	0	0	0	0	1	0	0	1	1	2	2		
"Secure Private Communications"	3	0	0	0	0	0	0	0	0	0	0	0	0	

Bij de zoekbibliotheek van EBSCOHOST zijn met de Engelse zoekopdrachten in totaal 968 zoekresultaten (ten hoogste 20 resultaten per zoekopdracht) bekeken en beoordeeld op relevantie en type informatie.

Google Scholar

In tabel 3 zijn de gebruikte combinaties van zoekopdrachten (uitgevoerd tussen quotes) weergegeven met op de kruispunten het aantal gevonden resultaten. Groene waarden bevatten relevante artikelen in de eerste 20 resultaten van de betreffende zoekopdracht.

Tabel 3: Zoekresultaatmatrix Google Scholar (Nederlandse zoektermen)

Aantal zoekresultaten bij verschillende zoektermen	<<LEEG>>	"Informatiebeveiliging"	"Huisartsenpraktijk"	"ICT in de Zorg"	"Patiëntengegevens"	"Elektronisch medisch dossier"	"Elektronisch Patiëntendossier"	"Huisarts Informatie Systeem"	"Landelijk Schakel Punt"	"Goed Beheerd Zorgsysteem"	"Elektronische gegevensuitwisseling"	"Elektronische informatie-uitwisseling"	"Communicatie in de zorg"	"Zorgorganisaties"
"Informatiebeveiliging"	511													
"Huisartsenpraktijk"	5040	14												
"ICT in de Zorg"	9330	17	54											
"Patiëntengegevens"	1020	25	112	53										
"Elektronisch medisch dossier"	3740	8	189	27	74									
"Elektronisch Patiëntendossier"	1790	42	245	62	179	50								
"Huisarts Informatie Systeem"	8340	4	117	7	45	24	20							
"Landelijk Schakel Punt"	4410	6	11	7	9	4	13	5						
"Goed Beheerd Zorgsysteem"	511	12	7	15	20	7	18	4	8					
"Elektronische gegevensuitwisseling"	813	19	29	14	35	9	27	2	1	7				
"Elektronische informatie-uitwisseling"	1750	3	11	7	14	3	15	0	3	5	10			
"Communicatie in de zorg"	31000	4	24	7	14	2	7	2	0	2	7	0		
"Zorgorganisaties"	1410	12	121	40	43	17	57	7	4	2	10	0	8	

Bij de zoekbibliotheek van Google Scholar zijn met de Nederlandse zoekopdrachten in totaal 1156 zoekresultaten (ten hoogste 20 resultaten per zoekopdracht) bekeken en beoordeeld op relevantie en type informatie.

In tabel 4 zijn de gebruikte combinaties van zoekopdrachten (uitgevoerd tussen quotes) weergegeven met op de kruispunten het aantal gevonden resultaten. Groene waarden bevatten relevante artikelen in de eerste 20 resultaten van de betreffende zoekopdracht.

Tabel 4: Zoekresultaatmatrix Google Scholar (Engelse zoektermen)

Aantal zoekresultaten bij verschillende zoektermen	<<LEEG>>	"eHealth"	"Electronic Patient record"	"eScience"	"General Practitioner" OR "general practices"	"Healthcare"	"Health Care Organizations"	"Healthcare Information"	"Information Exchange"	"Information Security"	"Information Technology"	"National Health Service"	"private communications Security"	"Secure Private Communications"
"eHealth"	46100													
"Electronic Patient record"	18300	3560												
"eScience"	30400	561	138											
"General Practitioner" OR "general pra	1460000	1690	782	50										
"Healthcare"	3440000	28800	14600	4850	130000									
"Health Care Organizations"	88600	4210	1270	73	2670	50700								
"Healthcare Information"	47100	9000	2750	317	1850	46900	2980							
"Information Exchange"	499000	9570	1950	1950	3640	77100	3870	5980						
"Information Security"	367000	7170	1050	2000	698	56100	1410	4210	15300					
"Information Technology"	2500000	26900	7690	11600	12100	620000	15200	22200	75600	161000				
"National Health Service"	590000	5370	2000	339	39900	232000	4740	2290	3760	1190	20100			
"Private communications Security"	10100	102	10	24	45	1730	37	57	598	997	2300	74		
"Secure Private Communications"	78	0	0	0	0	16	1	4	4	1360	42	0	0	

Bij de zoekbibliotheek van Google Scholar zijn met de Engelse zoekopdrachten in totaal 1635 zoekresultaten (ten hoogste 20 resultaten per zoekopdracht) bekeken en beoordeeld op relevantie en type informatie.

PUBmed

In tabel 5 zijn de gebruikte combinaties van zoekopdrachten (uitgevoerd tussen quotes) weergegeven met op de kruispunten het aantal gevonden resultaten. Groene waarden bevatten relevante artikelen in de eerste 20 resultaten van de betreffende zoekopdracht.

Tabel 5: Zoekresultaatmatrix PUBmed

Aantal zoekresultaten bij verschillende zoektermen	<<LEEG>>	"eHealth"	"Electronic Patient record"	"eScience"	"General Practitioner" OR "general practices"	"Healthcare"	"Health Care Organizations"	"Healthcare Information"	"Information Exchange"	"Information Security"	"Information Technology"	"National Health Service"	"Private communications Security"	"Secure Private Communications"
"eHealth"	22709													
"Electronic Patient record "	843	62												
"eScience"	101	1	0											
"General Practitioner" OR "general pra	5962	66	13	0										
"Healthcare"	1038997	19711	276	5	2531									
"Health Care Organizations"	3344	57	4	0	2	1827								
"Healthcare Information"	1198	82	12	0	1	1199	3							
"Information Exchange"	2606	138	13	0	6	1031	27	51						
"Information Security"	388	28	1	0	1	115	3	19	9					
"Information Technology"	16225	743	65	0	32	4224	141	213	243	46				
"National Health Service"	12134	67	13	0	136	4678	25	2	5	2	80			
"Private communications Security"	0	0	0	0	0	0	0	0	0	0	0	0		
"Secure Private Communications"	0	0	0	0	0	0	0	0	0	0	0	0	0	

Bij de zoekbibliotheek van PUBmed zijn in totaal 895 zoekresultaten (ten hoogste 20 resultaten per zoekopdracht) bekeken en beoordeeld op relevantie en type informatie.

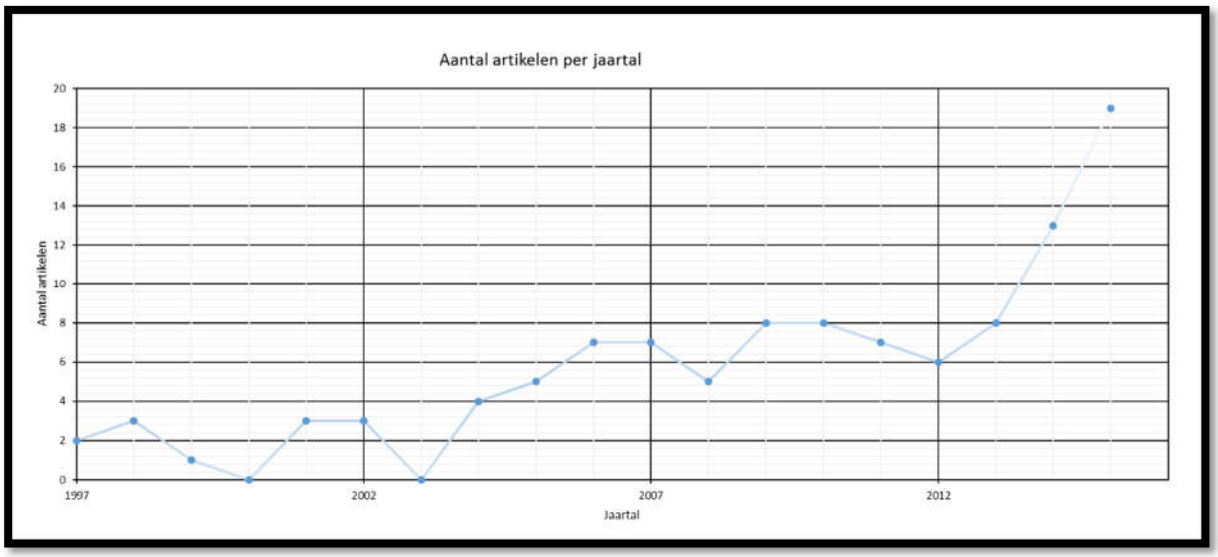
Tijdens gesprekken die zijn gevoerd met een huisartsenpraktijk en bij een bezoek aan een bijeenkomst van de NEN-organisatie (dd. 16-03-2016) met titel "Revisie NEN 7510 en NEN 7513" zijn nog 2 artikelen naar voren gekomen die zijn toegevoegd aan de zoekresultaten.

Na het doornemen van de artikelen en referentielijsten zijn met de sneeuwbalmethode nog een totaal van 12 artikelen toegevoegd aan de zoekresultaten.

Van alle zoekresultaten is het digitale artikel verkregen en vervolgens is deze verder bekeken.
Op basis van titel en abstract zijn uit alle vier de literatuurbibliotheken en uit direct verkregen tips en via de sneeuwbalmethode vervolgens 201 unieke artikelen geselecteerd, op basis van de vooraf gestelde criteria. Deze artikelen zijn vervolgens geheel doorgenomen, waarbij ze zijn ingevoegd in de zoekfiguren met zoektermen. De uiteindelijk geselecteerde en relevante 117 artikelen zijn gepubliceerd tussen 1997 en 2016.

In figuur 4 volgt een overzicht van de spreiding van het aantal gevonden artikelen afgezet tegen het jaartal. Het jaartal 2016 (8 artikelen) is hierbij weggelaten omdat de uitvoering van de zoekmethode in het eerste kwartaal van het lopende jaar is gedaan en geen goede voorspelling gedaan kan worden wat nog zal worden gepubliceerd in de overige maanden van 2016.

Figuur 4: Overzicht van het aantal gevonden artikelen, per jaartal waarin ze zijn gepubliceerd

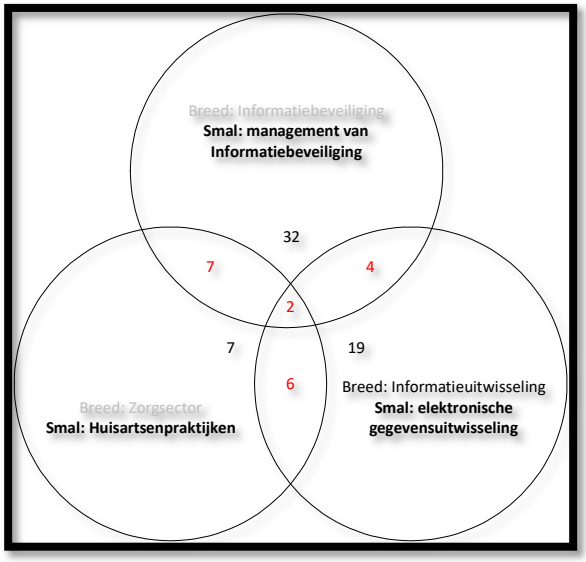


3.2 Behandeling zoekresultaten in termen van metadata

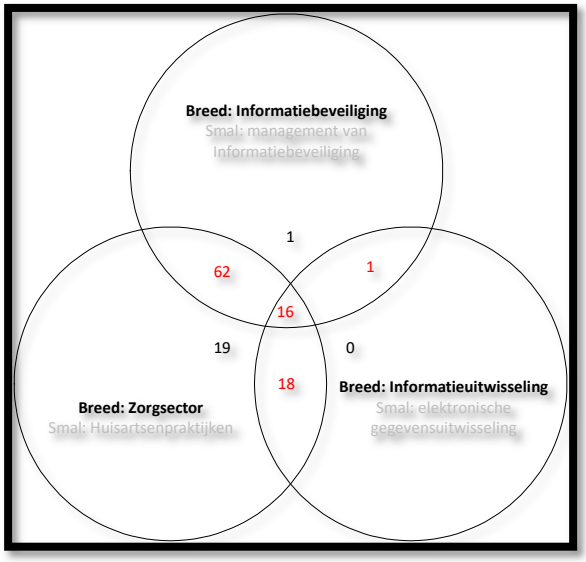
Zoals in het hoofdstuk Methode reeds is aangegeven zijn de zoekresultaten ingedeeld in aantallen per onderwerp waarop ze betrekking hebben. Waar de resultaten kunnen worden ingedeeld in de drie smalle zoekgebieden zijn deze opgeteld en in figuur 5 weergegeven. Hetzelfde is gedaan voor de drie brede zoekgebieden. De resultaten hiervan zijn opgeteld en in figuur 6 weergegeven.

Alle artikelen worden slechts 1 keer gebruikt per figuur. Hierdoor is bijvoorbeeld te zien dat er wel artikelen zijn te vinden over alleen elektronische uitwisseling (weergegeven cijfer 19, smalle term). Deze hebben dan geen betrekking op management van informatiebeveiliging of huisartsenpraktijken. Omdat deze artikelen wel betrekking hebben op de raakvlakken informatie-uitwisseling en zorgsector of informatiebeveiliging (brede termen), komen ze echter niet terug in het losse cijfer van Informatie-uitwisseling (weergegeven cijfer 0).

Figuur 5: Resultaat smalle zoekgebieden



Figuur 6: Resultaat brede zoekgebieden



Uit de methode van de gevonden literatuur is de gebruikte onderzoeksmethode gehaald, zoals deze door de auteur beschreven wordt. In figuur 7 is de onderverdeling weergegeven van de diverse methodes.

Figuur 7: Verdeling van resultaten naar onderzoeksmethode

Daarnaast zijn de zoekresultaten ook gegroepeerd op basis van gebruik van praktijkgerichte en theoriegerichte methode. Dit levert een verdeling op van 60 praktijkgerichte artikelen en 57 theoretisch gerichte artikelen.

Uit de praktijkgerichte literatuur is in bijna alle gevallen terug te herleiden via de methode en omschrijving van de dataverzameling bij wat voor organisatie(type) het onderzoek is verricht. Twee onderzoeken maken dit niet bekend vanwege privacyoverwegingen. Hierbij is de specifieke organisatie door de auteur gegeneraliseerd tot “zorginstelling”. Eén onderzoeker heeft de organisatie niet opgegeven, alleen aangegeven dat het een bedrijf in de zorgsector is. Figuur 8 geeft een weergave van de totale verdeling binnen de praktijkgerichte literatuur.

