ERROR: ACCESS DENIED

Adviesrapport ter verbetering bevoegdheidsverstrekking UMCG

Rocco Andela
Cor Jonker

UMCG,
Hanzehogeschool Groningen,
Technische Bedrijfskunde

Groningen, juli 2011

Studentenbureau UMCG

Universitair Medisch Centrum Groningen

ERROR: ACCESS DENIED

Adviesrapport ter verbetering bevoegdheidsverstrekking UMCG

Groningen, juli 2011

Auteur	Rocco Andela, Cor Jonker
Studentnummer	293622 294665
Afstudeerscriptie in het kader van	Technische Bedrijfskunde Hanzehogeschool Groningen
Opdrachtgever	mw. A. Weewer, Hoofd Functioneel- & Gegevensbeheer, bureau FGB, UMCG
Begeleider onderwijsinstelling	P. Penninga Technische Bedrijfskunde Hanzehogeschool Groningen
Begeleider UMCG	mw. L. Evers, Functioneel- & Gegevensbeheer bureau FGB, UMCG

ISBN 978-90-8827-098-7
800 Bedrijfskunde algemeen
Trefw Autorisatie, ICT, FGB, Informatiebeveiliging, Applicaties, NEN7510, Bevoegdheden, Toegangsrechten, IGZ, CBP, Audit.

Voorwoord

Voor u ligt het adviesrapport “ERROR: ACCESS DENIED”. Dit rapport is tot stand gekomen in het kader van ons afstudeertraject binnen de opleiding Technische Bedrijfskunde aan de Hanzehogeschool Groningen. Het rapport dient als advies aan het UMCG ter verbetering van de informatiebeveiliging rond het uitgeven, muteren en intrekken van bevoegdheden voor ICT applicaties.

Het UMCG heeft ons een afstudeerplek geboden waarin we veel hebben kunnen leren en ons hebben kunnen ontwikkelen. Hiermee zijn we goed op weg geholpen naar toekomstige master opleidingen en hebben we onze kansen op de arbeidsmarkt vergroot. Wij zijn hiervoor veel dank verschuldigd aan allen die dit mogelijk hebben mogen maken.

Dankzij de uitstekende begeleiding vanuit zowel de Hanzehogeschool Groningen en het UMCG zelf zijn wij in staat gesteld het afstudeertraject af te ronden met een gedegen advies. In de eerste plaats willen we daarvoor onze bedrijfsbegeleider Mw. L.Evers bedanken. Tijdens de wekelijkse feedback/coach momenten werden we door haar voorzien van veel tips en trucs over het functioneren in een grote organisatie als het UMCG. Hierdoor kregen we snel door hoe zaken geregeld worden in het UMCG wat ons hielp om dingen gedaan te krijgen.

evens zijn wij veel dank verschuldigd aan de stagebegeleider Dhr. P.Penninga. Door goed onderbouwde kritiek wist hij ons telkens weer op het goede pad te krijgen en behoede hij ons voor een val in de afgrond. Onze opdrachtgever Mw. A.Weewer heeft, ondanks haar drukke agenda, ons te woord gestaan wanneer wij dat nodig hadden. Dit getuigt van veel vertrouwen in ons en belang bij het adviesrapport. Hiervoor onze dank. Graag willen we Dhr. F. de Vries en Dhr. F.Erich ook nog noemen. Zij hebben ons uitermate goed geholpen met hun vakkundige inzichten en ervaring. Ten slotte een speciale dank aan de vele overige betrokkenen die ons voorzien hebben van informatie en gegevens. Zij hebben het fundament gevormd van dit adviesrapport.

Veel leesplezier gewenst!

Rocco Andela & Cor Jonker

Groningen, 4 juli 2011

Inhoudsopgave

Samenvatting

ERROR: Access Denied is een onderzoek wat uitgevoerd is bij het UMCG. De informatiebeveiliging in het UMCG voldoet niet aan de gestelde wet- en regelgeving. Dit heeft verschillende oorzaken. Eén van die oorzaken ligt in het proces over het toekennen, intrekken en muteren van bevoegdheden van medewerkers voor ICT-applicaties. Dit proces biedt veel ruimte tot verbetering. In dit onderzoek zijn de belangrijkste oorzaken van de genoemde problemen aan het licht gekomen en er zijn aanbevelingen aangedragen.

