Een veilig EPD?

Jan Michels, Niels Braakensiek, Paul van Poecke

9 juni 2008

Inhoudsopgave

1 Inleiding

Nederland is bezig met het invoeren van een landelijk systeem voor de uitwisseling van digitale patiënten gegevens. Het beoogde doel is dat gegevens makkelijker toegankelijk moeten worden voor mensen die betrokken zijn bij het verlenen van zorg. De hoop is dat daardoor de kwaliteit van de zorg beter wordt en de prijs van de zorg lager. Grootschalige digitalisering van patiënten dossiers en ontsluiting van die dossiers via het internet beloofd veel voordeel op te leveren voor alle betrokkenen in de zorg. Het brengt ook risico's met zich mee. Toegang tot het landelijk EPD betekent toegang tot een enorme hoeveelheid digitaal opgeslagen gegevens over patiënten. Deze zijn, doordat ze praktisch gestructureerd opgeslagen zijn, goed doorzoekbaar en daardoor heel geschikt om gebruikt of misbruikt te worden. Dit betekent dat het potentiëel voor goed toeneemt maar het potentieel voor kwaad ook. Het is nu dus meer dan ooit van belang dat de beveiliging van patiëntengegevens tegen onbevoegde toegang goed geregeld is. Dit is niet alleen een belang van medici of automatiseerders, maar meer nog een belang van alle Nederlanders. In dit stuk proberen we een antwoord te geven op de volgende vraag:

> Sluit de manier waarop er door zorgverleners in hun dagelijkse praktijk wordt omgegaan met hun informatiesystemen aan bij de veiligheidseisen die er gesteld worden aan de informatiesystemen en de omgang met die systemen?

2 Theoretisch Kader

EPD/AORTA Met EPD duiden we electronische patiëntendossiers in het algemeen aan. Als we het hebben over het systeem dat landelijke uitwisseling van electronische patiëntendossiers mogelijk moet maken hebben we het over het landelijke EPD. In Nederland wordt de invoering van het landelijk EPD gecoördineerd door het NICTIZ [5] (Nationale knooppunt voor ICT in de Zorg). Zij zijn verantwoordelijk voor het ontwerpen van de infrastructuur en het toezicht op de invoering. De infrastructuur die in nederland gebouwd wordt heet AORTA. We kunnen voor wat betreft de structuur van het landelijke EPD de volgende belangrijke onderdelen onderscheiden:

- Het LSP (Landelijke Schakelpunt).
- De informatiesystemen van de zorgverleners [5].

Als er een vraag binnenkomt van een zorgverlener bij het LSP, dan controleert deze of de betreffende zorgverlener wel geregistreerd staat als zorgverlener in het UZI-register. Verder wordt er gecontroleerd of het Burger Service Nummer (BSN) dat opgegeven is wel overeenkomt met het nummer van de patiënt waarover informatie opgevraagd wordt. Als dit allemaal in orde is dan kijkt het Landelijk Schakelpunt welke informatie er over die patiënt voor deze

zorgverlener beschikbaar is en laat dat zien aan de vragende zorgverlener. Een patiënt kan vastleggen dat bepaalde informatie alleen zichtbaar mag zijn voor bepaalde soorten zorgverleners.[whitepaper Ringholm instituut]

Veiligheid Wij hebben het in het kader van dit onderzoek over veiligheid van informatie als we het hebben over de bescherming van informatie tegen toegang door onbevoegden. Veiligheid wordt over het algemeen breder gedefinierd[1, 3]. Wij kiezen er voor om ons te richten op mogelijke problemen bij de bescherming van gegevens tegen ongeoorloofde inzage. De verplichting om patiëntengegevens te beschermen tegen ongeoorloofde inzage komt in Nederland onder andere voort uit de WBP (Wet Bescherming Persoonsgegevens) en indirect uit de WGBO (Wet op de Geneeskundige Behandelings Overeenkomst)[1, p.5]. Er is door het ministerie van Economische zaken en het Nederlands Normalisatie Instituut een norm opgesteld die geldt voor informatiebeveiliging in de medische sector. Deze norm bestaat uit een aantal delen. Het algemene deel dat geldt voor alle verschillende zorgverleners is de NEN7510 7510 norm. De NEN7510 norm bespreekt expliciet welke dimensies zij onderkent in het begrip veiligheid [1, p.6-8]. Uit wat zij daar presenteert gebruiken wij alleen het onderdeel over vertrouwelijkheid. Het programma van eisen dat het NICTIZ stelt aan informatiesystemen van zorgverleners (PvE GBZ) bespreekt niet expliciet wat ze onder veiligheid verstaat maar ze bevat wel paragrafen die gaan over beveiliging van gegevens tegen ongeoorloofde inzage. [4, 4.2, 4.20, 5.3, 6.4]