Figuur 8: Verdeling van praktijkgerichte literatuur naar organisatie(type)

In 29 van de 60 praktijkgerichte onderzoeken wordt een onderzoek uitgevoerd exclusief binnen een ziekenhuis of meerdere ziekenhuizen. Van de resultaten zijn 9 artikelen exclusief gericht op huisartsenpraktijken. De resultaten waarin meerdere organisaties voorkomen zijn gericht op casestudies (3x), uitgevoerde enquête bij grote groepen respondenten (5x) en interviews bij personen uit meerdere organisaties (3x). Binnen de groep van andere organisaties vallen studies uitgevoerd bij GGZ (2x), NHS Trust (1x), klinieken (3x) en technologiebedrijven (2x).

3.3 Inhoudelijke behandeling literatuur

Vanuit de gevonden artikelen is een beeld te maken van de beschikbare literatuur van informatiebeveiliging in de zorg. In deze paragraaf zal een uitwerking gegeven worden van de gevonden literatuur en zullen aan de hand daarvan de onderzoeksvragen beantwoord worden. Allereerst zal ingegaan worden op de begrippen die gebruikt worden in deze literatuurstudie en de doorzochte literatuur (beantwoording deelvraag 1). Omdat de literatuur rondom de smalle scope “management van informatiebeveiliging van gegevensuitwisseling bij huisartsenpraktijken” beperkt is, zullen resultaten uit de bredere scope “management van informatiebeveiliging in de zorg” ook weergegeven worden. Deze uitbreiding zal in de uitwerking van de resultaten terug te zien zijn. Zo zal binnen elke sub paragraaf allereerst ingegaan worden op literatuur die betrekking heeft op de smalle scope, waar deze literatuur beschikbaar is. Daarna wordt verbreed naar de literatuur uit de brede scope. Zo wordt getracht een goed beeld te creëren van de beschikbare literatuur ten aanzien van elke onderzoeksvraag en de grenzen aan de literatuur ten aanzien van de smalle scope.

3.3.1 Management van informatiebeveiliging in de zorg

In diverse artikelen worden definities voor informatiebeveiliging, informatietechnologie en informatie-uitwisseling gebruikt. Voorafgaand aan dit literatuuroverzicht moeten de definities goed worden neergezet, om te zorgen dat een eenduidige vergelijking van de gevonden artikelen mogelijk is en een eenduidige begripsvorming in dit literatuuroverzicht ontstaat.

De term informatie-uitwisseling komt in veel vormen terug. In deze literatuurstudie zal de term informatie-uitwisseling beperkt zijn tot het uitwisselen van patiëntgegevens en behandelmethoden tussen huisartsenpraktijken, al dan niet ondersteund door technische oplossingen. Hij gaat hier niet

in op communicatie(protocollen) van de technische systemen of vormen van (non-)verbale communicatie die niet tot doel hebben patiëntgegevens en behandelmethoden uit te wisselen.

Informatietechnologie (IT) omvat “alles wat te maken heeft met de geautomatiseerde verwerving en verwerking van informatie” (vandale.nl).

De NEN7510 normering omschrijft informatiebeveiliging als waarborgen van de Beschikbaarheid (Availability), Integriteit (Integrity) en Vertrouwelijkheid (Confidentiality) van systemen en informatie en inrichten van maatregelen om risico’s tot een acceptabel niveau te beperken. Binnen de norm kan elke organisatie zelf bepalen welke informatiebeveiligingsmaatregelen relevant zijn. Bonthuis (Bonthuis, 2007) vat de norm in een aantal beveiligingsaspecten samen;
“Beveiligingseisen ten aanzien van personeel en toegang. Aspecten als het laten afgeven van een verklaring omtrent het gedrag door personeel dat met gevoelige informatie werkt, het hebben van beschrijvingen van functies met diens rollen, verantwoordelijkheden, toegangsrechten, zwijgplichten en geheimhouding, maar ook het uitvoeren van beleid omtrent bewustwording over de beveiligingseisen worden in de norm behandeld. De norm bevat tevens richtlijnen om het fysieke beveiligingsbeleid deugdelijk op te zetten en gaat daarbij voornamelijk over de beveiliging van de omgeving. Aspecten als versleuteling, toegangsbeheer, firewalls, virusscanners (naast de fysieke beveiliging als sloten op kantoorruimtes) komen in de norm aan bod. Met betrekking tot het onderdeel ‘operationeel beheer van ICT’ gaat de norm voornamelijk in op aspecten als functionaliteit, betrouwbaarheid, doelmatigheid, onderhoudbaarheid en overdraagbaarheid van ICT. Ook schrijft de norm bepalingen voor omtrent functiescheidingen, ISO 9126, de norm om kwaliteitseisen aan ICT-diensten of producten te operationaliseren, de te nemen maatregelen tegen kwaadaardige apparatuur, het maken van reservekopieën, de keuze en beveiliging van gebruikte media en systeemdocumentatie, maar bevat vooral beleid omtrent gegevensuitwisseling. De norm is gebaseerd op de eisen uit de relevante wetgeving. Zij noemt daarbij de WGBo, de WBP, maar ook de Wet Computercriminaliteit (WCC) en de Wet Identificatie bij Dienstverlening (WID). Naast het borgen van de kwaliteitscriteria vereist de norm ook dat de informatiebeveiligingsmaatregelen op controleerbare wijze zijn ingericht voordat kan worden gesproken over adequate informatiebeveiliging. De norm is voornamelijk gespitst op technische maatregelen, voor de organisatorische maatregelen kunnen we kijken naar de normen zoals opgesteld door de praktijk.”

In de NEN7510 norm is ook opgenomen dat een Information Security Management Systeem (ISMS) ingericht moet worden om zo de informatiebeveiliging continu te beheersen en verbeteren. De maatregelen die getroffen worden, zijn de relevante risico’s uit de risicoanalyse die ook in de norm beschreven wordt. Bij de risicoanalyse worden zowel de algemene informatiebeveiligingsaspecten van een organisatie bekeken als ook die van specifieke informatie en systemen om zo “passende” maatregelen te kunnen nemen. De ISO-standaarden en NEN-normen zijn echter alleen een startpunt en bieden zelf geen uitgebreide informatie hoe beveiligingsmaatregelen moeten worden geïmplementeerd en beheerd (Orel & Bernik, 2013). De vereiste mate van beveiliging hangt onder andere af van stand van de informatietechnologie en de aard en omvang van de persoonsgegevens. Medische gegevens moeten als bijzondere persoonsgegevens worden beschouwd en vereisen dan ook een hoger beschermingsniveau (Bonthuis, 2007).

Om de toepassing binnen de praktijk te vergemakkelijken zijn in de NEN7511 toetsbare voorschriften ontwikkeld. Het is namelijk niet meer de vraag of informatie moet worden beveiligd, maar hoe dit snel en effectief aan te pakken (Daams & Ragetilie, 2005). Om verder onderscheid te maken in de toepassing bij verschillende typen organisaties zijn er drie varianten van de NEN7511 uitgegeven; Het resultaat; de NEN7511-1 voor ‘complexe organisaties’ zoals ziekenhuizen, NEN7511-2 voor ‘middelgrote organisaties’ zoals verpleegtehuizen en NEN7511-3 voor kleine praktijkhouders zoals huisartsen en fysiotherapeuten. (J. van der Wel, 2005)

De NHG-Standaarden vormen inmiddels een stevig wetenschappelijk fundament onder de huisartsgeneeskunde en zijn als normstellende documenten een belangrijk hulpmiddel voor het interne kwaliteits- en accrediteringsbeleid van de beroepsgroep. De uitdaging is het actueel houden van alle richtlijnen die beschikbaar zijn en een snelle(re) implementatie in de praktijk (Goudswaard, Veld, & Dijkstra, 2012).

Naast deze normen zijn verschillende handreikingen uitgegeven voor het uitvoeren van informatiebeveiliging in de zorg. Zo is het boek “Informatiebeveiliging in de zorg” (J. van der Wel, 2006) uitgegeven om zorgmanagers meer kennis en handvatten te geven voor het verder verbeteren van informatiebeveiliging en is “Informatiebeveiliging in de huisartsenpraktijk” (Nederlands Huisartsen Genootschap, 2009a) uitgegeven om huisartsenpraktijken te ondersteunen.

Ook in de literatuur wordt er gekeken naar het beheersen (management) van informatiebeveiliging en de reikwijdte van de benodigde maatregelen. Er worden voor toetsing en implementatie van informatietechnologie en informatiebeveiliging veel modellen voorgesteld, zoals het Technology Maturaty Model, die wellicht ook toepasbaar is op het domein van informatiebeveiliging (Brady, 2011), information security culture framework van AlHogail (2015) op basis van het STOPE model of het model van Goldstein en Frank (2016) die een IT security management en ontwerpmodel voorstellen dat vanuit meerdere perspectieven die bestaan bij verschillende stakeholders kan functioneren. Er is in sommige landen (Australië en Nieuw-Zeeland leiden hierin) een consensus dat er specifiekere informatie rondom informatiebeveiliging voor de zorg nodig is ten aanzien van informatiebeveiliging in andere sectoren (Orel & Bernik, 2013). Er zijn hiervoor standaarden ontwikkeld specifiek voor de zorg, zoals de ISO27799 en NEN7510.

Arnbak (2015) geeft in zijn thesis een advies aan de EU voor het veranderen van wetgeving op het gebied van beveiligde communicatie om de toenemende bedreigingen op veilige communicatie te weerstaan. Hij geeft aan dat door de zeer perverse incentives in de markt, surveillance en politiek de veilige communicatie ondermijnd wordt. Daarom is het van belang wetgeving op te nemen die cruciale rechten, socio-technische en marktontwikkelingen integreren. Ook stelt hij dat er nu fundamentele fouten in bestaande wetgeving zitten, waardoor beveiliging niet wordt afgedwongen bij nieuwe technologieën en verbeteringen niet worden doorgevoerd waar ze écht nodig zijn. Park (2015) laat zien dat de overheid van Nieuw Zeeland een grote rol speelt in de standaardisatie van zorgsystemen en informatiebeveiliging en een goede interactie met het bedrijfsleven bestaat voor het inventariseren van ideeën voor nieuwe standaarden. Dit kan een drijvende kracht zijn achter de hoge mate van standaardisatie van zorgsystemen in het land.

3.3.2 Kwaliteit van zorg en inzet van IT

De standaardisatie op het gebied van beveiliging moet leiden tot een hogere kwaliteit van de zorg. Ook door implementatie van IT worden processen in zorgorganisaties verder ondersteund of geautomatiseerd. Hierdoor is er een hogere kwaliteit van de processen die binnen een zorgorganisatie aanwezig zijn. In het artikel van Mahncke en Williams (2014) wordt een framework voor Security Governance ontwikkeld als toevoeging op Security Management om zo te kunnen zorgen dat management van informatiebeveiliging niet alleen goed uitgevoerd wordt, maar ook kan bijdragen aan de organisatie.

De studie van Scott, Hallett en Fettiplace (2013) laat zien dat, door een computer gegenereerde tekstuele samenvattingen van een patiëntendossier de benodigde informatie-zoek-tijd van de behandelend arts significant kan reduceren ten opzichte van het handmatig doorzoeken van het dossier zonder dat de kwaliteit van de verkregen informatie achteruit gaat. De studie van Pai en Huang (2011) laat zien dat systeemkwaliteit in de vormen van ontwerpkwaliteit, reactietijd en toegankelijkheid positief kan bijdragen aan de perceptie van gebruiksgemak voor de gebruiker. Ook laat het een positief verband zien tussen perceptie van gebruiksgemak en gebruiksintentie. Het gebruik van een informatiemanagement systeem draagt bij aan de productiviteit en efficiëntie, wat positief effect heeft op het daadwerkelijk gebruik van systemen. Het is dus nodig om bij introductie van zorgsystemen het gebruik ervan makkelijk te maken en eenvoudig om te leren, zodat ze sneller gebruikt zullen worden door de medewerkers. Wel is er een verschil tussen verschillende groepen stakeholders te vinden als het gaat om de attitude ten aanzien van het gebruik van elektronische patiëntdossiers die uitgewisseld worden tussen ziekenhuizen. Zo kunnen er volgens Jong-Yi et al. (2015) drie groepen worden onderscheiden, namelijk medici, ondersteunende medewerkers en patiënten.

Brandhorst (2008) maakt een ontwerp om de huisarts te helpen sneller en betere patiëntinformatie te kunnen verkrijgen tijdens het consult. Het vinden van de juiste informatie in de grote hoeveelheid gegevens die tegenwoordig beschikbaar is, kan een aanzienlijke hoeveelheid tijd kosten. Deze tijd is in veel gevallen niet beschikbaar tijdens het consult van 10 minuten. De tijd die benodigd is, is ook in de studie van Shapiro (Shapiro, Kannry, Kushniruk, & Kuperman, 2007) een belangrijk punt waarom spoedartsen graag sneller gegevens willen kunnen uitwisselen. Zij geven aan vaak met een incompleet patiëntbeeld te moeten werken omdat gegevens gewoonweg te traag kunnen worden verkregen bij andere afdelingen en zorgaanbieders.

De studie van Safran et al. (1998) laat zien dat introductie van nieuwe technologie zowel positieve als negatieve gevolgen kan hebben. Zo kan het communicatie, samenwerking en toegang tot informatie vergroten, maar bestaat ook de kans tot een stortvloed aan informatie die niet gewenst of onnodig is. Ook wordt opgemerkt dat bij het overnemen van een bepaalde rol in de organisatie door een computer, ook de verwachtingen aan die rol wijzigen. Als voorbeeld wordt hierbij de berichtenrol gegeven, waarbij niet meer de verwachting is dat post dezelfde week wordt bezorgd, maar direct na verzending. Daarnaast is het de vraag of alle nieuwe technologie bijdraagt aan een betere kwaliteit van zorg. In een van de gevonden artikelen wordt de opkomst van de iZorg beschreven. Hiermee worden de mobiele Apps voor het iOS en Android platform bedoeld. Omdat er waarschijnlijk geen medische specialisten in dienst zijn bij de makers van deze Apps is het de vraag of de kwaliteit van echte medische specialisten kan worden gehaald met de vele beschikbare zelf-diagnose Apps (Edlin & Deshpande, 2013).
Er zijn ook onderzoeken die nieuwe technologie inzetten en daarover rapporteren. Onder verpleegkundigen lijkt het gebruik van elektronische apparatuur voor onderlinge communicatie positief, al zijn er nog wel bezwaren ten aanzien van beveiliging, onvoldoende gebruikerskennis en minder sociaal contact (Koivunen, Niemi, & Hupli, 2015). Hersh et al. (2015) geven aan dat een analyse van de klinische risico's bij implementatie van uitwisselingssystemen in de zorg nog gedaan moet worden alhoewel er wel bewijs is dat in specifieke situaties al kwaliteitsverbeteringen worden gehaald met dergelijke implementaties.