Niet voldoen aan de normering voor informatiebeveiliging kan verstrekkende gevolgen voor een ziekenhuis hebben. Consequenties omvatten het inkorten van de mogelijkheden tot het verlenen van zorg of tot uitsluiting van deelname aan het landelijk EPD. Het is dus van groot belang deze problemen aan te pakken.

De centrale vraagstellingen die in het onderzoek beantwoordt worden:

"Het opleveren van een advies- en implementatierapport waarin oplossingen worden aangedragen voor de huidige problemen betreffende het bevoegdheidverstrekkingsproces."

"Wat zijn de oorzaken, achtergronden en samenhangen van de problemen die zich voordoen bij het proces omtrent het uitgeven van ICT bevoegdheden en hoe kunnen deze verbeterd worden?"

Verschillende problemen liggen ten grondslag aan de verminderde informatiebeveiliging door het bevoegdheidverstrekkingsproces.
- Accounts worden uitgeleend aan medewerkers
- Medewerkers met te veel of te weinig bevoegdheden
- Accounts blijven actief nadat een medewerker uit dienst is getreden

De problemen zijn geanalyseerd en de belangrijkste oorzaken ervan zijn gevonden.

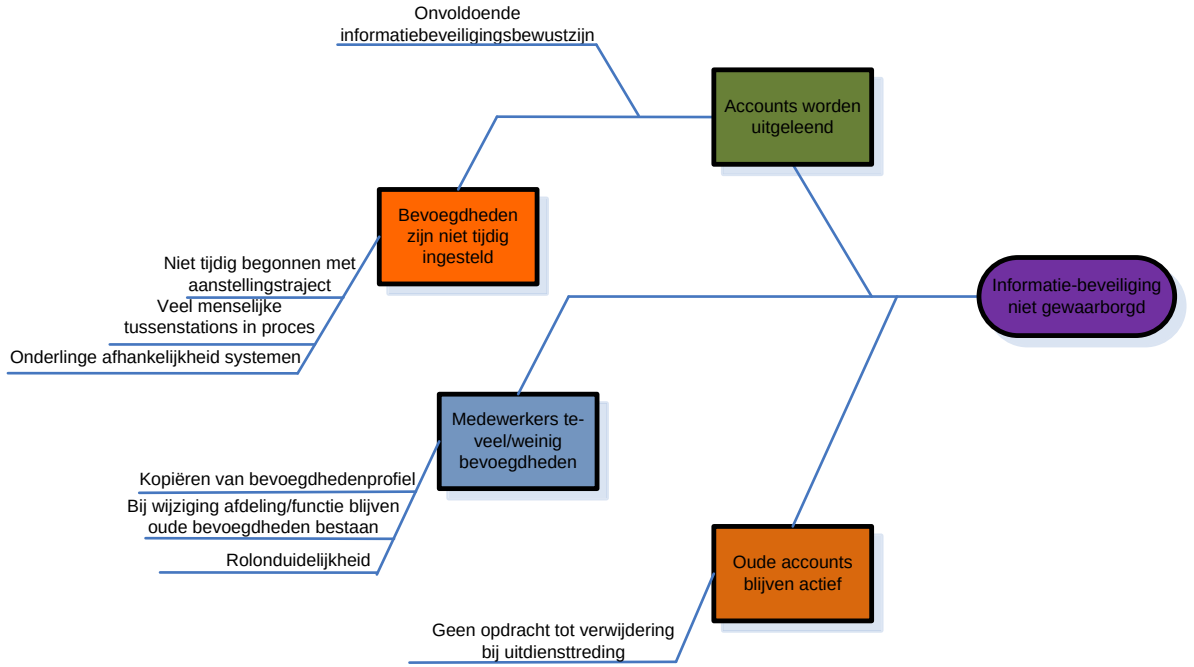
Het bevoegdheidsverstrekkingsproces is weinig transparant en bevat veel menselijke tussenstations.
Sleutelfiguren in het proces weten onvoldoende tot waar hun verantwoordelijkheid strekt en wat de gevolgen van een verminderde informatiebeveiliging kunnen zijn.
Hierdoor ontstaan in het proces onnodige vertragingen en hebben medewerkers te kampen met onjuiste bevoegdheden en toegangsrechten, blijven oude accounts actief en zijn bevoegdheden niet tijdig ingesteld. Er wordt bijvoorbeeld door leidinggevenden geen opdracht gegeven voor het verwijderen van een account wanneer een medewerker uitdienst gaat of wanneer een medewerker van functie wisselt behoudt hij zijn oude bevoegdheden.
Door de 'rolonduidelijkheid' wordt er geen vaste manier waarop de medewerkers toegangsrechten aanvragen gebruikt. Hierdoor ontstaat er een waaier van verschillende werkwijzen binnen de muren van het UMCG.