Eisen en Normen

De NEN7510 en NEN7511 normen zijn gemaakt om het niveau van de informatiebeveiliging te bevorderen. De NEN7510 is het algemene deel. De andere onderdelen (7511 1-3) zijn toegespitst op verschillende vormen van zorgverlenende instellingen [2]. Een eenmanspraktijk moet de regels uit NEN7510 op een andere manier in de praktijk brengen dan een ziekenhuis met honderden medewerkers. Normen 7511 1-3 zijn gemaakt om te helpen bij de implementatie van NEN 7510. De norm geeft zorgverleners en ook IT dienstverleners een middel om zicht te krijgen op de kwaliteit van hun informatiebeveiliging [1, p.7-8]. Door hun informatiebeveiliging zo in te richten dat ze voldoet aan de norm kunnen zorgverleners er vertrouwen in hebben dat hun informatiebeveiliging in orde is. Dat is tenminste het idee. Of dit ook daadwerkelijk het geval is hangt natuurlijk af van de kwaliteit van de norm. Wij gaan in het kader van dit onderzoek niet expliciet in op de kwaliteit van de NEN 7510 norm. Belangrijk is het nog om op te merken dat de NEN7510 norm een algemene norm is voor informatiebeveiliging in de zorg. Zij geldt dus ook voor informatiesystemen van zorgverleners die nog niet op het landelijke EPD zijn aangesloten.

Het programma van eisen voor een Goed Beheerd Zorgsysteem is een set eisen die gesteld worden aan een informatiesysteem van een zorgverlener als voorwaarde om aangesloten te mogen worden op het LSP. Een deel van die

eisen gaat over veiligheid, maar het meeste niet. De eisen worden gesteld in de vorm van eisen aan functionaliteit die het systeem moet hebben. Er wordt van uitgegaan dat het zorgsysteem al voldoet aan die normen die gesteld worden door de NEN7510 norm en door wetten als de WGBO en de WBP.

3 Methode

Onze methode is een recept dat bestaat uit 5 stappen.

1. In de eerste stap maken we een selectie van punten uit de NEN7510 norm en een selectie van eisen uit het PvE GBZ die we belangrijk vinden voor de veiligheid als vertrouwelijkheid. (Deze normen zijn te vinden in de tabel in de bijlage.)

2. In de tweede stap maken we een vragenlijst voor zorgverleners waarin we een aantal soorten vragen opnemen:

   - Vragen die direct vragen naar het voldoen aan normen en voorschriften.
   - Vragen die vragen naar ondermijnend gedrag. Ondermijnend gedrag is gedrag dat de effectiviteit van beveiligingsmaatregelen teniet doet.
   - Vragen die gaan over het algemene informatiebeveiligings klimaat/beleid in de organisatie.
   - Preselectie vragen die er voor zorgen dat we de andere vragen beter kunnen interpreteren.

3. In de derde stap verzamelen we e-mail adressen van zorgverleners en versturen we een e-mail aan zorgverleners met het verzoek om onze online vragenlijst in te vullen.

4. In de vierde stap trekken we conclusies over de individuele respondenten.

   We hebben zoals gezegd drie soorten vragen die op hun eigen manier iets zeggen over de informatieveiligheid binnen een organisatie (één soort vraag gaat niet over de veiligheid maar test op toepasselijkheid van andere vragen). We hebben een tabel gemaakt met daarin voor de verschillende vragen de normen waar ze aan verbonden zijn. Uit die tabel kunnen we met de antwoorden in de hand bepalen of:

   a) Voldaan wordt aan de normen.
   b) Er sprake is van ondermijning van eventueel wel nageleefde normen.