Ook kan geleerd worden door de evaluatie van zorg IT-implementaties te gebruiken en deze verder te verbeteren. Voornamelijk op het gebied van de verschuivende markt kunnen deze evaluatiemethoden verbeterd worden (Cresswell, 2016). Waar goed op moet worden gelet is het verschil tussen landelijke en stedelijke praktijken. MacGregor, Hyland en Harvie (2009) laten zien dat de keuzes binnen ICT adoptie verschillen bij deze verschillende typen praktijken en er daarom waarschijnlijk geen universele factoren van ICT adoptie kunnen worden gevonden. In de studie van Leung (2012) wordt gesteld dat bij ziekenhuizen, de grootte uitmaakt als gekeken word naar de manier waarop het beste informatiesystemen kunnen worden geadopteerd. Zo zijn de grotere ziekenhuizen beter in het absorberen van nieuwe informatie en systemen. De kleine zijn er beter in de eigen en bestaande processen en resources aan te passen.

Belangrijke factoren waarom praktijken afwachtend zijn bij het implementeren van andere zorgsystemen zijn de snelle technologische veranderingen en het dynamische bedrijfsklimaat (Goroll, Simon, Tripathi, Ascenzo, & Bates, 2009). Zo zijn er ontwikkelingen op het gebied van cloud computing en big data gaande die vragen oproepen rondom informatiebeveiliging en privacy. Deze vragen vertragen verdere adoptie van ontwikkelingen als cloud computing en big-data in de zorg (J.-J. Yang et al., 2015). Als gekeken wordt naar het Outsourcen van systemen valt op dat voornamelijk privacygevoelige systemen sneller geoutsourced worden dan niet-privacygevoelige systemen, zo stellen Lorence en Spink (2004) in hun artikel. Ook op het gebied van de huidige mogelijkheden van e-health heerst er nog onwetendheid over de beveiliging van dergelijke gegevens (Vanlaer, 2015).

Poon et al. (2006) laten zien dat adoptie van ICT waarbij financiële voordelen gehaald worden ver vooruit loopt ten aanzien van adoptie van systemen die enkel veiligheid en kwaliteit verbeteren. Organisaties staan voor enorme financiële uitdagingen om zorginformatiesystemen te implementeren. De adoptie kan worden geholpen door financiële incentives, zodat het initiële productiviteitsverlies de adoptie niet tegenhoudt. Voornamelijk kleinere praktijken vinden het moeilijk om dit soort systemen te kopen en te onderhouden. Daarnaast bestaat een hoge kans op fouten bij de implementatie, waardoor het onwaarschijnlijk is dat ze zullen worden uitgerold.

Het artikel van Innis, Dryden-Palmer, Perreira en Berta (2015) laat zien dat bestaande literatuur duidelijk maakt dat er financiële middelen nodig zijn voor de adoptie van veranderingen, maar dat er geen details worden gegeven als het gaat om de kosten. Het zou daarom, in deze tijd van financiële beperkingen, interessant zijn om te onderzoeken in hoeverre financiële ondersteuning effect heeft op het oppakken en implementeren van best-practices in de zorg. Ook zien Luzi, Pecoraro en Tamburis (2016) veel knelpunten die een goede evaluatie in de weg staan. Ze geven in hun onderzoek algemene punten om tot een mogelijke kostenberekening te komen. Als gekeken wordt naar het maken van een volledige kostenevaluatie van de inzet van zorgsystemen, zal nog wel veel onderzoek verricht moeten worden.

Naast het verhogen van de snelheid van diagnosestelling en het weghalen van (de kosten van) dubbele behandelingen kan nieuwe IT ook bijdragen aan verdere kostenreductie (H. Park et al., 2015). Dit kan ervoor zorgen dat introductie van nieuwe IT in de zorg de kosten van zorg verder omlaag brengt. Toch wordt hier ook sceptisch tegen de introductie van nieuwe zorgsystemen aan gekeken, omdat zorgsystemen die gegevensuitwisseling mogelijk maken wellicht minder opleveren voor de zorgaanbieder die het implementeert dan voor de overige stakeholders (Cohn et al., 2009).

Bij de meeste onderzoeken wordt gekeken naar inzet van IT en de verbetering van zorgkwaliteit die deze teweeg brengt. Bij informatiebeveiliging van medische gegevens is een dergelijke kostenberekening moeilijker te maken. Er wordt veel over deze inschatting gedebatteerd. Het komt neer op het inschatten van de waarde van de medische informatie, grootte van het risico van ongeoorloofde bekendmaking, kosten van een dergelijk incident en kosten van preventieve maatregelen (Rindfleisch, 1997).

3.3.3 Eisen aan management van informatiebeveiliging

Binnen de zorg wordt steeds meer informatietechnologie ingezet om taken te automatiseren, beschikbaarheid en kwaliteit van informatie te verhogen en veiligheid van informatie en van de patiënt te verbeteren. Er is door de artikelen heen een duidelijke verwevenheid te zien tussen informatiebeveiliging en de informatietechnologie die wordt beveiligd of de informatietechnologie die voor de beveiliging nodig is. Het is ook logisch dat informatietechnologie wordt ingezet om zorgprocessen te ondersteunen en de mate van informatiebeveiliging te verhogen. Papier wordt bijvoorbeeld gezien als foutgevoelig en inefficiënt voor gegevensuitwisseling, zo laten de artikelen van Westerman, Hull en Bezemer en Gort en Branger et al. (geciteerd; Schabetsberger et al., 2004) zien. Omdat de zorgsector specifieke eisen heeft aan de informatiebeveiliging, zal ook specifiek naar deze sector moeten worden gekeken bij het beschouwen van de beschikbaarheid van literatuur over informatiebeveiliging.

Vanuit het artikel van Mommers (2008) worden de wetten “Wet op de Geneeskundige Behandelovereenkomst (WGBO)”, “Wet gebruik burgerservicenummer in de Zorg” en “Wet Bescherming Persoonsgegevens (Wbp)” genoemd die toezien op de bescherming van de persoonsgegevens van de patiënt. De WGBO bevat een aantal artikelen die betrekking hebben op de informatiepositie van behandelaar, patiënt en derden. Daarnaast wordt gezegd in welke mate anderen dan patiënt en zijn behandelaar toegang mogen hebben tot deze informatie. De Wet gebruik burgerservicenummer in de Zorg geeft voorwaarden weer waaraan het EPD-systeem (Elektronisch Patiënten Dossier) van de zorgverlener moet voldoen om aansluiting te kunnen krijgen op het landelijk EPD. De Wbp bevat regels onder welke omstandigheden de persoonsgegevens verwerkt mogen worden. Verwerking is buiten de voorwaarden binnen deze regels om verboden.

- Artikel 13 Wbp, “passende technische en organisatorische maatregelen ten uitvoer om Persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking”

Het Wbp schrijft een aantal dwingende normen voor, die in het artikel van Borking (2001) globaal uiteen worden gezet. Deze normen ten aanzien van de verwerking van de persoonsgegevens zijn; Melding van de verwerking, Transparantie van de verwerking, Doelbinding voor de verwerking, Rechtmatige grondslag voor de verwerking, Kwaliteit van de gegevens, Rechten van de betrokkenen, Beveiliging tegen verlies of onrechtmatige verwerking van persoonsgegevens, Verwerking van persoonsgegevens door een bewerker en Gegevensverkeer met landen buiten de EU.

De studie van Evers en Barels (2014) geeft 18 wetteksten en 10 normen en richtlijnen op die specifiek betrekking hebben op eHealth in Nederland. Daarvan heeft een deel betrekking op de informatiebeveiliging van de gegevens van patiënten en overdracht daarvan. Wetten als de Wbp (Wet Bescherming Persoonsgegevens), Wbsn-z (Wet gebruik Burgerservicenummer in de zorg) en normen “Gedragscode Elektronische Gegevensuitwisseling in de Zorg”, NEN7510, NEN7512, NEN7513, NHG-richtlijnen over informatie-uitwisseling (veelal zijn de praktische beveiligingsrichtlijnen in de bijlage opgenomen) worden genoemd. Meersbergen (2007) geeft in de uitgave “KNMG Richtlijn Arts-Patiënt contact” nog een aanvulling ten aanzien van het arts- en patiëntcontact. Zowel de arts als de patiënt, met een actieve behandelrelatie, mogen gegevens uitwisselen, mits zij beiden voldoende maatregelen nemen.

Kotz, Fu, Gunter en Rubin (2015) vertellen dat de ISO27799 specifiek gemaakt is voor de zorgsector en ondersteuning biedt bij de implementatie en interpretatie van de ISO27002 standaard. Met het implementeren van deze standaard kunnen de ergste beveiligingsrisico’s vermeden worden en kan een minimaal niveau van vertrouwelijkheid, integriteit en beschikbaarheid behaald worden.

Tot deze conclusie komen Gomes en Lapao (2008) ook tijdens het uitvoeren van een case met deze standaard. Met de ISO27002 is een goede benchmark voor diverse organisaties te maken. Dit betekent echter wel dat specifieke standaarden nog moeten worden ontwikkeld door de organisaties. Orel en Bernik (2013) geven daarnaast de ISO-standaarden 27799:2008 “Health informatics - Information security management in health using ISO/IEC 27002”, ISO/TR 18307 “Health informatics - Interoperability and compatibility in messaging and communication standards - Key characteristics” en ISO/TS 18308 “Health informatics - Requirements for an electronic health record architecture” op. Ze geven hierbij aan dat deze standaarden zijn geschreven voor specialisten in het veld. In het geval van de zorg gaat het dan om beveiligingsspecialisten. Mahncke en Williams (2014) noemen de ISO/IEC 27014:2013 standaard “Information technology -- Security techniques -- Governance of information security” bij huisartsenpraktijken in hun onderzoek en doen een voorstel voor een praktische implementatie van de standaard.

Ook internationaal zijn er verwijzingen naar wetgeving en standaarden. Zo benoemen Przybylo et al. (2014) de Health Insurance Portability and Accountability Act (HIPAA), de wetgeving in de Verenigde Staten waarin regels zijn opgenomen over beveiligde uitwisseling binnen de zorg.

In diverse standaarden zit ook de aanpak verwerkt om de vereiste maatregelen te implementeren in de organisatie. Jašek, Králík en Popelka (2015) geven in hun artikel een samenvatting van de ITIL aanpak en ISO 2700x standaarden die het management van informatiebeveiliging beschrijven. Hoerbst, Hackl, Blomer en Ammerwerth (2011) geven hierbij aan dat op basis van hun studie een verband lijkt te zijn tussen het niveau van implementatie van ITIL en het aantal ITIL gecertificeerde medewerkers. Wel hebben ziekenhuizen duidelijk hulp nodig bij het succesvol verder implementeren van ITIL, alhoewel de literatuur specifiek hiervoor schaars is. Janczewski & Xinli Shi (2002) hebben een set informatiebeveiliging maatregelen voorgesteld voor het gebruik van informatietechnologie in de zorg in Nieuw-Zeeland. Deze set maatregelen lijkt in opbouw van management sterk op de later verschenen ISO27001 standaard.

Ook de ISO27003 standaard beschrijft het opzetten van een managementsysteem. Haufe, Dzombeta en Brandis (2014) lichten in hun artikel de vijf stappen van deze opzet verder toe. Deze stappen zijn; managementtoestemming verkrijgen voor het opzetten van een ISMS, ISMS-scope en beleid bepalen, organisatorische analyse uitvoeren, risico-inventarisatie en -mitigatieplan opstellen en het ISMS ontwerpen. Door het opstellen van duidelijke eisen in deze fase zal de daadwerkelijke implementatie van een ISMS zo effectief mogelijk kunnen worden uitgevoerd. Als een Maturity Model voor het ISMS wordt aangehouden, kan deze zo transparant en kosten effectief mogelijk worden ingezet. In het artikel van Gritzalis (1997) wordt een Security Baseline Policy voorgesteld om te zorgen dat er voortgang blijft zitten in de ontwikkeling van beveiliging van systemen. Ze geven hierbij aan dat het lastig is om hier voldoende steun voor te krijgen. Ze stellen; “experts must always try to make information systems more secure, while they must simultaneously keep alive the belief that these systems will harm the confidentiality, integrity or availability of the healthcare data”.

In het artikel van Elrefaey (2015) wordt een Security Scorecard voorgesteld, waarmee de staat van informatiebeveiliging in de organisatie weergegeven kan worden op een leesbaar niveau voor managers en bestuurders zoals de Chief Information Officer of de Chief Financial Officer.

Om informatiebeveiliging in een organisatie te implementeren is een bedrijfsimpact analyse en risicoanalyse het belangrijkste element. Tsung-Han, Cheng-Yuan en Man-Nung (2016) geven een informatiebeveiligingsmethode op basis van de SQUARE methodologie om zo alle benodigde taken van informatiebeveiligingsmanagement te kunnen uitvoeren.

Ook de SEISMED en ISHTAR geven richtlijnen voor het opzetten van een compleet informatiebeveiligingsbeleid. Risicoanalyse is hierbij één van de algemene uitgangspunten om bedreigingen en mogelijke oplossingen in kaart te brengen (Bourka, N, & D, 2001). Voor IT management is informatiebeveiliging inmiddels een belangrijk onderwerp en een zeer substantiële uitdaging geworden (Goldstein & Frank, 2016).

Maar zelfs als management van informatiebeveiliging op zijn plaats is, kan het nog zijn dat de gebruiker een zwak wachtwoord kiest en daarmee een kwetsbaarheid creëert. Het artikel van Cazier (2006) stelt dat awarenesstraining hier een belangrijke positieve bijdrage kan leveren.

3.3.4 Informatiebeveiliging en de medewerker

In de master thesis van Mouw (2012) wordt aangegeven dat het uitvoeren van een risico analyse alleen gedaan kan worden door medewerkers die kennis hebben van de vakgebieden IT- als beveiliging. Dit wordt bevestigd door Orel en Bernik (2013) die stellen dat standaarden op het gebied van informatiebeveiliging zouden moeten worden gelezen door experts op het vakgebied, maar ze vaak worden voorgelegd aan niet-technische zorgmedewerkers. Wel moet de awareness omhoog om te zorgen dat bedreigingen voldoende tegengegaan kunnen worden.

De gebruiker bewust maken van informatiebeveiliging is een van de factoren hoe gewenst gedrag kan worden gecreëerd. Box en Pottas (2014) laten in hun literatuuroverzicht zien dat er overeenstemming bestaat over het feit dat trainen van gebruikers een positieve impact heeft op de informatiebeveiliging (2014). D'Arcy, Hovav en Galletta (2009) tonen aan dat het bewust maken van de gebruiker door informatiebeveiligingsproblemen op een praktische manier uit te leggen via awareness trainingen effect heeft op de intentie tot misbruik van systemen. Dit effect is indirect verkregen via het gevoel van zekerheid bij het gebruik van informatietechnologie door de gebruiker en de waargenomen strafmaat.