De belangrijkste aanbevelingen om de informatiebeveiliging omtrent ICT-bevoegdheden te verbeteren zijn:
- UMCG brede standaard werkwijzen invoeren
- Automatiseren van het proces

Door het opstellen van UMCG brede werkwijzen en een gestructureerd proces worden zwakke punten in het proces aangepakt waardoor vertragingen minder snel voorkomen. Wanneer er dan tijdig wordt begonnen met het aanstellen van de medewerker, in combinatie met een paar lopende ICT projecten die het proces deels ondersteunen, zijn veel van de problemen al verholpen.

Feit blijft dat er veel schakels in het proces aanwezig zijn. Wanneer één van de schakels niet functioneert, valt het proces daar stil. Door het automatiseren van het proces wordt menselijke inbreng omzeild waardoor het risico op fouten verkleint. Als het Ziekenhuisinformatiesysteem ge-

koppeld wordt aan het personeelsregistratiesysteem, zoals de toekomstige koppeling tussen ADS en het personeels-registratiesysteem (IAM), kunnen bevoegdheden automatisch ingesteld worden op grond van afdeling, functie en rol van de nieuwe medewerker.



Figuur 1 Ingevuld Ishikawa diagram.

1 Inleiding

1.1 Aanleiding

Het Universitair Medisch Centrum Groningen (UMCG) is één van de grootste ziekenhuizen in Nederland en de grootste werkgever van Noord-Nederland. De ruim 10.000 medewerkers werken in de patiëntenzorg en aan vooraanstaand wetenschappelijk onderzoek, waarbij de focus ligt op 'gezond en actief ouder worden'. In het kader van wetenschappelijk onderzoek en onderwijs wordt nauw samen gewerkt met de Rijksuniversiteit Groningen. Er worden studenten opgeleid tot arts, tandarts of bewegingswetenschapper en artsen opgeleid tot medisch specialist. Patiënten komen in het UMCG voor basiszorg, maar ook voor zeer specialistische diagnostiek, onderzoek of behandeling. De zorg wordt gegeven door de beste dokters en verpleegkundigen. Samen met ondersteunend personeel werken zij dagelijks aan die ene, gemeenschappelijke doelstelling: bouwen aan de toekomst van gezondheid.

Dagelijks zijn er duizend patiënten opgenomen, bezoekt een veelvoud daarvan een polikliniek en werken meer dan 10.000 medewerkers samen aan zorg, onderzoek en onderwijs. Het merendeel van de medewerkers heeft één of meerdere bevoegdheden om met ondersteuning van verschillende applicaties en informatiesystemen de werkzaamheden te verrichten. Hiervoor is het noodzakelijk dat deze bevoegdheden bij aanstelling van de medewerker worden uitgereikt, tussentijds zo nodig worden aangepast en bij vertrek weer worden ingetrokken. Idealiter gebeurt dit tijdig, juist en volledig. Een in opdracht van de Inspectie voor de Gezondheidszorg (IGZ) in 2010 gehouden audit, die het UMCG toetst aan het voldoen aan richtlijnen voor informatiebeveiliging, wijst echter uit dat het huidige proces omtrent het uitgeven, muteren en intrekken van bevoegdheden van ICT applicaties niet naar behoren verloopt. Dit wordt ondersteund door signalen die medewerkers vanuit verschillende afdelingen hebben afgegeven. Hierop is besloten het proces omtrent bevoegdhedenverstrekking te optimaliseren.