   We hebben eerder, in het kader van een presentatie, een poging gedaan om de betekenis van een aantal normen wat concreter te maken door een aantal scenario's te bedenken waarin er dreigt iets mis te gaan met de informatieveiligheid. We hebben daarbij normen gezocht in de documenten die gebruikt wordt om deze problemen te ondervangen. In de conclusie zullen we hierop ook kort terugkomen als daar aanleiding toe is.

5. In de vijfde stap kijken we of we op basis van de aantallen antwoorden en de verdeling van de antwoorden een iets algemenere conclusie kunnen trekken en een antwoord kunnen geven op onze vraag.

   > Sluit de manier waarop er door zorgverleners in hun dagelijkse praktijk wordt omgegaan met hun informatiesystemen aan bij de veiligheidseisen die er gesteld worden aan de informatiesystemen die door de zorgverleners gebruikt worden?

4 Resultaten

- 35 verzoeken verstuurd met verzoek de online vragenlijst in te vullen.
- 5 reacties.

We ordenen de resultaten op twee manieren. In de eerste 5 tabellen worden de totalen per vraag per antwoord weergegeven. In de laatste tabel worden de totalen per respondent weergegeven.

Totalen per vraag?

Onderstaand ziet u een versie van de vragenlijst zoals die online te vinden is\was, onder de mogelijke antwoorden ziet u het aantal keer dat dat antwoord is gegeven.

Vraag	Zelf	Uitbesteed	Geen Idee	N.V.T.
Heeft uw organisatie een beleid voor de beveiliging van patiëntgegevens?	4	1	0	0
Is er één persoon of afdeling verantwoordelijk voor de beveiliging van patiëntgegevens?	2	3	0	0
Zo nee, is er een heldere en expliciete verdeling van deel verantwoordelijkheden?	3	1	0	1
Is er binnen uw organisatie een inventarisatie en analyse gemaakt van de mogelijke veiligheid-srisico's?	1	4	0	0
Zijn alle mensen of afdelingen die gevolgen zullen ondervinden van het informatiebeveiligingsbeleid betrokken bij het nemen van beslissingen?	3	1	1	0
Wordt er regelmatig, vaker dan 1 keer per jaar, overlegd door de mensen die betrokken zijn bij het nemen van beslissingen over het beveiligings-beleid?	2	3	0	0
Wordt het personeel ingelicht over maatregelen om de informatie te beveiligen?	4	1	0	0
Wordt er met enige regelmaat gecontroleerd of men zich aan de voorschriften houdt?	2	1	0	2
Wordt met enige regelmaat geëvalueerd of het beleid de informatiebeveiliging ook verbeterd?	1	4	0	0
	Zelf	Uitbesteed	Geen Idee	N.V.T.
Heeft uw organisatie zelf een informatiebeveiliging-sbeleid ontwikkeld of is dat uitbesteed?	2	2	1	0

Vraag	Zelf	Uitbesteed	Geen Idee	N.V.T.	
Zijn de patiëntgegevens al digitaal opgeslagen in uw organisatie? (d.w.z. is er al een electronisch patiënten dossier (EPD)?)		5	0	0	0
Bent u al op de een of andere manier aangesloten op het landelijk EPD?		1	4	0	0
Zijn er al wijzigingen in procedures in verband met de aansluiting van uw EPD aan het landelijke EPD?		2	2	1	0
	0-6	6-12	12-18	18-24	24+
Hoeveel maanden schat u dat het nog zal duren voordat u volledig bent aangesloten op het landelijk EPD?	2	0	1	0	2

Vraag	Zelf	Uitbesteed	Geen Idee	N.V.T.
Zijn er mensen van buiten uw organisatie die toegang hebben tot uw patiëntgegevens?	1	4	0	0
Zijn er juridische maatregelen genomen om te zorgen dat deze mensen geen misbruik maken van de informatie waartoe ze toegang hebben?	1	1	0	3
Heeft u technische maatregelen genomen om te zorgen dat gebruikers geen misbruik kunnen maken van de informatie waartoe ze toegang hebben? (onmogelijk maken van gebruik van usb-sticks bijvoorbeeld)	3	1	0	1
Moeten medewerkers binnen uw organisatie die toegang hebben tot patiëntgegevens zoiets als een geheimhoudingsverklaring tekenen?	4	1	0	0
Is er een procedure die ervoor zorgt dat vertrekkende medewerkers geen toegang meer hebben tot patiëntgegevens?	4	1	0	0