In de UK hebben Malik en Hossain (2015) een open brief geschreven aan de School of Medicine met een onderbouwing waarom informatietechnologie in het curriculum van zorg opleidingen moet worden opgenomen. Door beter kennis zou ook een betere afweging van de financiële, ethische en wettelijke risico's gemaakt kunnen worden. In Nederland werd omstreeks dezelfde tijd via Zorgvisie eenzelfde oproep gedaan in het blog van Kamman (2015).

Ook Lee, Moy, Kruck en Rabang (2015) geven in hun artikel aan dat onderwijsinstellingen kunnen helpen bij het verbeteren van informatiebeveiliging. Omdat de wetgeving de snelle ontwikkelingen niet bijhoudt, kan educatie een rol spelen om de volgende generatie managers, technici en zorgverleners voldoende op te leiden.

In het artikel van Renaud en Goucher (2012) worden verder aanbevelingen gedaan ten aanzien van de druk die medewerkers voelen door de informatiebeveiligingsmaatregelen. Hier geven ze aan dat de gevoelde druk verminderd kan worden, als er op een positieve manier aandacht wordt besteed aan informatiebeveiliging zoals door middel van beloningen, heldere communicatie en maatregelen, die zichtbaar gelijk zijn voor alle medewerkers. Ook Stahl, Doherty en Shaw (2012) geven aanbevelingen ten aanzien van het opstellen van management van informatiebeveiliging. Zij geven zes aanbevelingen die het gebruik van de maatregelen in de organisatie moeten bevorderen; gebruik van geschreven maatregelen in een toegankelijke taal, lever een medewerker georiënteerde subset van richtlijnen die van toepassing zijn op alle medewerkers, borg de maatregelen met voorbeelden van zaken die belangrijk zijn voor de gebruiker zodat zij het belang beseffen, leg nadruk op de zaken die voor de gehele staff van algemeen belang zijn, verplaats gespecialiseerde inhoud naar bijlagen, geef specifieke en gebruiksklare adviezen en richtlijnen.

Imam en Hammoud (2014) kijken ook naar de niet-technische aspecten van management van informatiebeveiliging die centraal staan binnen de informatiebeveiliging. Dit terwijl juist de technische aspecten vaak de grootste aandacht krijgen bij uitvoerende beveiligers. Ook zij zien, net als de andere studies, een positief verband tussen informatiemanagement en -beleid, organisatorische cultuur en menselijk gedrag. Dit bevestigt dat effectief management van informatiebeveiliging kan worden bereikt door niet-technische aspecten van informatiebeveiliging te borgen in de organisatie. De studie van Sohrabi, Von en Furnell (2016) bevestigd de aanbevelingen die gegeven worden in de eerdergenoemde studies met bevindingen die laten zien dat kennisdeling van informatiebeveiliging, samenwerken voor het behalen van gezamenlijke beveiligingsdoelen en het trainen van de medewerkers bijdragen aan veilig werken.

Wat er ook gekozen wordt, het kan lang duren voordat kleine veranderingen in de processen ten behoeve van informatiebeveiliging écht zijn ingeburgerd in de organisatie. Het is dus zeer belangrijk dat er een heldere strategie, professioneel leiderschap en betrokkenheid vanuit het senior management is (Gaunt, 1998). Dit wordt bevestigd in het artikel van Jašek, Králík en Popelka (2015) die de ITIL aanpak en ISO standaarden voor informatiebeveiliging samenvat.

Zorgverleners omzeilen beveiligingsmaatregelen als ze het gevoel hebben dat deze in de weg staan van tijd die met de patiënt kan worden gespendeerd. Aan de andere kant worden beveiligingsmaatregelen wel opgevolgd als deze niet merkbaar aanwezig zijn (Fernando & Dawson, 2009). Training van de zorgverlener kan hierin een belangrijke rol spelen, omdat deze wellicht niet de kennis heeft om efficiënt met veilige systemen om te gaan.

3.3.5 Eisen aan informatiebeveiliging bij elektronische uitwisseling tussen huisartsenpraktijken

Er is een gedragscode opgesteld door het KNMG en het Nictiz voor gegevensuitwisseling in de zorg, de “Gedragscode voor Elektronische gegevensuitwisseling in de Zorg”. Dit is een van de handreikingen die beschikbaar is om de verscheidenheid aan privacyregels te bundelen en de zorgaanbieder te helpen om een gegronde beslissing te kunnen maken wanneer hij wel of geen medische gegevens mag delen of opvragen en met wie.
De handreiking stelt een aantal voorwaarden voor ten aanzien van rechtmatige verwerking van persoonsgegevens:

- Het geeft een aanvulling op Artikel 13 Wbp met de tekst “De Verantwoordelijke legt aan de personen die zijn belast met het beheer van het Elektronisch Uitwisselingssysteem een geheimhoudingsplicht op”
- Er moet worden voldaan aan de toepasselijke NEN-normen (NEN 7510:2011, NEN 7512)
- Verantwoordelijke bewaart Persoonsgegevens niet langer dan noodzakelijk voor het doel van de Verwerking van persoonsgegevens. Voor zover Persoonsgegevens deel uitmaken van een patiëntendossier in de zin van de Wgbo mogen deze niet langer worden bewaard dan de toepasselijke wettelijke bewaartermijn of zoveel langer als noodzakelijk is voor een goede behandeling van de patiënt
- Indien Persoonsgegevens worden verwerkt door een berwerker, wordt door de verantwoordelijke toegezien op de naleving van eerder genoemde beveiligingsmaatregelen bij deze Bewerker.

Het Nederlands Huisartsengenootschap komt tot dezelfde eisen in hun praktijkwijzer "Informatiebeveiliging in de Huisartsenpraktijk" (Nederlands Huisartsen Genootschap, 2009a), als gekeken wordt naar de eisen, die gesteld worden aan gegevensuitwisseling in de zorg. De afwijking is hier wel dat de NHG de norm NEN7511-3 ook benoemd, omdat deze onder meer voor solopraktijken geldt.

De studie van Nouwt (2006) geeft aan dat er tussen zorgaanbieder en verzekeraar specifieke eisen zijn t.a.v. de beveiliging van uitgewisselde informatie. Het artikel waarnaar verwezen wordt (art. 7.2b Regeling Zorgverzekering) eist hierbij "passende technische en organisatorische maatregelen".

Op landelijk niveau is er het Landelijk Schakel Punt, wat de naam is van de verwijsindex. Er is een landelijke basisinfrastructuur in de zorg, genaamd AORTA, die het mogelijk maakt dat zorgaanbieders, ten behoeve van verschillende zorgtoepassingen op landelijke schaal patiëntgegevens kunnen uitwisselen. Binnen bepaalde randvoorwaarden aan de ICT-beveiliging kan de zorgverlener hier aansluiting op krijgen (Sijm, 2008). Specifiek voor aansluiting op het Landelijk Schakel Punt, een opdracht die het Nictiz (Pluut, 2010) in 2004 heeft gekregen, worden de eisen, die gesteld worden aan een "Goed Beheerd Zorgsysteem" (GBZ) vastgelegd. Dit Landelijk Schakel Punt moet identificatie, authenticatie, logging en een verwijsindex voor alle aangesloten systemen op deze landelijke infrastructuur bevatten. Er worden in een pilottraject 12 "koplopers" geselecteerd die met kennis, expertise en een financiële bijdrage worden ondersteund om te voldoen aan de eisen van een GBZ.
Daarnaast is de Inspectie voor de Gezondheidszorg op zoek naar indicatoren om de mate van implementatie van informatiebeveiliging inzichtelijk te maken, wat illustratief is voor de complexiteit van deze implementatie in de praktijk (Markenstein, 2005).

Bij nieuwe ontwikkelingen zoals eHealth zijn vaak nog veel vragen rondom informatiebeveiliging aanwezig op het juridisch vlak. Voor zorginstellingen blijkt dat vaak toch te complex; ook de ICT leveranciers kunnen hen daar vaak niet in adviseren (de Mul, Adams, Aspria, Otte-Trojel, & Bal, 2013). Ook op landelijk niveau blijven er veel vragen bestaan over informatiebeveiliging. De studie van Greenhalgh, Morris, Wyatt, Thomas en Gunning (2013) vergelijkt casestudies van de vier nationale gedeelde patiodossiersystemen van het Verenigd Koninkrijk. Ook hier is langdurig over beveiliging gesproken. De oplossingen werd echter pragmatisch ingevuld en niet in maatregelen gegoten. Waar dit wel zo was, ging het voornamelijk om technische oplossingen die als bureaucratisch werden gezien door de gebruikers. Op dit moment ontbreekt het nog aan (inter)nationaal geaccepteerde standaarden die data-uitwisseling van patiëntgegevens ondersteunen (Goud, Riper, & Sent, 2014).

Mamlin en Tierney (2016) geven aan dat de wetten voor privacy en beveiliging nog wel geüpdatet moeten worden om bij te blijven bij de technologische ontwikkelingen. Daarnaast moet er informatie gedeeld worden over beveiligingsincidenten en standaard best-practices.

3.3.6 Praktijk: management van informatiebeveiliging binnen de zorg

Op het gebied van management van informatiebeveiliging binnen de zorg is de literatuur beperkt aanwezig (Appari & Johnson, 2010). Er is dan ook onderzoek nodig die zorgorganisaties helpt bij het implementeren van frameworks of het opzetten van een continuïteitsplanning.

Huisartsenpraktijken zijn erg afhankelijk van het vertrouwen in hun medewerkers bij het gebruiken van IT als het gaat om informatiebeveiliging. Doordat er te weinig kennis is van de mogelijke risico's en benodigde technologische beveiligingsmaatregelen, worden de benodigde informatiebeveiligingsmaatregelen niet serieus genomen (Williams, 2008). 'I have awareness but I don't know the details'. Er is daarom een compleet model van beveiligingsmaatregelen nodig om de medische praktijk te helpen bij het verbeteren van de informatiebeveiliging. Dit model kan ook bijdragen aan de zorgen rondom kosten en tijd die benodigd zijn om goede informatiebeveiliging te implementeren en de maatregelen up-to-date te houden.

Voor het vertrouwen van de patiënt in zijn privacy en de geleverde zorgkwaliteit is informatiebeveiliging van het grootste belang. Zonder vertrouwen in de zorgaanbieder en de gebruikte informatietechnologie zullen de ingevoerde data wellicht niet correct of volledig zijn of zelfs in zijn geheel gewantrouwd worden (D. A. Gritzalis, 1998). Een belangrijk punt wat onthouden moet worden is dat de patiënt op de hoogte wenst te zijn wat er met zijn data gebeurt bij uitwisseling. Dit verhoogt de acceptatie van deze uitwisseling (Whiddett, Hunter, Engelbrecht, & Handy, 2006). Ook zou de patiënt graag willen dat niet alles uit zijn dossier voor iedereen beschikbaar is, voornamelijk in relatie tot de gegevens uit de privésfeer (Jong & Schee, 2006).

Uitwisseling van patiëntinformatie tussen huisartsen wordt wel als nuttig geacht bij huisartsen, alleen de matige kwaliteit van patiëntinformatie in andere dossiers dan die van de eigen praktijk zien de huisartsen nog als belemmering (Ellis, Howard, Dedman, & Hawking, 2011). Tekstanalyse suggereert voornamelijk dat coderingsverschillen hier een belangrijke rol spelen in de kwaliteit van de informatie-uitwisseling tussen de verschillende EPD-systemen van de praktijken. Goede samenwerking in de zorg is noodzakelijk (Hammelburg, Lubbers, & Nauta, 2014), er is echter wel aandacht gewenst op het gebied van regelgeving vanwege de snelle technologische ontwikkelingen, toename van informatiemanagement en toename van beslissingsondersteunende systemen. Waar voor gewaakt moet worden is dat de introductie van nieuwe systemen fouten kan produceren in plaats van reduceren (Ash, Berg, & Coiera, 2004). Uitwisseling van informatie kan de patiëntveiligheid ten goede komen. Maar uitwisseling van gegevens die niet op orde zijn is niet zinvol en kan juist leiden tot meer risico's voor de patiëntveiligheid (Khan, Visscher, & Verheij, 2011).

Er is te zien dat veel artsen zich keren tegen landelijke gegevensuitwisseling omdat het principiële bezwaar vanuit de hippocratische eed te groot is. "Je kunt als huisarts niet meer naar eer en geweten zorgdragen voor veilige informatieopslag als honderdduizenden anderen op enigerlei wijze toegang hebben tot de gegevens." (Pluut, 2010). Mommers (2008) beschrijft dit ook zijn artikel. Hij geeft aan dat door te kiezen voor een relatief 'open' landelijk EPD-systeem de regering weliswaar veel praktische problemen in de invoering en het gebruik voorkomen heeft, maar ook een belangrijk risico van misbruik geïntroduceerd.

In vergelijking met andere landen is het gebruik van elektronische patiëntdossiers in Nederland erg hoog, zo laten Grol, Faber, Braspenning en Timmermans (2007) in hun studie zien. Echter geven zij ook aan dat ICT-mogelijkheden in combinatie met het EPD nog onvoldoende benut worden. Khan, Visscher en Verheij (2011) geven de uitkomsten van een EPDscan die gedaan is in de regio Twente. De EPDscan meet de kwaliteit van de informatie in elektronische patiëntendossiers en geeft daarmee een beeld van de kwaliteit van informatie die kan worden uitgewisseld met andere zorgaanbieders. Daarnaast geeft het rapport weer dat één huisartseninformatiesysteem vaak gebruikt wordt door meerdere huisartsen én assistenten. Het rapport geeft ook aan dat huisartsenpraktijken met diverse externe partijen, waaronder andere huisartsen in de regio (onbekend percentage), huisartsenposten (99%), Fysiotherapeut (19%), Apotheek (95%), Ziekenhuis (87%) en Laboratorium (87%) elektronisch gegevens uitwisselen.