1.2 Problematiek

De problemen met bevoegdheden die zich voordoen zijn gebleken uit de audit IGZ-2010 en de meldingen die medewerkers hebben afgeven aan bureau Functioneel Gegevens Beheer (FGB). Inzage in de audit zelf is wegens vertrouwelijke informatie over andere onderwerpen dan de informatiebeveiliging niet mogelijk..Wel is er een proefaudit beschikbaar, gehouden door het UCMG zelf, waarin problemen rond informatiebeveiliging aangestipt worden. In het kort komt het er op neer dat de informatiebeveiliging te wensen overlaat en daarmee kan de patiëntveiligheid niet gewaarborgd worden.

Een universitair medisch centrum moet voldoen aan een groot pakket van wetten en regels. Voor het bevoegdheidsproces zijn de volgende documenten van toepassing: De NEN7510 met haar uitbreidingen NEN7511 en NEN7512 en de Wet bescherming persoonsgegevens (Wbp). Op dit moment voldoet het UMCG niet voldoende aan de gestelde regelgeving en richtlijnen. Dit brengt allerlei risico's met zich mee. Zowel juridisch als ethisch. Het UMCG kan imagobreuk oplopen door zulke zaken maar ook met het niet voldoen aan de NEN normering is het mogelijk dat het medisch centrum gekort wordt in haar mogelijkheden tot het verlenen van zorg of tot uitsluiting van deelname aan een landelijk EPD. (CBP, IGZ. 2008: 3) Het UMCG heeft er dus veel belang bij dat de problematiek aangepakt wordt en er voldaan wordt aan de gestelde regelgeving en richtlijnen.

1.3 Onderzoeksopzet

Voordat het onderzoek van start is gegaan is er een onderzoeksplan opgesteld om de opzet van het onderzoek vast te leggen. Deze onderzoeksopzet wordt kort weergegeven in deze paragraaf. De onderzoeksopzet bestaat uit vier delen. Op de eerste plaats wordt de formulering van de doelstelling van het onderzoek gepresenteerd. De globale wijze waarop het onderzoek is gestructureerd wordt vervolgens vormgegeven in een onderzoeksmodel. Aan de hand hier-

van is de centrale vraag met de bijbehorende onderzoeksvragen geformuleerd. Tot slot worden de methodes van onderzoek beschreven.

1.3.1 Doelstelling

De opdrachtgever, het hoofd van bureau Functioneel Gegevens Beheer (FGB) ziet graag dat er onderzocht wordt welke oorzaken ten grondslag liggen aan de problemen die zijn vermeld in §1.2 Problematiek en hoe deze problemen opgelost kunnen worden.
De onderstaande doelstelling kan dan vanuit deze vraag en problematiek geformuleerd worden:

"Het opleveren van een advies- en implementatierapport waarin oplossingen worden aangedragen voor de huidige problemen betreffende het bevoegdheidverstrekkingsproces."