Vraag	Zelf	Uitbesteed	Geen Idee	N.V.T.
Is de toegang tot patiëntgegevens op de een of andere manier beveiligd met een autorisatie procedure?	4	1	0	0
Maakt u gebruik van een wachtwoord/gebruikersnaam combinatie?	4	1	0	0
Maakt u gebruik van een smartcard/uzi-pas systeem?	2	3	0	0
Maakt u gebruik van biometrie? (irisscan of vingerafdruk)	0	5	0	0
Hebben alle medewerkers toegang tot alle patiëntgegevens?	4	1	0	0
Zijn er medewerkers die toegang hebben tot slechts een deel van de patiëntgegevens?	1	4	0	0
Is er een duidelijke officieel omschreven manier om te bepalen wie wel en wie geen toegang krijgt?	2	1	0	2
Delen werknemers wel eens een pas/wachtwoord?	3	2	0	0
Wordt er wel eens informatie opgevraagd met de autorisatie-gegevens van een collega?	1	4	0	0

Vraag	Zelf	Uitbesteed	Geen Idee	N.V.T.
Regelt u het beheer van de servers met patiëntgegevens zelf?	1	3	0	1
	Ja	Nee	Geen Idee	N.V.T.
Zijn er toegangsbeperkingen voor de ruimten waar de servers met patiënten gegevens zich bevinden?	2	1	1	1

Totalen per respondent. We hebben voor iedere respondent geteld aan hoeveel normen ze voldoen, aan hoeveel normen ze niet voldoen en in hoeveel gevallen ze ondermijnend gedrag vertonen. De zo verkregen getallen vindt u in onderstaande tabel.

Resp.	Voldaan	Niet Voldaan	Ondermijnend	Commentaar
1	1	9	3	Misschien niet bij de juiste persoon in de organisatie terecht gekomen. Dat de persoon in kwestie niet weet of het ontwikkelen van het informatiebeveiligingsbeleid is uitbesteed of zelf ter hand genomen wordt lijkt hier op te wijzen.
2	9	1	3	
3	8	1	1	Is al op de een of andere manier aan landelijk EPD aangesloten
4	7	2	1	
5	9	0	1	

5 Discussie

5.1 Haken en ogen aan de methode en de uitvoering Er zijn nogal wat problemen met de manier waarop we dit onderzoek heben opgezet en uitgevoerd. Hieronder een selectie.

Grote verschillen tussen de respondenten. We hebben in ons onderzoek geen onderscheid gemaakt tussen het soort zorgverlener, en dat betekent concreet dat er grotere praktijken, en zelfs een gezondheidscentrum, gevraagd is te reageren, maar ook eenmanspraktijken van huisartsen. We kunnen ons voorstellen dat dat van invloed is op de gegeven antwoorden. Een gezondheidscentrum heeft meer faciliteiten en waarschijnlijk een automatiseringsafdeling en een manager die overzicht heeft over het informatiebeveiligings beleid. Een huisarts, die alles zelf moet regelen en waarschijnlijk het meeste uitbesteed, heeft misschien minder zicht op bepaalde details. Daar staat tegenover dat die huisarts minder mensen hoeft te controleren of te informeren. De verschillen tussen verschillende zorgverlenende organisaties zijn zo groot en zo relevant voor het informatieveiligheidsbeleid van de organisaties dat het de volgende keer beter is om wel onderscheid te maken in het onderzoek of het onderzoek te beperken tot een soort zorgverlener.

NEN zoals gebruikt niet toetsbaar. Wij hebben vragen gesteld en concluderen op grond van de antwoorden of een organisatie al dan niet voldoet aan de normen die voor ons de basis voor die vragen waren. Opgemerkt moet

worden dat in de NEN7510 norm expliciet gezegd wordt dat de norm zoals die in dat document opgesteld is niet toetsbaar is zonder gebruik te maken van de implementatievoorschriften [1, p.5]. We hebben desondanks toch met NEN7510 gewerkt omdat we ons niet gebonden voelen aan de normen die het NNI aanhoud voor toetsbaarheid en omdat we in de resultaten van de enquête niet meer kunnen onderscheiden naar soort zorgverlener.