In het werk van Park et al. (W.-S. Park et al., 2010) wordt een studie gedaan bij 5 ziekenhuizen. Er wordt gebruik gemaakt van een informatiebeveiliging checklist die is samengesteld uit internationale standaarden en lokale regels die van toepassing zijn. In de studie wordt het managementsysteem wel gevonden, maar onvoldoende geacht om de privacy van de patiënt en het veilige gebruik van patiëntdossiers te garanderen. Voornamelijk op het gebied van inventarisbeheer en continuïteitsmanagement zijn nog verbeteringen te maken. Ook op het gebied van verhelpen en het opvolgen van beveiligingsincidenten wordt zwak gepresteerd. De studie stelt op de 11 geïdentificeerde gebieden verbeteringen voor en stelt dat het allerbelangrijkste is om de informatiebeveiliging continu te verbeteren en te proberen aan de standaarden te voldoen. Mehraeen, Ayatollahi en Ahmadi (2016) hebben de studie van Park et al. herhaald in 29 universiteitsziekenhuizen, waar net als bij de eerdere studie een gemiddelde score werd behaald. Wat opvalt is dat de IT-managers in deze studie de technische maatregelen veiliger inschatten dan deze waarschijnlijk zijn. Narayana Samy, Ahmad en Ismail (Narayana Samy, Ahmad, & Ismail, 2010) bekijken in één ziekenhuis de aanwezige risico's op het Healthcare Informatie Systeem en stellen hiermee een totaalbeeld op van risico's met bijbehorende prioriteiten, zodat meer inzicht komt van de verschillende bedreigingen op de patiëntgegevens.

Lorence en Churchill (2005) hebben via een survey een negatief verband laten zien tussen de mate waarin patiëntinformatie digitaal wordt gebruikt binnen de organisatie en de adoptie van vereiste beveiligingsmaatregelen. Daarnaast kwam naar voren dat bij het verder digitaliseren, de kans hoger was dat een specifiek persoon werd aangenomen om over de informatiebeveiliging toe te zien. Daarnaast is opgevallen dat er veel verschillende methodes werden gebruikt om beveiligingsmaatregelen te implementeren, waardoor het gebruik van deze methodes tussen zorgaanbieders niet per se tot veiligere data hoeft te leiden.

Rondom informatiebeveiliging is veel interesse. Toch is er nog maar weinig gepubliceerd ten aanzien van de uitdagingen die bij de zorg spelen (Appari & Johnson, 2010).

3.3.7 Praktijk versus eisen

Bij de Nederlandse huisartsenpraktijken is 45% van de huisartsen van buiten de praktijk in staat bij het EPD-systeem van die praktijk te kunnen. Nederland scoort hiermee het hoogst van alle onderzochte landen. Toegang op afstand tot de eigen EPD-systemen is in 32% van de gevallen mogelijk. De mogelijkheden van ICT worden daarom toch nog te weinig benut (Grol et al., 2007)

Artsen vinden de kosten van implementatie van een gedeeld Elektronisch Medisch Dossier en toename in werkdruk nog wel een drempel om rekening mee te houden (Vanlaer, 2015). Bij elektronische informatie-uitwisseling is te zien dat het vertrouwen van zorgverleners in de veiligheid en de betrouwbaarheid van elektronische informatie-uitwisseling afneemt zodra de schaalgrootte van de uitwisseling toeneemt. Zo zijn er vragen over de wijze van uitwisseling en de controle op de rechtmatigheid van toegang tot patiëntgegevens (Ploem et al., 2011). Voornamelijk wordt gevraagd om extra maatregelen om de privacy van de patiënten te kunnen waarborgen. Een voorbeeld van zo'n maatregel is verdere scheiding van diverse rollen in een organisatie. Toegang tot dezelfde systemen hoeft nog niet te betekenen dat er toegang mag zijn tot dezelfde informatie. Daarom is scheiden van toegang noodzakelijk. Er is onderzocht hoe je selectief informatie kan delen, terwijl je niet geautoriseerde toegang minimaliseert. Zhang, Ahn en Chu (2002) hebben hiervoor een framework opgesteld en een proof-of-concept geïmplementeerd.

Op het gebied van zorg IT wordt vaak gekozen om te focussen op het gebruiksgemak en wordt aan beveiliging minder aandacht gegeven. De meest voorkomende fouten zijn dan ook technisch van aard en gaan in op data integriteit en onbeschikbaarheid van applicaties en systemen. Deze informatiebeveiligingsfouten worden vaak niet herkend omdat het medisch personeel vaak workarounds toepast om door te kunnen werken. Niet-technische maatregelen tijdens het ontwikkelproces van deze applicaties en systemen zouden deze fouten veelal kunnen verhelpen (Boyer, 2015). Ook is het mogelijk om via Ground Theory de zorgmedewerkers meer te betrekken bij de ontwikkeling van veilige EPD-systemen en de toegangscontrole beter te laten aansluiten op de werkprocessen en het dagelijks gebruik (Ferreira, Antunes, Chadwick, & Correia, 2010). Goossen (2009) geeft met betrekking tot informatiebeveiliging in zijn artikel "Hoe maak je een EPD en wie heeft er wat aan?" aan dat het EPD-systeem in ieder geval moet verzekeren dat uitsluitend in noodsituaties anderen dan door de patiënten vertrouwde zorgverleners bij de gegevens kunnen. Specifieke eisen en testen komen met betrekking tot dit punt niet voor.

De beperkte resources en tijd binnen de organisatie zorgen ervoor dat bij de beveiligingsstrategie keuzes gemaakt moeten worden. De inventarisatie en evaluatie van bestaande risico's is daarom zeer belangrijk bij het prioriteren van de maatregelen. Dit concept ondersteunt het werken met standaarden en frameworks, omdat organisaties nog wel zelf hun invulling aan de maatregelen moeten geven op basis van de eigen prioriteiten (Coleman, 2004). Ook moet er gelet worden op organisatie overstijgende informatiebeveiliging. Hier zal gelet moeten worden op chronologisch kunnen terughalen van gebeurtenissen over organisaties heen en bijvoorbeeld versiebeheer en auditlogging door diverse systemen heen (Linden, Kalra, Hasman, & Talmon, 2009)
In de studie van Beer en Smits (2005), gedaan bij de GGZ regio Breda, is voor implementatie van informatiebeveiliging het INK-managementmodel gebruikt. Dit model is gebaseerd op zelfevaluatie van de organisatie. Daarnaast worden diverse managementinstrumenten genoemd, zoals een meerjarenplan, standaarden voor interne jaarplannen en verslaglegging, monitors en interne audits. Beoordeling van het bestaande niveau van de informatiebeveiliging wordt volgens het Capability Maturity Model (CMM) gedaan. Met deze methode wordt een duurzame implementatie van informatiebeveiliging in zorgorganisaties beschreven.

Gordon en Loeb (2002) geven in hun artikel een framework hoe beveiliging kostenefficiënt ingericht kan worden. Zo stellen zij dat bedreigingen in verschillende niveaus moeten worden gegroepeerd en dat slechts in een fractie van de verwachte schade veroorzaakt door een bedreiging, moet worden geïnvesteerd. Het optimale investeringsbedrag zou daarbij nooit hoger moeten zijn dan 37% van de verwachte schade bij een incident. Specifiek voor informatiebeveiliging rondom landelijke uitwisseling hebben Huang, Behara en Goo (2014) inzicht gegeven in de financiële aspecten van informatiebeveiliging. Zo laten zij zien dat pas vanaf een bepaald financieel risico maatregelen worden genomen en dat de maatregelen die organisaties nemen meestal te weinig zijn ten aanzien van de risico's die organisaties moeten afdekken. Ze stellen dat er drie vragen zijn rondom informatiebeveiligingsinvesteringen bij bedrijven; 1. De optimale investering in informatiebeveiliging, 2. In welke maatregelen geïnvesteerd moet worden en 3. Hoe wordt deze investering zo efficiënt mogelijk? De onderzoekers zien dat investeringen vaak gemaakt worden alléén om risico's te reduceren, maar dat investeringen in bedrijfsvoordelen op gebieden als het voldoen aan de eisen om aan te sluiten bij landelijke EPD-systemen niet worden meegerekend. Bij grotere zorgbedrijven zijn investeringen die gemaakt worden om risico's te reduceren én gebruik te kunnen maken van additionele voordelen zoals aansluiting op een landelijke infrastructuur relatief kleiner. Bij kleinere organisaties is echter te zien dat ze, door het beperkte budget, onderinvesteren en alleen hun eigen risico's proberen te reduceren.

Rindfleisch (1997) verklaart deze onderinvestering door te stellen dat de implicaties van een kwetsbaarheid op de informatiebeveiliging van patiëntgegevens zo groot kunnen zijn dat zorgaanbieders deze risico's, in tegenstelling tot bijvoorbeeld banken, financieel niet kunnen dragen. Smith en Eloff (Smith & Eloff, 1999) stellen ook dat risicoanalyses binnen de zorg afwijkt van de analyses bij andere organisaties, maar dat er wel geleerd kan worden van de manier waarop deze andere organisaties naar risico's kijken.

Proactief investeren in beveiligingsmaatregelen is een betere keuze dan het maken van reactieve investeringen in verhelpen van de risico's. De kans bestaat hierbij dat er bij proactieve maatregelen wordt overgeïnvesteerd, maar omdat de zorg achterloopt bij de adoptie van IT ten aanzien van de markt, is de kans dat de investering in een maatregel verkeerd wordt ingeschat beduidend lager dan te zien is in de rest van de markt (Juhee & Johnson, 2014). Omdat proactieve investeringen effectiever zijn dan reactieve investeringen, zouden beveiligingsmanagers met name bij de investeringskeuzes rondom deze aspecten moeten aansturen op proactieve investeringen. Brill en Leetz (Brill & Leetz, 2005) geven met hun artikel een methode voor risicoanalyse en kostenanalyse omdat er geen voorbeeld informatiebeveiligingsbeleid is wat op alle organisaties van toepassing is. Deze methode kan helpen bij het uitvoeren van een eigen implementatie van informatiebeveiliging.

De studie van Kwon en Johnson (2014) laat zien dat er drie clusters organisaties zijn aan te wijzen als gekeken wordt naar de compliance van informatiebeveiliging; Leiders, volgers en achterblijvers. Als gekeken wordt naar de implementatie adoptie van beveiligingsmaatregelen is in technisch opzicht geen significant verschil te vinden, maar in niet-technisch opzicht juist wel. Daarnaast laat de studie zien dat bij de volgers vooral de uitvoering van audits zorgt voor verbeterde compliance en bij de leiders, beveiligingstesten door derde partijen en training belangrijke factoren waren voor een hoger niveau van compliance.

In Australie hebben Mahncke en Williams (2014) een onderzoek gedaan naar de mogelijkheid tot implementatie van de ISO/IEC 27014:2013 “Information technology -- Security techniques -- Governance of information security” bij huisartsenpraktijken. Deze ISO-standaard is toepasbaar op organisaties van alle groottes en bied een framework voor het beoordelen en implementeren van governance elementen van informatiebeveiliging. De conclusie van het onderzoek is, dat de standaard toepasbaar is bij huisartsenpraktijken voor het opzetten van een governance framework voor informatiebeveiliging. Er is echter een aanvullend framework nodig om ook de informatiebeveiligingsmaatregelen te managen. Stahl, Doherty en Shaw (2012) geven aan dat er een erg grote consensus bestaat dat management van informatiebeveiliging het sleutelmechanisme is voor effectieve promotie van uitvoering van informatiebeveiligingsmanagement. Of dit op waarheid berust is echter moeilijk te achterhalen, omdat er weinig empirische studies zijn op dit gebied en géén theoretisch inzicht is op het gedrag en de impact van informatiebeveiligingsmaatregelen.

3.3.8 Uitwisseling van patiëntgegevens

Patiënten die ondervraagd zijn over de manier waarop zij bijvoorbeeld lab uitslagen gecommuniceerd kunnen krijgen geven aan dat e-mail ook tot de mogelijkheden mag behoren, maar zijn wel sceptisch over de beveiligingsaspecten (Grayston, Fairhurst, & McKinstry, 2010). Toch geeft een zeer grote meerderheid nog de voorkeur aan het gesprek met de dokter of praktijk, face-to-face of per telefoon, boven het gebruik van nieuwe technologieën voor de communicatie van uitslagen.

Vooral op het gebied van het wereldwijde web is er nog veel nodig op het gebied van beveiliging. Zo moeten er nieuwe diensten ontwikkeld worden om bestaande markten te ondersteunen en trends te volgen. De projecten TRUSTHEALTH en EUROMED-ETS maken het mogelijk in de zorg gebruik te maken van beveiligde datacommunicatie en authenticatie op basis van rol over het wereldwijde web (Bourka et al., 2001). Ook is er meer interlandelijke wetgeving nodig om diensten van derden veilig te kunnen gebruiken. Helaas kan wetgeving de ontwikkelingen op het gebied van beveiliging ook tegenwerken, zo laat Rindfleisch (1997) zien. Hij geeft aan dat de Verenigde Staten de adoptie van goede cryptografische beveiliging door leveranciers van computersystemen en software heeft afgeremd door wetgeving rondom nationale veiligheid en handhaving.

Ook binnen regio’s is het belangrijk dat veilige en goede data uitwisseling plaatsvindt. De meeste artikelen concluderen dat een gebrek aan standaardisatie, problemen met financiën en methodologische verschillen moeten worden overwonnen om verder te komen bij gemeenschappelijke zorg voor de patiënt. Enkele voorbeelden zijn de artikelen van Schabetsberger et al. (2004), Poon et al. (2006) en Riper (2007).

Turan en Palvia (2014) benoemen in hun studie dat zorgen ten aanzien van productiviteit, beveiliging, privacy, kwaliteit, wijzigingen en compliance een snelle implementatie in de weg staan in ontwikkelingslanden. Op lokaal en regionaal niveau lijken er minder barrières te zijn voor het gebruik van elektronische zorgsystemen. Veel van de bezwaren komen naar voren bij elektronische uitwisseling van gegevens, zo laten Zwaanswijk, Verheij, Wiesman en Friele (2011) zien. Ze geven aan dat het Technology Acceptance Model bijdraagt aan de positieve adoptiefactoren, maar de negatieve factoren negeert. Ook de zorgen van de gebruikers zullen moeten worden geadresseerd. Zo vinden patiënten het belangrijk dat ze geïnformeerd blijven en vindt de meerderheid van de patiënten dat het uitwisselen van gegevens niet mag worden gedaan met overheden of zorgverzekeraars (Whiddett et al., 2006).

