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 patienten 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 patienten dossiers en ontsluiting van die dossiers via het internet beloofd veel voordeel op te leveren voor alle betrokkenen in de zorg. Het brengt ook z'n eigen risico's met zich mee. Toegang tot het landelijk EPD betekent toegang tot een enorme hoeveelheid digitaal opgeslagen gegevens over patienten. Deze zijn doordat ze praktisch gestructureerd opgeslagen zijn goed doorzoekbaar en heel geschikt zijn om gebruik maar ook om misbruik van te maken. M.a.w. het potentieel voor goed neemt toe maar het potentieel voor kwaad ook. Het is dus nu meer dan ooit van belang dat de beveiliging van patientengegevens 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 patientendossiers in het algemeen aan. Als we het hebben over het systeem dat landelijke uitwisseling van electronische patientendossiers mogelijk moet maken hebben we het over het landelijke EPD. In Nederland wordt de invoering van het landelijk EPD gecordineerd door het NICTIZ (Nationale knooppunt voor ICT in de Zorg) . Zij zijn verantwoordelijk voor het ontwerpen van de infrastructuur en het toezicht houden 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) en
- de informatiesystemen van de zorgverleners [ ].

plaatje [ringholm whitepaper]

Als er een informatievraag 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 dat opgegeven is wel overeenkomt met de patient waarover informatie gevraagd wordt. Als dit allemaal in orde is dan wordt de vragende zorgverlener verbonden met de Zorg Informatie Makelaar (ZIM) dat een onderdeel is van het LSP. Het ZIM heeft een index voor de informatie die bij verschillende zorgverleners over verschillende patienten aanwezig is en weet welke informatie ingezien mag worden en welke niet. Het ZIM stuurt de informatie van de plek waar het is opgeslagen (in het zorgsysteem van een of andere zorgverlener) naar de vragende zorgverlener. (Dit is een vereenvoudigde weergave het process zoals dat in de whitepaper van het Ringholm instituut wordt uitgelegd.)

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 gedefinieerd [NEN .....] [Beveiliging van het EPD ...]. Wij kiezen er voor om ons te richten op mogelijke problemen bij de bescherming van gegevens tegen ongeoorloofde inzage. misschien moeten we hier nog een verantwoording van die keuze geven als we daar een reden voor kunnen aangeven De verplichting om patientengegevens te beschermen tegen ongeoorloofde inzage komt in nederland voort uit de WBP (Wet Bescherming Persoonsgegevens) en indirect uit de WGBO (Wet op de Geneeskundige Behandelings Overeenkomst) [Veiligheid van het EPD p.5]. Er is door het ministerie van Economische zaken en het Nederlands Normalisatie Instituut een norm opgesteld die geld voor informatiebeveiliging in de medische sector. Deze norm bestaat uit een aantal delen. Het algemene deel dat geld voor alle verschillende zorgverleners is de NEN 7510 norm. De NEN norm bespreekt expliciet welke dimensie zij onderkent in het begrip veiligheid [NEN p.6-8]. Uit wat zij daar presenteerd gebruiken wij alleen het onderdeel vertrouwelijkheid. Het programma van eisen dat het NICTIZ stelt aan informatiesystemen van

zorgverleners bespreekt niet expliciet wat ze onder veiligheid verstaat maar ze bevat wel paragrafen die gaan over beveiliging van gegevens tegen ongeoorloofde inzage [o.a. PvE GBZ 4.2, 4.20, 5.3, 6.4]

Eisen en Normen

NEN 7510 De NEN7510 norm is gemaakt om het niveau van de informatiebeveiliging te bevorderen. De norm geeft zorgverleners en ook it dienstverleners een middel om zicht te krijgen op de kwaliteit van hun informatiebeveiliging [NEN 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 af. Wij gaan in het kader van dit onderzoek niet in op de kwaliteit van de NEN 7510 norm. De NEN7510 norm is een algemene norm voor informatiebeveiliging in de zorg. Zij geld dus ook voor informatiesystemen van zorgverleners die nog niet op het landelijke EPD zijn aangesloten

PvE GBZ Het programma van eisen voor een Goed Beheerd Zorgsysteem is een set eisen die gesteld worden aan een informatiesysteem van een zorgverlener om aangesloten te mogen worden op het LSP. Een deel van die eisen gaat over veiligheid maar de meeste niet. 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. De eisen worden gesteld in de vorm van eisen aan functionaliteit die het systeem moet hebben.

3 Methode

1. We maken een selectie van punten uit NEN7510 norm en een selectie van eisen uit het programma van eisen die belangrijk vinden voor de veiligheid als vertrouwelijkheid
2. We maken 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 gedrag dat mogelijk wel genomen maatregelen uit de eisen en normen ondermijnen
   - 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. We versturen mail aan zorgverleners met het verzoek om onze online vragenlijst in te vullen.