Bespreking van de verbinding tussen de vragen en de eisen. Bespreking van de betekenis van antwoorden op vragen gebeurt in de daarvoor gemaakte tabel. Voor zover die verbinding toelichting nodig heeft gebeurt dat bij het commentaar in die tabel.

Mogelijkheid dat een persoon meerdere keren gereageerd heeft. Het online vragenformulier waarvan wij gebruik hebben gemaakt is niet beveiligd met een gebruikersnaam en een wachtwoord. Daardoor is het mogelijk dat iemand meerdere keren een reactie instuurt of zelfs dat er mensen per ongeluk bij het vragenformulier uitkomen en een reactie insturen die nergens op gebaseerd is. De vragenlijst is wel beveiligd met een cookie die voorkomt dat een lijst meermaals door dezelfde persoon wordt ingevuld(mits deze persoon de cookie niet verwijdert). We realiseren ons dat we hiermee de resultaten principieel onbetrouwbaar hebben gemaakt. We waren bezig met een betere versie, maar omdat we al erg vertraagd waren met het versturen van de verzoeken en het openstellen van de vragenlijst hebben we besloten dat het beter was om resultaten te krijgen die problematisch zijn dan helemaal geen resultaten. De antwoorden zijn echter allemaal afkomstig van verschillende IP-adressen, wat waarschijnlijk betekent dat alle respondenten de lijst slechts eenmaal ingevult hebben.

Sociaal wenselijke antwoorden. We vragen ons af in hoeverre er bij de beantwoording van vragen 27 en 28 eerlijk geantwoord is. We hebben geen vragen ingebouwd die ons die informatie zouden kunnen geven omdat we geen idee hadden hoe we dat hadden moeten doen. Dit is duidelijk een nadeel van de vragenlijst t.o.v. een interview. Wij verwachten dat we in een interview beter in hadden kunnen schatten of er een sociaal wenselijk antwoord gegeven wordt en in een interview kan je doorvragen als je ergens aan twijfelt.

5.2 Beoordeling van bruikbaarheid van de resultaten. We kunnen op basis van de reacties onze onderzoeksvraag beantwoorden voor de zorgverleners die gereageerd hebben. D.w.z. als we er van uitgaan dat hun antwoorden een getrouwe weergave zijn van de situatie in hun organisatie.

We kunnen op basis van deze resultaten onze vraag niet beantwoorden voor enige groep groter dan de vijf zorgverleners die gereageerd hebben. Het aantal reacties is te klein. Het is in alle gevallen een riskante kwestie om op basis van een eindig aantal gevallen tot een algemene conclusie te komen maar met zo weinig basis is het wel erg gevoelig voor vreemde afwijkingen. Voorbeeld: Als er in heel nederland maar één zorgverlener is die aan geen van de normen

voldoet dan zou die ene 20% van de zorgverleners vertegenwoordigen in ons onderzoek. Afwijkende gevallen kunnen altijd wel wat verwarring veroorzaken maar hebben een veel minder sterke invloed en zijn veel makkelijker te herkennen als het aantal reacties groter is.

6 Conclusie

Respondent nummer 1 heeft ofwel een groot probleem met de informatie beveiliging in zijn organisatie of de vragenlijst is beantwoord door de verkeerde persoon in die organisatie (zie commentaar in antwoordinterpretatietabel).

De andere respondenten voldoen aan de meeste normen en lijken in ieder geval een serieuze poging te wagen de informatie in hun beheer goed te beveiligen. Uit het feit dat aan de meeste normen voldaan wordt trekken wij de conclusie dat de aansluiting van hun praktijk aan de eisen die gesteld worden vrij goed is. Het valt wel op dat er bij allemaal wel sprake is van enig ondermijnend gedrag. Het belangrijkste, in onze ogen, is wel de afwezigheid (behalve bij respondent 5) van een risico analyse. Je zou je kunnen afvragen waarop het beleid dat gemaakt is gebaseerd is.

7 Literatuur

Referenties

[1] Nederlands Normalisatie Instituut.
NEN7510 (nl), 2004.