3.3.9 Aandachts-, verbeterpunten en modellen

Zorgorganisaties als de Landelijke Huisartsen Vereniging geven in hun uitgegeven materialen aan dat een zorgaanbieder zo veel mogelijk gebruik moet maken van ICT en zo veel mogelijk up-to-date moet blijven op dit gebied (Fisscher & van Bemmel, 2015). Artikelen beschrijven veel positieve resultaten die gehaald worden door standaardisatie van IT in de zorg en de procedures daaromheen. Ook bij uitwisseling van informatie is door standaardisatie veel positief resultaat te behalen (H. Park et al., 2015). Zo kan het kwaliteit verhogend, kosten- en tijdbesparend werken (Linthorst, 2006).
Ook bieden organisaties als de LHV trainingen aan specifiek voor informatiebeveiliging. Veel van de artikelen laten zien dat er een positief verband bestaat tussen de kennis van de medewerker en het correcte gebruik van zorgsystemen. Het verder uitbreiden van die kennis door trainingen is dan ook onderdeel van de conclusie in studies van onder andere Warm, Thomas, Heart, Jones en Hawkins-Brown (2009), D'Arcy, Hovav en Galletta (2009) en Zwaanswijk, Verheij, Wiesman en Friele (2011). De studie van Warm, Thomas, Heart, Jones en Hawkins-Brown (2009) toont ook een positief effect aan van de verhoging van IT kennis van de medewerker op de perceptie van beschikbare tijd voor de patiënt. Dit effect is het grootst onder de personen met de minste IT-kennis, wat logisch is omdat medewerkers op een gegeven moment een plafond bereiken als het gaat om hun IT-kennis en -kunde. Arnbak (2015) laat zien dat beveiliging awareness, betrokkenheid en beveiligingscultuur indicatoren een sterk verband hebben met de effectiviteit en het gedrag ten aanzien van informatiebeveiliging.

In het artikel van van der Kamp et al. (2010) worden praktische checklists en andere verwijzingen naar ibgz.nl uitgelicht. Ze geven daarmee een praktische beschrijving om informatiebeveiliging in de huisartsenpraktijk te kunnen uitvoeren onder het motto “gewoon doen”. In de omschrijving wordt een centrale rol gelegd bij de coördinerend assistente, die voldoende kennis van informatiebeveiliging moet bezitten.

Liu, Chung, Chen en Wang (2012) geven een invulling van de beveiliging van netwerkinfrastructuren door de beveiligingsaspecten uit te leggen aan de hand van de HIPAA. Daarnaast worden van enkele technische onderdelen praktische voorbeelden gegeven in het artikel.

Xiao, Hu, Croitoru, Lewis & Dasmahapatra (2010) stellen een meerlaags beveiligingsmodel voor, voor gedistribueerde zorgsystemen. Dit model is een complete uitwerking en lijkt sterk op l-EDP in Nederland en HIE in de UK. Ook Kotulic (Kotulic & Clark, 2004) stelt een informatiebeveiligingsmodel voor. Ze geven hiervoor de theoretische uitwerking, echter hebben ze dit model niet kunnen valideren omdat ze grote moeite hadden om voldoende respondenten te krijgen die hun informatiebeveiligingsbeleid bloot wilden leggen. Er wordt wel het advies gegeven om een sponsor te zoeken in de bedrijven om zo deze gevoelige informatie te kunnen verkrijgen of de opzet van het onderzoek aan te passen zodat deze hogere response oplevert. Voornamelijk lijkt de non-response feedback te zeggen, dat het bedrijfsbeleid is om onderzoeken te weren “omdat het er zo veel zijn”.

Oladimeji, Chung, Jung en Kim (2011) laten zien welke veranderingen nodig zijn binnen de traditionele informatiebeveiliging om te kunnen bewegen naar eHealth. Het gaat hier om de verandering van een voornamelijk centraal georiënteerde infrastructuur rondom netwerken, opslag en gebruiker naar een wereldwijd georiënteerd domein, waarin context specifieke beveiliging en privacy een rol spelen.

Fernández-Alemán, Señor, Lozoya en Toval (2013) laten in hun literatuurreview zien dat er zeer veel literatuur beschikbaar is op het gebied van technische informatiebeveiligingsmaatregelen en uitwerkingen daarvan. Ze geven echter wel aan dat voornamelijk beleid op en uitrol van veilige patiëntdossiersystemen nog onderzocht moet worden.

In het artikel van Vorakulpipat, Siwamogsatham en Kawtrakul (2014) wordt Information Security as a Service aangeraden voor kleinere ziekenhuizen omdat deze met beperkte resources (budget en mensen) toch een zeer hoog beveiligingsniveau moeten behalen. In het artikel wordt een model voorgesteld die zowel op de informatiebeveiligingsaspecten als de aspecten van de bedrijfsvoering ingaat. Ook wordt aangeraden beveiligingsdiensten van externe partijen af te nemen om een voldoende niveau van beschikbaarheid, integriteit en vertrouwelijkheid te kunnen halen.

4 Conclusies

In deze literatuurstudie is een overzicht gegeven van de beschikbare literatuur rondom management van informatiebeveiliging bij elektronische uitwisseling tussen huisartsenpraktijken. De studie is uitgevoerd zoals vooraf aangegeven in het hoofdstuk Methode en in het hoofdstuk Resultaten.

Allereerst is gekeken naar de metadata van de zoekresultaten. In deze data is te zien dat er de afgelopen jaren een sterke toename van het aantal publicaties plaatsvindt. In totaal zijn er 117 artikelen gevonden, tussen 1997 en 2016, die aansluiten op de gegeven zoekcriteria. Van die artikelen is ongeveer de helft gepubliceerd in de afgelopen 5 jaar.
Van alle praktijkgerichte studies is bijna de helft uitgevoerd bij ziekenhuizen. 85% van de praktijkgerichte studies heeft te maken met grotere organisaties of ketens. Slechts 9 praktijkgerichte onderzoeken gingen alleen in op huisartsenpraktijken. Dit waren daarbij de enige kleine organisaties die losstaand besproken werden.

Na het bekijken van de metadata is ingegaan op de inhoud van de gevonden artikelen. Allereerst is opgevallen dat de terminologie niet consistent gebruikt wordt. Zo wordt “Healthcare Information Exchange” gebruikt voor aanduiding van zowel interactie met de patiënt, het elektronisch patientdossiër als de informatietechnologie die de uitwisseling ondersteunt. Ook de scope van termen is vooraf niet altijd uitgelegd. Zo wordt informatietechnologie (IT) in diverse vormen gebruikt. Het kan hier administratief, operationeel, infrastructureel of strategisch zijn.
Andersom is het ook het geval, zo zijn de termen LSP (Landelijk Schakelpunt), EPD (Elekotronisch Patiëntendossier) en EHR (Electronic Health Record) vaak door elkaar gebruikt voor aanduiding van landelijke systemen.

Er zijn diverse artikelen die in inleiding, samenvatting, conclusie en discussie spreken over de Healthcare/ zorgsector. Echter komt in de methode of resultaten naar voren dat interviews zijn afgenomen, onderzoek is gedaan of surveys zijn uitgezet alléén bij managers of IT-personeel van ziekenhuizen. Voorbeelden hiervan zijn de artikelen van Lorence en Churchill (2005) en Gardner, Boyer en Gray (2015).

In het hoofdstuk Resultaten is te vinden dat nieuwe initiatieven voornamelijk effectief zijn waar voldoende (financiele) aanmoediging aanwezig is top-down of voldoende sponsoring bottom-up. Voornamelijk IT Security blijft een aandachtsgebied omdat het tot dusver niet direct zichtbaar financieel bijdraagt.

Onderzoek naar informatiebeveiliging beperkt zich voornamelijk tot grotere organisaties. Veel aandacht is er voor informatiebeveiliging en mogelijke toepassing van regels en normenkaders. Hierin zit een (niet uitgesproken) aanwezigheid van diepgaande IT- en beveiligingsexpertise, die bij kleinere zorgorganisaties niet aanwezig is. Dit suggereert dat informatiebeveiliging bij kleinere organisaties niet haalbaar is vanwege de afwezigheid van deze specifieke kennis en de benodigde financiële middelen. Enkele artikelen gaan zelfs zo ver dat ze stellen dat het voor kleinere organisaties helemaal niet haalbaar is aan alle eisen rondom informatiebeveiliging te voldoen. Artikelen over kleine zorgorganisaties blijven steken bij analyse van regels en normenkader. Compliance en haalbaarheid zijn niet terug te vinden.

Er kan gesteld worden dat de literatuur ten aanzien van de menselijke factoren rondom management van informatiebeveiliging voldoende belicht zijn in de wetenschappelijke literatuur. Er komt hier wel naar voren dat er nog een duidelijke lacune in kennis bij de gebruiker aanwezig is met betrekking tot informatiebeveiliging.

Ten aanzien van de onderzoeksvragen kunnen we het volgende in de literatuur vinden;

1. *Wat is, volgens de wetenschappelijke literatuur, management van informatiebeveiliging binnen de zorgsector?*

Er is onderzoek uitgevoerd naar de eisen aan informatiebeveiliging binnen de zorg. De literatuur hierover is echter niet te generaliseren naar de gehele zorgsector, maar is voornamelijk gericht op de grotere zorgonderneming zoals ziekenhuizen. De artikelen gaan veelal in op de eisen die wetgeving en normen stellen aan informatiebeveiliging en geven hiervoor modellen voor de toepassing. Het management van informatiebeveiliging wordt ook besproken, hier blijft het vaak bij een verwijzing naar wetgeving die is gebruikt bij de ontwikkeling van een door de auteur voorgesteld model.

2. *Wat zegt de literatuur over de eisen die gesteld worden aan informatiebeveiliging binnen de zorg?*

Ten aanzien van de eisen die gesteld worden is de literatuur duidelijk. Er wordt consistent verwezen naar een set wetgeving, standaarden en normen waarop de literatuur modellen voorstelt en implementaties uitwerkt. De literatuur geeft aan dat er veel nationale en internationale regelgeving bestaat rondom informatiebeveiliging in de zorg. Specifiek voor Nederland kan hier gekeken worden naar de Nederlandse wetgeving en normenkaders van NEN. Daarnaast zijn er tal van handreikingen die organisaties hebben uitgegeven om onderdelen van de zorgsector te ondersteunen bij de implementatie van informatiebeveiliging. Er zijn geen “minimale eisen” modellen in de literatuur beschikbaar als het gaat om implementatie en beheersen van informatiebeveiliging.

3. *Wat zegt de literatuur over de eisen aan informatiebeveiliging die gesteld worden bij elektronische gegevensuitwisseling tussen huisartsenpraktijken?*

Specifieker gekeken naar management van informatiebeveiliging bij elektronische uitwisseling tussen huisartsenpraktijken zijn er nog meer eisen te vinden. Er is voor alle gegevensuitwisseling in de zorg wetgeving beschikbaar ten aanzien van informatiebeveiliging. Deze wetgeving spreekt van het maken van “passende technische en organisatorische maatregels”. Zo is veilige communicatie via Goed Beheerde Zorgsystemen via de wetgever gewaarborgd in het geval van het Landelijk Schakel Punt.

4. *Wat zegt de literatuur over de mate en effectiviteit van inrichting van informatiebeveiliging binnen de zorg?*

In praktijksituaties wordt veel gebruik gemaakt van informatietechnologie die beveiligd moet worden. Het overgrote deel van de literatuur stelt dat voornamelijk de kennis (awareness en training) van de gebruiker een belangrijke factor is voor het niveau waarop informatiebeveiliging in de organisatie kan functioneren. Er wordt ook aangegeven dat bij enkele ziekenhuizen, maar voornamelijk bij huisartsen de factoren tijd en kosten belangrijke belemmeringen zijn bij het invoeren van management van informatiebeveiliging.
De literatuur gaat met name in op de zorgen die spelen rondom privacy. Bij ziekenhuizen wordt gevonden dat informatiebeveiliging nog wel verbetert kan worden, echter zijn factoren als tijd en kosten een grote beperking. Bij huisartsen is geen literatuur gevonden over het management van informatiebeveiliging. Wel geven zij aan dat kosten van implementatie van zorg IT nog wel een drempel is.

Als gekeken wordt naar de bestaande literatuur, zal voornamelijk de grootschalige kennisneming van praktische handleidingen zoals de "NHG-PraktijkWijzer – Informatiebeveiliging in de huisartsenpraktijk" en de checklists van van der Kamp et al. (2010) kunnen bijdragen aan een hoger niveau van informatiebeveiliging bij huisartsenpraktijken.

5. *Wat zegt de literatuur over de mate waarin de eisen die gesteld worden aan management van informatiebeveiliging bij huisartsenpraktijken gehaald worden?*

De literatuur laat specifiek zien dat het wellicht niet mogelijk is voor huisartsenpraktijken (en andere kleinere zorgorganisaties) om te voldoen aan alle regels en eisen die gesteld worden aan informatiebeveiliging. Er is echter geen literatuur terug te vinden die specifiek naar deze kleinere zorgorganisaties kijkt. Er kan geconcludeerd worden dat er een gat in de literatuur zit als het gaat om informatiebeveiliging in de zorg, bij kleinere zorgorganisaties.

6. *Wat stelt de literatuur voor als aandachts- of verbeterpunten om te voldoen aan de gestelde eisen?*

Er zijn voor de zorgsector diverse modellen gegeven die kunnen worden toegepast om informatiebeveiliging succesvol binnen een zorgorganisatie te implementeren. Omdat er echter een vraag bestaat of alle eisen wel haalbaar zijn voor kleinere zorgorganisaties, kan gesteld worden dat de literatuur op dit punt niet volledig is.

Probleemstelling; ***Is er voldoende managementcapaciteit beschikbaar bij huisartsenpraktijken voor het goed doen van informatiebeveiliging?***

Als ik kijk naar de gevonden literatuur, kan ik komen tot dezelfde bevinding die in de studie van Appari en Johnson (2010) al vluchtig wordt gegeven. Ze geven aan dat het managen van informatiebeveiligingsrisico's een complex proces is, dat investeringen in organisatorische resources en een aanpak op meerdere fronten vereist. Met de resultaten van dit literatuuronderzoek in de hand, zijn vragen hoe informatiebeveiliging gedaan zou moeten worden te beantwoorden in termen van standaarden (Orel & Bernik, 2013) en gebruik maken van modellen. De vraag, die niet in de literatuur beantwoord wordt, blijft daarbij hoeveel investering daadwerkelijk nodig is. Daarnaast blijft ook de vraag aanwezig hoe ondernemingen, zonder de specifieke kennis of andere benodigde resources het managen van hun informatiebeveiliging nu doen én hoe een hoogstwaarschijnlijk aanwezig verschil tussen de actuele situatie en de vereiste situatie doorlopend verkleind of helemaal overbrugd kan worden door adequate inzet van informatiebeveiliging in de organisatie.