4. we trekken 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. 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 onderzoek ook 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 dan een norm gezocht in de documenten die gebruikt wordt om dit probleem te ondervangen. In de genoemde tabel staat bij die normen die van belang zijn voor een van de genoemde scenarios een commentaar dat over de gevolgen van het niet voldoen aan de normen

5. We kijken 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

Onderstaand ziet u een versie van de vragenlijst zoals die online te vinden is/tekstbackslash was op www.hoogeweide.nl/tekstbackslash epd onder de mogelijke antwoorden ziet u in getallen het aantal keer dat dat antwoord is gegeven

vraag	Ja	Nee	Geen idee	n.v.t
Heeft uw organisatie een beleid voor de beveiliging van patiëntgegevens?	4	1	0	0
Is er n 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

vraag	Ja	Nee	Geen idee	n.v.t
Is er binnen uw organisatie een inventarisatie en analyse gemaakt van de mogelijke veiligheidsrisico'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 beveiligingsbeleid?	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 gevalueerd of het beleid de informatiebeveiliging ook verbeterd?	1	4	0	0
	Zelf	Uitbesteed	Geen idee	N.V.T.
Heeft uw organisatie zelf een informatiebeveiligingsbeleid ontwikkeld of is dat uitbesteed?	2	2	1	0

vraag		Ja	Nee	Geen idee	n.v.t
Zijn de patintgegevens al digitaal opgeslagen in uw organisatie? (d.w.z. is er al een electronisch patinten dossier (E.P.D.)?)		5	0	0	0
Bent u al op de een of andere manier aangesloten op het landelijk E.P.D.?		1	4	0	0
Zijn er al wijzigingen in procedures in verband met de aansluiting van uw E.P.D. aan het landelijke E.P.D.?		2	2	1	0
	0-6	6-12	12-18	18-24	24-

vraag		Ja	Nee	Geen idee	n.v.t
Hoeveel maanden schat u dat het nog zal duren voordat u volledig bent aangesloten op het landelijk E.P.D.?	2	0	1	0	2

vraag	Ja	Nee	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 er voor zorgt dat vertrekkende medewerkers geen toegang meer hebben tot patintgegevens?	4	1	0	0

vraag	Ja	Nee	Geen idee	n.v.t
Is de toegang tot patintgegevens 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

vraag	Ja	Nee	Geen idee	n.v.t
Maakt u gebruik van biometrie? (irisscan of vingerafdruk)	0	5	0	0
Hebben alle medewerkers toegang tot alle patintgegevens?	4	1	0	0
Zijn er medewerkers die toegang hebben tot slechts een deel van de patintgegevens?	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 autorisatiegegevens van een collega?	1	4	0	0

vraag	Zelf	Uitbesteed	Geen idee	n.v.t
Regelt u het beheer van de servers met patintgegevens zelf?	1	3	0	1
	ja	nee	geen idee	n.v.t.
Zijn er toegangsbeperking voor de ruimten waar de servers met patinten gegevens zich bevinden?	2	1	1	1

Overzicht per respondent.

resp.	Voldaan	Niet voldaan	Ondermijnend	Commentaar
1	1	9	3	Misschien niet bij de juiste persoon in de organisatie terecht gekomen. Dat de persoon ik 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	

resp.	Voldaan	Niet voldaan	Ondermijnend	Commentaar
5	9	0	1	

5 discussie

5.1 Haken en ogen aan de methode en de uitvoering

5.1.1 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. We hebben geen idee of het verschil maakt maar het zou kunnen en bij het lezen van de conclusies moet dit put niet vergeten worden.

5.1.2 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 [NEN7510 p.5].

5.1.3 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.

5.1.4 Mogelijkheid dat er slechts 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. 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.

subsubsection 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 kunnen schatten of er een sociaal wenselijk antwoord gegeven wordt en in een interview kun je doorvragen als je ergens 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.

6 conclusie

respodent nr 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.

De andere respondenten voldoen aan de meeste van de 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. De 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

- Beveiliging van het EPD, Rapportage van het juridisch laboratorium mr. Sjaak Nouwt
  ZonMw 2002

- NEN 7510 (nl)
  Nederlands Normalisatie instituut 2004

- Programma van Eisen voor een Goed Beheerd Zorgsysteem (GBZ)
  NICTIZ 2007

- Whitepaper van het Ringholm instituut over AORTA
  http://www.ringholm.de/docs/00980_en.htm

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 n persoon of afdeling verantwoordelijk voor de beveiliging van patintgegevens?		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 geist 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

		PvE	NEN	Commentaar
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
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 gevalueerd of het beleid de informatiebeveiliging ook verbeterd?		5.1.2 6.1.7	Als er niet gevalueerd 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

		PvE	NEN	Commentaar
11	Zijn de patintgegevens al digitaal opgeslagen in uw organisatie? (d.w.z. is er al een electronisch patinten dossier (E.P.D.)			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 E.P.D.?			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 E.P.D. aan het landelijke E.P.D.?			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 E.P.D.?			context
15	Zijn er mensen van buiten uw organisatie die toegang hebben tot uw patintgegevens?			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 patintgegevens 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 patint-gegevens?		8.3.4	norm
20	Is de toegang tot patint-gegevens 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 gebruiker-snaam combinatie?	4.2.1		om vast te stellen welk 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 patint-gegevens?			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 patint-gegevens?			Maakt zorgvuldig omgaan met restricties belangrijker context

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