[2] Nederlands Normalisatie Instituut.
Handboek NEN7510, 2005.

[3] mr. Sjaak Nouwt.
Beveiliging van het epd rapportage van het juridisch laboratorium.
Technical report, ZonMW, 2002.

[4] NICTIZ.
Programma van eisen voor een goed beheerd zorgsysteem, 2007.

[5] René Spronk.
Aorta, the dutch national infrastructure.
http://www.ringholm.de/docs/00980_en.htm, 2007.

A Bijlage

Antwoordinterpretatietabel

		PvE	NEN	Commentaar
1	Heeft uw organisatie een beleid voor de beveiliging van patiëntgegevens?		5.1.1	Als er geen beleid is dan voldoet de organisatie niet aan deze norm en het laat zien dat er nog veel te doen is. Men is nog niet eens begonnen met het beveiligen van de informatie. Of de informatie ook daadwerkelijk in gevaar is hangt af of de ad hoc maatregelen die er eventueel genomen zijn toch zoden aan de dijk zetten. Geen idee duid er waarschijnlijk op dat de vragenlijst bij de verkeerde persoon in de organisatie is terecht gekomen. **norm**
2	Is er één persoon of afdeling verantwoordelijk voor de beveiliging van patiëntgegevens?		6	De NEN norm vraagt om een heldere verdeling van de verantwoordelijkheden voor het uitvoeren van het beleid. Als die er niet zijn dan ondermijnd dat een mogelijk wel geformuleerd beleid. **norm/ondermijnend**
3	Zo nee, is er dan een heldere en expliciete verdeling van deelverantwoordelijkheden?		6	
4	Is er binnen uw organisatie een inventarisatie en analyse gemaakt van de mogelijke veiligheidsrisico's?			Deze analyse wordt niet geëist maar in het handboek bij de NEN norm wordt het wel genoemd als een essentieel onderdeel om tot een beleid te komen. Dat lijkt ons ook. Als je niet weet waar je op aan gaat sturen lijkt het moeilijk effectief beleid te maken. Als er geen analyse is dan kun je je vraagtekens stellen bij de inhoud van het beleid. **ondermijnend**
5	Zijn alle mensen of afdelingen die gevolgen zullen ondervinden van het informatiebeveiligingsbeleid betrokken bij het nemen van beslissingen?			Draagvlak is erg belangrijk voor de kwaliteit van de uitvoering en de bereidheid van medewerkers en afdelingen om zich in te zetten. Geen heldere eis over gesteld **ondermijnend**
6	Wordt er regelmatig, vaker dan 1 keer per jaar, overlegd door de mensen die betrokken zijn bij het nemen van beslissingen over het beveiligingsbeleid?			
7	Wordt het personeel ingelicht over maatregelen om de informatie te beveiligen?		5.1.1 8.2.1 8.2.2	Draagvlak is erg belangrijk voor de kwaliteit van de uitvoering en de bereidheid van medewerkers en afdelingen om zich in te zetten. Geen heldere eis over gesteld **norm**