Er kan geconcludeerd worden dat er onvoldoende literatuur beschikbaar is om de probleemstelling voldoende te beantwoorden. Vanuit de literatuur is er wel voldoende materiaal beschikbaar om te kunnen stellen dat het waarschijnlijk is dat huisartsenpraktijken niet aan alle eisen kunnen voldoen. Met name de grote hoeveelheid expertise die vereist is bij het management van informatiebeveiliging valt in de gevonden literatuur op en zal zeker een belemmering vormen voor kleinere organisaties om informatiebeveiliging goed te beheersen. Gezien de noodzaak van goede informatiebeveiliging van zorgsystemen, die steeds meer koppelingen hebben met andere systemen, is er zeker meer onderzoek nodig op dit vlak.

5 Discussie

Dit onderzoek moet in het licht worden gezien van diverse beperkingen;

- Alle zoektermen zijn tussen quotes zijn gezet. Er is hiermee gevraagd om exacte zoekresultaten. Dit kan betekenen dat vergelijkbaar werk is gemist wat net andere bewoordingen heeft gekozen, waar dit met meer zoektermen of zonder quotes andere of meer resultaten had opgeleverd. Ook is een beperking aangebracht in het aantal gebruikte zoekmachines en het aantal bekeken zoekresultaten.
- Het onderzoek is uitgevoerd naar aanleiding van een korte voorlopige analyse en diverse gesprekken met huisartsen, ICT-dienstverleners in de zorg en de studiebegeleider. Dit kan een sturende werking gehad hebben in de gezochte resultaten.
- Ook moet deze literatuurstudie in het licht gezien worden van een in Nederland uitgevoerde studie. Door de opname van Nederlandse zoektermen zal ook de studie bovengemiddeld op de Nederlandse uitvoering van management van informatiebeveiliging in de zorg gericht zijn.
- De screening van artikelen is uitgevoerd door één persoon aan de hand van de vooraf vastgestelde zoekcriteria. Er kunnen, door de enkelvoudige interpretatie van de zoekcriteria, artikelen zijn (af)geselecteerd die bij review door meerdere personen een ander selectieresultaat hadden verkregen.

6 Literatuurlijst

- AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior, 49*, 567-575. doi:http://dx.doi.org/10.1016/j.chb.2015.03.054
- Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: current state of research. *International Journal of Internet & Enterprise Management, 6*(4), 1-1. doi:10.1504/IJIEM.2010.035624
- Arnbak, A. M. (2015). Securing private communications: Protecting private communications security in EU law: fundamental rights, functional value chains and market incentives (pp. 380).
- Ash, J. S., Berg, M., & Coiera, E. (2004). Some Unintended Consequences of Information Technology in Health Care: The Nature of Patient Care Information System-related Errors. *Journal of the American Medical Informatics Association, 11*(2), 104-112. doi:10.1197/jamia.M1471
- Beer, R. d., & Smits, M. (2005). Implementatie van Informatiebeveiliging: een casus in de Gezondheidszorg: EPD-auditor.
- Bonthuis, M. J. (2007). Privacy en het landelijk Elektronisch Patiënten Dossier (EPD) *Een onderzoek naar het Landelijk EPD op basis van een juridisch raamwerk van de Wet Geneeskundige Behandelingsovereenkomst(beroepsgeheim), de Wet Bescherming Persoonsgegevens en de NEN 7510.* .
- Borking, J. J. (2001). Mag het een bitje minder zijn? *Over Privacy Enhancing Technologies (PET) en de juridische basis van hun gebruik*.
- Bourka, N, P., & D, K. (2001). An overview in healthcare information systems security. Stud Health Technol Inform. 2001;84(Pt 2):1242-6.: Biomedical Engineering Laboratory, Department of Electrical and Computer Engineering, NTUA, 15773 Athens, Greece. abourka@biomed.ntua.gr.
- Box, D., & Pottas, D. (2014). A Model for Information Security Compliant Behaviour in the Healthcare Context. *Procedia Technology, 16*(1), 1462-1470.
- Boyer, E. D. (2015). Understanding usability-related information security failures in a healthcare context. *76*.
- Brady, J. W. (2011, 4-7 Jan. 2011). *Securing Health Care: Assessing Factors That Affect HIPAA Security Compliance in Academic Medical Centers.* Paper presented at the System Sciences (HICSS), 2011 44th Hawaii International Conference on.
- Brandhorst, C., J. (2008). Medintel : intelligente elektronische ondersteuning voor huisartsen.
- Brill, R., & Leetz, W. (2005). Security implementations in the healthcare enterprise. *International Congress Series, 1281*, 290-295. doi:http://dx.doi.org/10.1016/j.ics.2005.03.033
- Cazier JA, M. B. (2006). How secure is your information system? An investigation into actual healthcare worker password practices. Perspect Health Inf Manag. 2006 Sep 27;3:8.: Appalachian State University, Boone, North Carolina, USA.
- Cohn, K. H., Berman, J., Chaiken, B., Green, D., Green, M., Morrison, D., & Scherger, J. E. (2009). Engaging Physicians to Adopt Healthcare Information Technology. *Journal of Healthcare Management, 54*(5), 291-300.
- Coleman, J. (2004). Assessing information security risk in healthcare organizations of different scale. *International Congress Series, 1268*, 125-130. doi:http://dx.doi.org/10.1016/j.ics.2004.03.136
- College Bescherming Persoonsgegevens. (2015, 21-9-2015). De meldplicht datalekken in de Wet bescherming persoonsgegevens (Wbp). *Consultatieversie.* Retrieved from https://www.cbpweb.nl/sites/default/files/atoms/files/richtsnoeren_meldplicht_datalekken.pdf

- Cresswell, K. (2016). Evaluation of Implementation of Health IT. Stud Health Technol Inform. 2016;222:206-19.: eHealth Research Group, Usher Institute of Population Health Sciences and Informatics, The University of Edinburgh, Edinburgh, UK.
- D'Arcy, Hovav, & Galletta. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach (March 2009 ed., Vol. Vol. 20, , pp. pp. 79–79). Information Systems Research.
- Daams, C., & Ragetilie, P. (2005). Informatiebeveiliging taak van een zorgadministratie (121 ed., Vol. 121): Vereniging voor Zorgadministratie en Informatie.
- de Mul, M., Adams, S. A., Aspria, M. J. C., Otte-Trojel, E. T., & Bal, R. A. (2013). Hart voor de regio: Patientportalen en regionale ontwikkelingen in Nederland.
- Edlin, J. C. E., & Deshpande, R. P. (2013). Caveats of smartphone applications for the cardiothoracic trainee. *The Journal of Thoracic and Cardiovascular Surgery, 146*(6), 1321-1326. doi:http://dx.doi.org/10.1016/j.jtcvs.2013.08.033
- Ellis, B., Howard, J., Dedman, D., & Hawking, M. (2011). Perceptions on the quality of records received via the GP2GP electronic transfer service: pilot online questionnaire study. *Informatics in Primary Care, 19*(4), 233-240.
- Elrefaey, H., Borycki, E., & Kushniruk, A. (2015). Developing a Security Metrics Scorecard for Healthcare Organizations. *Healthcare Quarterly, 18*(3), 61-68.
- Evers, J., & Barels, E. W. (2014). Business Models & eHealth: Een bedrijfsmatige aanpak in de gezondheidszorg.
- Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á. O., & Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. *Journal of Biomedical Informatics, 46*(3), 541-562. doi:http://dx.doi.org/10.1016/j.jbi.2012.12.003
- Fernando, J. I., & Dawson, L. L. (2009). The health information system security threat lifecycle: An informatics theory. *International Journal of Medical Informatics, 78*(12), 815-826. doi:http://dx.doi.org/10.1016/j.ijmedinf.2009.08.006
- Ferreira, A., Antunes, L., Chadwick, D., & Correia, R. (2010). Grounding information security in healthcare. *International Journal of Medical Informatics, 79*(4), 268-283. doi:http://dx.doi.org/10.1016/j.ijmedinf.2010.01.009
- Fisscher, Y., & van Bemmel, C. (2015). Een eigen praktijk. In Y. Fisscher & C. van Bemmel (Eds.), (pp. 97-104): Bohn Stafleu van Loghum.
- Gardner, J. W., Boyer, K. K., & Gray, J. V. (2015). Operational and strategic information processing: Complementing healthcare IT infrastructure. *Journal of Operations Management, 33*, 123-139. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=100874992&site=ehost-live doi:10.1016/j.jom.2014.11.003
- Gaunt, N. (1998). Installing an appropriate information security policy. *International Journal of Medical Informatics, 49*(1), 131-134. doi:http://dx.doi.org/10.1016/S1386-5056(98)00022-7
- Goldstein, A., & Frank, U. (2016). Components of a multi-perspective modeling method for designing and managing IT security systems. *Information Systems & e-Business Management, 14*(1), 101-140. doi:10.1007/s10257-015-0276-5
- Gomes, R., & Lapao, L. V. (2008). The adoption of IT security standards in a healthcare environment. Studies in health technology and informatics 02/2008; 136:765-70. .
- Goossen, W. (2009). Hoe maak je een EPD en wie heeft er wat aan? *Een praktische verkenning van een complexe taak. Zwolle: Christelijke Hogeschool Windesheim*.
- Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Trans. Inf. Syst. Secur., 5*(4), 438-457. doi:10.1145/581271.581274
- Goroll, A. H., Simon, S. R., Tripathi, M., Ascenzo, C., & Bates, D. W. (2009). Community-wide Implementation of Health Information Technology: The Massachusetts eHealth Collaborative Experience. *Journal of the American Medical Informatics Association, 16*(1), 132-139.

- Goud, R., Riper, H., & Sent, D. (2014). ICT-ondersteuning: de volgende stap in de evolutie van richtlijnen. In J. J. E. Everdingen, D. H. H. Dreesens, J. S. Burgers, J. A. Swinkels, T. A. Barneveld, & T. Weijden (Eds.), *Handboek evidence-based richtlijnontwikkeling: Een leidraad voor de praktijk* (pp. 233-243). Houten: Bohn Stafleu van Loghum.
- Goudswaard, A. N., Veld, C. J., & Dijkstra, R. (2012). Van richtlijnen, de dingen die niet voorbijgaan. *Huisarts en Wetenschap, 53*(1), 51-54. doi:10.1007/s12445-010-0014-7
- Grayston, J., Fairhurst, K., & McKinstry, B. (2010). Using new technologies to deliver test results in primary care: structured interview study of patients? views. *Primary Health Care Research and Development, 11*(2), 142-154.
- Greenhalgh, T., Morris, L., Wyatt, J. C., Thomas, G., & Gunning, K. (2013). Introducing a nationally shared electronic patient record: Case study comparison of Scotland, England, Wales and Northern Ireland. *International Journal of Medical Informatics, 82*(5), e125-e138. doi:http://dx.doi.org/10.1016/j.ijmedinf.2013.01.002
- Gritzalis, D. (1997). A baseline security policy for distributed healthcare information systems. *Computers & Security, 16*(8), 709-719. doi:http://dx.doi.org/10.1016/S0167-4048(97)00009-6
- Gritzalis, D. A. (1998). Enhancing security and improving interoperability in healthcare information systems. *Medical Informatics, 23*(4), 309-323. doi:10.3109/14639239809025367
- Grol, R., Faber, M., Braspenning, J., & Timmermans, A. (2007). De kwaliteit van zorg: huisartsen aan het woord in zeven landen. *Huisarts en Wetenschap, 50*(7), 480-487. doi:10.1007/bf03085224
- Hammelburg, R., Lubbers, W. J., & Nauta, A. (2014). *Veranderende samenwerking in de zorg*: Bohn Stafleu van Loghum.
- Haufe, K., Dzombeta, S., & Brandis, K. (2014). Proposal for a Security Management in Cloud Computing for Health Care. *The Scientific World Journal, 2014*(1).
- Hersh, W., Totten, A., Eden, K., Devine, B., Gorman, P., Kassakian, S., . . . McDonagh, M. S. (2015). Health Information Exchange. Evidence Reports/Technology Assessments, No. 220: Agency for Healthcare Research and Quality (US).
- Hoerbst, A., Hackl, W. O., Blomer, R., & Ammenwerth, E. (2011). The status of IT service management in health care - ITIL® in selected European countries. *BMC Medical Informatics and Decision Making, 11*(1), 1-12. doi:10.1186/1472-6947-11-76
- Huang, C. D., Behara, R. S., & Goo, J. (2014). Optimal information security investment in a Healthcare Information Exchange: An economic analysis. *Decision Support Systems, 61*, 1-11. doi:10.1016/j.dss.2013.10.011
- Imam, A. H., & Hammoud. (2014). Examining the impact of non-technical security management factors on information security management in health informatics. *74*.
- Innis, J., Dryden-Palmer, K., Perreira, T., & Berta, W. (2015). How do health care organizations take on best practices? A scoping literature review. *International Journal of Evidence-Based Healthcare (Lippincott Williams & Wilkins), 13*(4), 254-273. doi:10.1097/XEB.0000000000000049
- Inspectie voor de Gezondheidszorg. (2008). Informatiebeveiliging ziekenhuizen voldoet niet aan de norm: Inspectie voor de Gezondheidszorg.
- Janczewski, L., & Xinli Shi, F. (2002). Development of Information Security Baselines for Healthcare Information Systems in New Zealand. *Computers & Security, 21*(2), 172-192. doi:http://dx.doi.org/10.1016/S0167-4048(02)00212-2
- Jašek, R., Králík, L., & Popelka, M. (2015). ITIL® and Information Security. *AIP Conference Proceedings, 1648*(1), 1-4. doi:10.1063/1.4912775
- Jong-Yi, W., Hsiao-Yun, H., Jen-De, C., Sinkuo, C., Chih-Jaan, T., & Yung-Fu, C. (2015). Attitudes toward inter-hospital electronic patient record exchange: discrepancies among physicians, medical record staff, and patients. *BMC Health Services Research, 15*(1), 1-15. doi:10.1186/s12913-015-0896-y