1.3.2 Vraagstelling

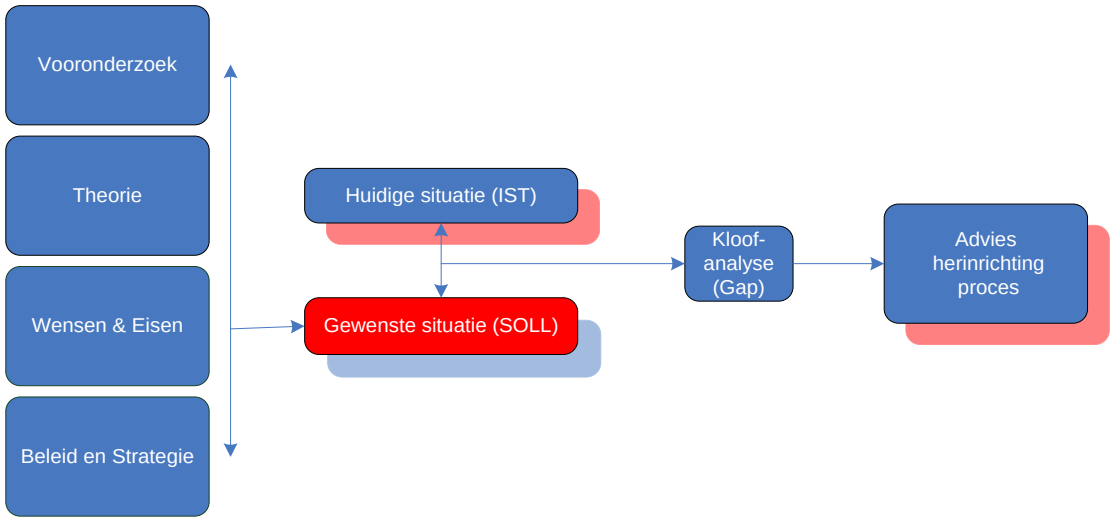
De centrale vraag wordt afgeleidt vanuit de problematiek en doelstelling en luidt als volgt:

"Wat zijn de oorzaken, achtergronden en samenhangen van de problemen die zich voordoen bij het proces betreffende het uitgeven van ICT bevoegdheden en hoe kunnen deze verbeterd worden?"

1.3.3 Onderzoeksmodel

Het onderzoeksmodel is een sterk visuele weergave van de stappen die in het onderzoek gedaan moeten worden om tot het beoogde eindresultaat c.q. de doelstelling te behalen. *Figuur 1* geeft het opgestelde onderzoeksmodel weer. Het schema is van rechts naar links opgesteld. Beginnend bij de doelstelling is er terug geredeneerd om zo globaal de te maken stappen, te definiëren. Het schema dient wel van links naar rechts gelezen te worden. Onderaan de figuur wordt het onderzoeksmodel verder verwoord.

De basis (A) bestaat uit een combinatie van vooronderzoek, theorie, de wensen en eisen die het UCMG stelt aan de nieuwe situatie en het gehanteerde beleid en de strategie. Dit legt de basis voor de gewenste SOLL situatie(B).



Figuur 2 Onderzoeksmodel.

De huidige situatie (IST) wordt geconfronteerd met de SOLL om zo tot een verzameling knel en verbeterpunten (GAP) (C) te komen die na analyse (C) verwerkt worden tot een advies betreffende de herinrichting van het bevoegdheidverstrekkingsproces. (D)

1.3.4 Onderzoekstype

Het onderzoekstype is voornamelijk een ontwerpgericht onderzoek. De problematiek is al ruime tijd bekend binnen de afdeling ICT en ook medewerkers van andere afdelingen ondervinden die problemen. De opdracht is mede vanuit de ICT afdeling aangedragen en leeft daar zodoende ook. Een ontwerpgericht onderzoek richt zich op het dusdanig inrichten van een structuur teneinde de problematiek te verhelpen. Daarnaast heeft het onderzoek ook een diagnostisch kant. Het is niet duidelijk wat precies de oorzaken zijn van de problemen die zich voordoen. Voordat er oplossingen geboden kunnen worden zullen eerst de oorzaken achterhaald moeten worden. (Verschuren, P. 2003: 40)

1.3.5 Onderzoeksobject

Het onderzoeksobject (Verschuren, P. 2003: 50) is het fenomeen wat bestudeerd is tijdens het onderzoek. Het onderzoeksobject voor dit onderzoek is het proces betreffende het aanvragen, muteren en intrekken van bevoegdheden voor ICT applicaties. Dit proces begint al bij de aanstelling van de medewerker en betrekt de ICT afdeling, de tekenbevoegde van de desbetreffende afdeling of sector en andere belanghebbenden die inspraak hebben in dit proces.

1.3.6 Onderzoeksvragen

De deelvragen zijn ontrokken uit het onderzoeksmodel en vormen samen de centrale vraag. Elke deelvraag is opgesplitst in specifiekere onderzoeksvragen.

Wat zijn de oorzaken, achtergronden en samenhangen van de problemen die zich voordoen bij het proces betreffende het uitgeven van ICT bevoegdheden en hoe kunnen deze verbeterd worden?