		PvE	NEN	Commentaar
8	Wordt er met enige regelmaat gecontroleerd of men zich aan de voorschriften houdt?		5.1.2	Als er niet gecontroleerd wordt op naleving dan hoeft dat niet ernstig te zijn. Een huisarts die zichzelf niet controleert is geen ernstige misstand maar een ziekenhuis waar geen zicht is op de vraag of mensen zich aan de regels houden lijkt zijn eigen beleid niet serieus te nemen. **norm**
9	Wordt met enige regelmaat geëvalueerd of het beleid de informatiebeveiliging ook verbeterd?		5.1.2 6.1.7	Als er niet geëvalueerd wordt hoeft dat niet te betekenen dat informatie in die organisatie niet goed beveiligd is. **norm**
10	Heeft uw organisatie zelf een informatiebeveiligingsbeleid ontwikkeld of is dat uitbesteed?			Deze vraag test of bepaalde (de meeste) vragen wel zinvol gesteld kunnen worden aan de mensen binnen de organisatie. **context**
11	Zijn de patiëntgegevens al digitaal opgeslagen in uw organisatie? (d.w.z. is er al een electronisch patiënten dossier (EPD)			Test of deze organisatie wel behoort tot de doelgroep van het onderzoek. **context**
12	Bent u al op de een of andere manier aangesloten op het landelijk EPD?			Kijkt of de organisatie al zou moeten voldoen aan de eisen in het PvE GBZ. **context**
13	Zijn er al wijzigingen in procedures in verband met de aansluiting van uw EPD aan het landelijke EPD?			Eigenlijk onduidelijk wat we uit deze vraag hopen te leren.
14	Hoeveel maanden schat u dat het nog zal duren voordat u volledig bent aangesloten op het landelijk EPD?			**context**
15	Zijn er mensen van buiten uw organisatie die toegang hebben tot uw patiëntgegevens?			Hoort bij volgende vraag. **context**
16	Zijn er juridische maatregelen genomen om te zorgen dat deze mensen geen misbruik maken van de informatie waartoe ze toegang hebben?		8.1.2 tm 8.1.4	**norm**
17	Heeft u technische maatregelen genomen om te zorgen dat gebruikers geen misbruik kunnen maken van de informatie waartoe ze toegang hebben? (onmogelijk maken van gebruik van usb-sticks bijvoorbeeld)	5.3.e04	9.3.2.	Slecht geformuleerde vraag. Leert ons niets. Diffuus. Wel een belangrijke norm dus jammer dat we dit niet eerder hebben opgemerkt.
18	Moeten medewerkers binnen uw organisatie die toegang hebben tot patiëntgegevens zoiets als een geheimhoudingsverklaring tekenen?		8.1.4	**norm**

		PvE	NEN	Commentaar
19	Is er een procedure die er voor zorgt dat vertrekkende medewerkers geen toegang meer hebben tot patiëntgegevens?		8.3.4	**norm**
20	Is de toegang tot patiëntgegevens op de een of andere manier beveiligd met een autorisatie procedure?	4.2/4.2.1	11.3	**norm**
21	Maakt u gebruik van een wachtwoord/gebruikersnaam combinatie?	4.2.1		Om vast te stellen fwelk technische niveau van beveiliging er aanwezig is in de organisatie. norm Zegt alleen dat er een van deze methoden gebruikt dient te worden of meer afhankelijk van het soort informatie waar het om gaat. In geval van aansluiting aan het landelijke EPD is zowel wachtwoord als UZI-card een eis **norm/context**
22	Maakt u gebruik van een smartcard/uzi-pas systeem?	4.2.1.		
23	Maakt u gebruik van biometrie? (irisscan of vingerafdruk)	4.2.1		
24	Hebben alle medewerkers toegang tot alle patiëntgegevens?			Verminderd het belang van autorisatie en het negatieve effect van ondermijning door delen van passen of wachtwoorden. **context**
25	Zijn er medewerkers die toegang hebben tot slechts een deel van de patiëntgegevens?			Maakt zorgvuldig omgaan met restricties belangrijker. **context**
26	Is er een duidelijke officieel omschreven manier om te bepalen wie wel en wie geen toegang krijgt?		(11.1.1)	Zo niet dan lijkt er sprake van willekeur te zijn. Het kan ook zijn dat de normen die wel degelijk gehanteerd worden nog niet expliciet gemaakt zijn. Dit is een onderdeel van het veiligheidsbeleid. ondermijnend. De vraag vraagt de regels die bepalen of iemand al dan niet toegang krijgt en de norm is niet zo expliciet. Daarom beschouwen we het niet hebben van zo'n protocol/zulke regels niet als overtreding van de norm maar als ondermijnend voor de effectiviteit van de norm.
27	Delen werknemers wel eens een pas/wachtwoord?			Kan ondermijnend zijn voor autorisatie regime. Hoeft niet zo te zijn als het pas delen alleen gebeurt door mensen met dezelfde rechten. Is wel altijd funest voor de kwaliteit van de logs. **ondermijnend**
28	Wordt er wel eens informatie opgevraagd met de autorisatiegegevens van een collega?			

		PvE	NEN	Commentaar
29	Regelt u het beheer van de servers met patiëntgegevens zelf?.			hoort bij de volgende vraag. **context**
30	Zijn er toegangsbeperking voor de ruimten waar de servers met patiënten gegevens zich bevinden?		9	**norm (Het woord servers is misschien niet handig gekozen.)**