- Jong, J. d., & Schee, E. v. d. (2006). Ruim een kwart van de bevolking wil gebruik maken van het recht om bepaalde zorgverleners de toegang tot hun elektronisch patiënten dossier te ontzeggen: NIVEL.
- Jongenelen, J., & Ligtvoet, M. (2015). Risico's en oplossingen voor veilig e-mailverkeer in de zorg. Retrieved from https://www.nictiz.nl/publicaties/veilig-omgaan-met-e-mail-in-de-zorg
- Juhee, K., & Johnson, M. E. (2014). Proactive versus reactive security investments in the healthcare sector. *MIS Quarterly, 38*(2), 451-A453.
- Kamman, R. (2015). Opleidingen ICT in de zorg bittere noodzaak. Zorgvisie ICT.
- Kamp, J. v. d., Nabavi, S. M. H., Meer, C. E. v. d., & Heuberger, P. H. J. (2010). De verantwoordelijkheden van de huisarts op het gebied van informatiebeveiliging. *Bijblijven, 26*(9), 36-45. doi:10.1007/s12414-010-0124-y
- Khan, N. A., Visscher, S., & Verheij, R. A. (2011). De kwaliteit van het elektronisch patiëntendossier van huisartsen gemeten: EPDscan regio Twente, eerste meting: NIVEL.
- Koivunen, M., Niemi, A., & Hupli, M. (2015). The use of electronic devices for communication with colleagues and other healthcare professionals - nursing professionals' perspectives. *Journal of Advanced Nursing, 71*(3), 620-631. doi:10.1111/jan.12529
- Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more information security research studies. *Information & Management, 41*(5), 597-607. doi:http://dx.doi.org/10.1016/j.im.2003.08.001
- Kotz, D., Fu, K., Gunter, C., & Rubin, A. (2015). Security for Mobile and Cloud Frontiers in Healthcare. *Communications of the ACM, 58*(8), 21-23. doi:10.1145/2790830
- Lee, A., Moy, L., Kruck, S. E., & Rabang, J. (2015). The Doctor Is In, but Is Academia? Re-Tooling II Education for a New Era in Healthcare. *Journal of Information Systems Education, 25*(4), 275-281.
- Leung, R. (2012). Health information technology and dynamic capabilities. Health Care Manage Rev. 2012 Jan-Mar;37(1):43-53: School of Medicine, Department of Health Management and Informatics, University of Missouri, Columbia, Missouri, USA. rleung@missouri.edu.
- Linden, H. v. d., Kalra, D., Hasman, A., & Talmon, J. (2009). Inter-organizational future proof EHR systems: A review of the security and privacy related issues. *International Journal of Medical Informatics, 78*(3), 141-160. doi:http://dx.doi.org/10.1016/j.ijmedinf.2008.06.013
- Linthorst, H.-J. (2006). De mogelijkheden van ICT in het effectiever en efficiënter functioneren van de diabetesketen.
- Liu, C.-H., Chung, Y.-F., Chen, T.-S., & Wang, S.-D. (2012). The Enhancement of Security in Healthcare Information Systems. *Journal of Medical Systems, 36*(3), 1673-1688. doi:10.1007/s10916-010-9628-3
- Lorence, D. P., & Churchill, R. (2005). Incremental adoption of information security in health-care organizations: implications for document management. *IEEE Transactions on Information Technology in Biomedicine, 9*(2), 169-173. doi:10.1109/TITB.2005.847137
- Lorence, D. P. D. P., & Spink, A. (2004). Healthcare information systems outsourcing. *International Journal of Information Management, 24*(2), 131-145.
- Luzi, D., Pecoraro, F., & Tamburis, O. (2016). Economic Evaluation of Health IT. Stud Health Technol Inform. 2016;222:165-80.: Institute for Research on Population and Social Policies, National Research Council, Italy. Department of Veterinary Medicine, University of Naples Federico II, Italy.
- MacGregor, R. C., Hyland, P. N., & Harvie, C. (2009). Do organisational characteristics explain the differences between drivers of ICT adoption in rural and urban general practices in Australia? *Australasian Journal of Information Systems, 16*(1), 77-97.
- Mahncke, R., & Williams, P. (2014). Interpreting international governance standards for health IT use within general medical practice. Stud Health Technol Inform. 2014;204:86-91.: E-Health Research Group, School of Computer and Security Science, Edith Cowan University, Perth, Australia.

- Mahncke, R. J., & Williams, P. A. H. (2014). Developing and Validating a Healthcare Information Security Governance Framework (12 ed., Vol. 8(2)). Special Issue on e-Health Informatics and Security: e-Journal for Health Informatics
- Malik, H. H., & Hossain, I. T. (2015). Healthcare information technology in medical education – a forgotten focus (Vol. 20). Med Educ Online.
- Mamlin, B. W., & Tierney, W. M. (2016). The Promise of Information and Communication Technology in Healthcare: Extracting Value From the Chaos. *The American Journal of the Medical Sciences, 351*(1), 59-68. doi:http://dx.doi.org/10.1016/j.amjms.2015.10.015
- Markenstein, L. F. (2005). Juridische hordes op de route naar een elektronisch patiëntendossier (EPD) in de zorg; een inventarisatie van de stand van zaken. *Tijdschrift voor Gezondheidsrecht, 29*(5), 320-329. doi:10.1007/bf03056155
- Meersbergen, D. Y. A. v. (2007). RICHTLIJN ONLINE ARTS- PATIENT CONTACT KNMG.
- Mehraeen, E., Ayatollahi, H., & Ahmadi, M. (2016). Health Information Security in Hospitals: the Application of Security Safeguards. *Acta informatica medica : AIM : journal of the Society for Medical Informatics of Bosnia & Herzegovina : casopis Drustva za medicinsku informatiku BiH, 24*(1), 47-50. doi:10.5455/aim.2016.24.47-50
- Mensink, G. (2010). Informatiebeveiliging in de huisartsenpraktijk: een kwestie van maatwerk. *SynthesHis, 9*(1), 20-22. doi:10.1007/s12494-010-0009-6
- Mommers, L. (2008). Het elektronisch patientendossier: de overheid als koppelbaas. Tijdschrift voor Internetrecht.
- Mouw, E. (2012). Data Protection and Privacy in eScience.
- Narayana Samy, G., Ahmad, R., & Ismail, Z. (2010). Security threats categories in healthcare information systems. *Health Informatics Journal, 16*(3), 201-209. doi:10.1177/1460458210377468
- Nederlands Huisartsen Genootschap. (2009a). Informatiebeveiliging in de huisartsenpraktijk *NHG-PraktijkWijzer*.
- Nederlands Huisartsen Genootschap. (2009b). *NHG-PraktijkWijzer Informatiebeveiliging*: Nederlands Huisartsen Genootschap.
- Nouwt, J., & Lucieer, V. (2006). De staat van de privacybescherming van de patient en de client 2005-2006.
- Oladimeji, E. A., Chung, L., Jung, H. T., & Kim, J. (2011). *Managing security and privacy in ubiquitous eHealth information interchange*. Paper presented at the Proceedings of the 5th International Conference on Ubiquitous Information Management and Communication, Seoul, Korea.
- Orel, A., & Bernik, I. (2013). Implementing healthcare information security: standards can help. Stud Health Technol Inform. 2013;186:195-9.: Marand d.o.o., Ljubljana, Slovenia. andrej.orel@marand.si.
- Pai, F.-Y., & Huang, K.-I. (2011). Applying the Technology Acceptance Model to the introduction of healthcare information systems. *Technological Forecasting and Social Change, 78*(4), 650-660. doi:http://dx.doi.org/10.1016/j.techfore.2010.11.007
- Park, H., Lee, S.-i., Hwang, H., Kim, Y., Heo, E.-Y., Kim, J.-W., & Ha, K. (2015). Can a health information exchange save healthcare costs? Evidence from a pilot program in South Korea. *International Journal of Medical Informatics, 84*(9), 658-666. doi:10.1016/j.ijmedinf.2015.05.008
- Park, W.-S., Seo, S.-W., Son, S.-S., Lee, M.-J., Kim, S.-H., Choi, E.-M., . . . Kim, O.-N. (2010). Analysis of Information Security Management Systems at 5 Domestic Hospitals with More than 500 Beds. *Healthcare Informatics Research, 16*(2), 89-99. doi:10.4258/hir.2010.16.2.89
- Park YT, A. K. (2015). Current National Approach to Healthcare ICT Standardization: Focus on Progress in New Zealand. Healthc Inform Res. 2015 Jul;21(3):144-51. doi: 10.4258/hir.2015.21.3.144. Epub 2015 Jul 31.: Research Institute for Health Insurance Review & Assessment, Health Insurance Review & Assessment Service, Seoul, Korea.

Auckland Bioengineering Institute, University of Auckland, Auckland, New Zealand. ; National Institute for Health Innovation, University of Auckland, Auckland, New Zealand.
- Ploem, M. C., Zwaanswijk, M., Wiesman, F. J., Verheij, R. A., Friele, R. D., & Gevers, J. K. M. (2011). *Vertrouwen van zorgverleners in elektronische informatie-uitwisseling en het landelijk EPD: een juridische en sociaal-wetenschappelijke studie naar de positie van zorgverleners* (9789071433825). Retrieved from Amsterdam/Utrecht: http://www.nivel.nl/sites/all/modules/wwwopac/adlib/publicationDetails.php?database=ChoicePublicat&priref=1001999
- Pluut, B. (2010). Het landelijk EPD als blackbox. (45).
- Poon, E. G., Jha, A. K., Christino, M., Honour, M. M., Fernandopulle, R., Middleton, B., . . . Kaushal, R. (2006). Assessing the level of healthcare information technology adoption in the United States: a snapshot. *BMC Medical Informatics and Decision Making, 6*(1), 1-9. doi:10.1186/1472-6947-6-1
- Przybylo, J. A., Wang, A., Loftus, P., Evans, K. H., Chu, I., & Shieh, L. (2014). Smarter hospital communication: Secure smartphone text messaging improves provider satisfaction and perception of efficacy, workflow. *Journal of Hospital Medicine, 9*(9), 573-578. doi:10.1002/jhm.2228
- Renaud, K., & Goucher, W. (2012). Health service employees and information security policies: an uneasy partnership? *Information Management & Computer Security, 20*(4), 296-311. doi:10.1108/09685221211267666
- Rindfleisch, T. C. (1997). Privacy, information technology, and health care. *Commun. ACM, 40*(8), 92-100. doi:10.1145/257874.257896
- Riper, H. (2007). E-mental Health *programmeringsstudie e-mental health*: Trimbos Instituut.
- Safran, C., Jones, P. C., Rind, D., Bush, B., Cytryn, K. N., & Patel, V. L. (1998). Electronic communication and collaboration in a health care practice1. *Artificial Intelligence in Medicine, 12*(2), 137-151. doi:http://dx.doi.org/10.1016/S0933-3657(97)00047-X
- Schabetsberger, T., Gross, E., Haux, R., Lechleitner, G., Pellizzari, T., Schindelwig, K., . . . Wilhelmy, I. (2004). Approaches towards a regional, shared electronic patient record for health care facilities of different health care organizations--IT-strategy and first results. Stud Health Technol Inform. 2004;107(Pt 2):979-82.: University for Health Informatics and Technology, Tyrol Institute for Health Information Systems, Innsruck, Austria. thomas.schabetsberger@umit.at.
- Scott, D., Hallett, C., & Fettiplace, R. (2013). Data-to-text summarisation of patient records: Using computer-generated summaries to access patient histories. *Patient Education and Counseling, 92*(2), 153-159. doi:http://dx.doi.org/10.1016/j.pec.2013.04.019
- Shapiro, J. S., Kannry, J., Kushniruk, A. W., & Kuperman, G. (2007). Emergency Physicians' Perceptions of Health Information Exchange. *Journal of the American Medical Informatics Association, 14*(6), 700-705. doi:http://dx.doi.org/10.1197/jamia.M2507
- Sijm, N. (2008). Onderzoeksrapport LSP - Privacy en security in het Landelijk Schakelpunt.
- Smith, E., & Eloff, J. H. P. (1999). Security in health-care information systems—current trends. *International Journal of Medical Informatics, 54*(1), 39-54. doi:http://dx.doi.org/10.1016/S1386-5056(98)00168-3
- Sohrabi Safa, N., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security, 56*, 70-82. doi:http://dx.doi.org/10.1016/j.cose.2015.10.006
- Stahl, B. C., Doherty, N. F., & Shaw, M. (2012). Information security policies in the UK healthcare sector: a critical evaluation. *Information Systems Journal, 22*(1), 77-94.
- Turan, A. H., & Palvia, P. C. (2014). Critical information technology issues in Turkish healthcare. *Information & Management, 51*(1), 57-68. doi:10.1016/j.im.2013.09.007
- Vanlaer, S. (2015). Ethische grenzen bij het delen van het elektronisch medisch dossier: visie van de zorgverlener.

- Vorakulpipat, C., Siwamogsatham, S., & Kawtrakul, A. (2014). An investigation of information security as a service practice: case study in healthcare. *International Journal of Computer Applications in Technology, 49*(3/4), 365-371. doi:10.1504/IJCAT.2014.062372
- VZVZ. Goed Beheerd Zorgsysteem. Retrieved from https://www.vzvz.nl/page/ICT-leverancier/Het-LSP/Hoe-werkt-het/GBZ
- Warm, D. L., Thomas, S. E., Heard, V. R., Jones, V. J., & Hawkins-Brown, T. M. (2009). Benefits of information technology training to National Health Service staff in Wales. *Learning in Health and Social Care, 8*(1), 70-80.
- Wel, J. v. d. (2005). Waarom de norm voor informatie beveiliging in de zorg NEN 7510 (121 ed., Vol. 121): Vereniging voor Zorgadministratie en Informatie.
- Wel, J. v. d. (2006). Informatiebeveiliging in de zorg.
- Whiddett, R., Hunter, I., Engelbrecht, J., & Handy, J. (2006). Patients' attitudes towards sharing their health information. *International Journal of Medical Informatics, 75*(7), 530-541. doi:http://dx.doi.org/10.1016/j.ijmedinf.2005.08.009
- Williams, P. A. H. (2008). When trust defies common security sense (Vol. September 2008 vol. 14 no. 3 pp. 211-221). Health Informatics Journal.
- Xiao, L., Hu, B., Croitoru, M., Lewis, P., & Dasmahapatra, S. (2010). A knowledgeable security model for distributed health information systems. *Computers & Security, 29*(3), 331-349. doi:http://dx.doi.org/10.1016/j.cose.2009.08.002
- Yang, J.-J., Li, J., Mulder, J., Wang, Y., Chen, S., Wu, H., . . . Pan, H. (2015). Emerging information technologies for enhanced healthcare. *Computers in Industry, 69*, 3-11. doi:10.1016/j.compind.2015.01.012
- Yang, T.-H., Ku, C.-Y., & Liu, M.-N. (2016). An integrated system for information security management with the unified framework. *Journal of Risk Research, 19*(1), 21-41. doi:10.1080/13669877.2014.940593
- Zhang, L., Ahn, G.-J., & Chu, B.-T. (2002). *A role-based delegation framework for healthcare information systems*. Paper presented at the Proceedings of the seventh ACM symposium on Access control models and technologies, Monterey, California, USA.
- Zwaanswijk, M., Verheij, R. A., Wiesman, F. J., & Friele, R. D. (2011). Benefits and problems of electronic information exchange as perceived by health care professionals: an interview study. *BMC Health Services Research, 11*(1), 256-265. doi:10.1186/1472-6963-11-256