Deelvraag 1:
Hoe ziet de SOLL situatie eruit en welke KPI's kunnen er worden opgesteld?

Onderzoeksvragen:
1.1 Wat zijn de wensen en eisen met betrekking tot de gewenste situatie?
1.2 Wat is het beleid betreffende het bevoegdheidsproces?
1.3 Welk deel van de strategie heeft betrekking tot het bevoegdheidsproces?
1.4 Hoe ziet de gewenste situatie eruit? Ergo, welke KPI's kunnen er worden opgesteld?

Deelvraag 2:
Hoe wordt de IST situatie beoordeeld in het licht van de SOLL situatie?

Onderzoeksvragen:
2.1 Hoe ziet de huidige situatie eruit?
2.2 Waarin wijken de IST en SOLL van elkaar af?
2.3 Wat zijn de oorzaken van de afwijkingen?

Deelvraag 3:
Hoe kan met de kennis ontrokken aan de confrontatie tussen IST en SOLL de oorzaken van de problemen worden aangepakt?

Onderzoeksvragen:
3.1 Hoe kunnen de oorzaken van de problemen worden aangepakt?
3.2 Wat voor aanbevelingen kunnen er gedaan worden?

Deelvraag 4:
Hoe kunnen de bevindingen geïmplementeerd worden?

Onderzoeksvragen:
4.1 Wat zijn de verwachte effecten van de implementatie van deze bevindingen?
4.2 Welke bevindingen hebben het meeste rendement?
4.3 Wat moet er gebeuren om een succesvolle verandering door te voeren?
4.4 Hoe kan deze verandering gewaarborgd blijven?
De onderzoeksvragen worden in het rapport beantwoord. Deelvraag 1 is beschreven in de Hoofdstuk 2 Probleemschets. Deelvraag 2 wordt behandeld in zowel Hoofdstuk 3

Probleemanalyse als in Hoofdstuk 4 Conclusie en Aanbevelingen. Deelvraag 3 wordt eveneens behandeld in Hoofdstuk 4. De beantwoording van deelvraag 4 is terug te vinden in Hoofdstuk 5 Implementatie.

1.3.7 Methode van onderzoek

Theoretisch kader

Strategisch Management
Kleijn, H. Rorink, F. (2009) Verandermanagement
'Organisatie veranderingen' Verandermanagement geeft een methodische aanpak voor het vaststellen, ontwerpen, implementeren en evalueren van organisatieveranderingen. Aan de hand van de door verandermanagement gegeven huidige-(IST) en gewenste(SOLL)situatie methodiek is inzicht in deze situaties verkregen.

Operationeel Management
Krajewski, L. Ritzman, L. Malhotra, M., (2007) Operations Management. Processes and Value Chains.
Theorie over procesanalyse en waardeketens. Operations Management biedt een algemeen kader voor de aanpak van operationele proces en waardeketen vraagstukken. De methode maakt gebruik van een gesystematiseerd aanpak waarbij de focus op actuele aspecten.

Keuze van ondervragen
Gramsbergen-Hoogland,Y.H. Molen, van der, H.T., (2005) Gesprekken in organisaties
'informatie verschaffing methode' Aan de hand van Gesprekken in organisaties zijn de keuzes ter verschaffing van informatie gemaakt. Er is gekeken op welke manier de meest effectief situatie gericht informatie verschaft kon worden.

Juridische aansprakelijkheid
Roest, van der, O.A.P. (2006) Basisboek Recht.
'Aansprakelijkheid' Met behulp van het Basisboek Recht is gekeken wie aansprakelijk is in het geval van het niet waarborgen van de informatiebeveiliging. Op deze manier is gekeken wie zorg zou moeten dragen op het toezien van het volbrengen van de beleidseisen om de informatiebeveiliging te waarborgen.

Ethisch verantwoordelijkheid
Fledderman, C.B. (2008) Engineering Ethics
'Ethische verantwoordelijkheid' Met behulp van gegeven ethische verantwoordelijkheden uit de literatuur is gekeken hoe als manager uit ethisch oogpunt zorg gedragen moet worden voor het proces.

Methodiek

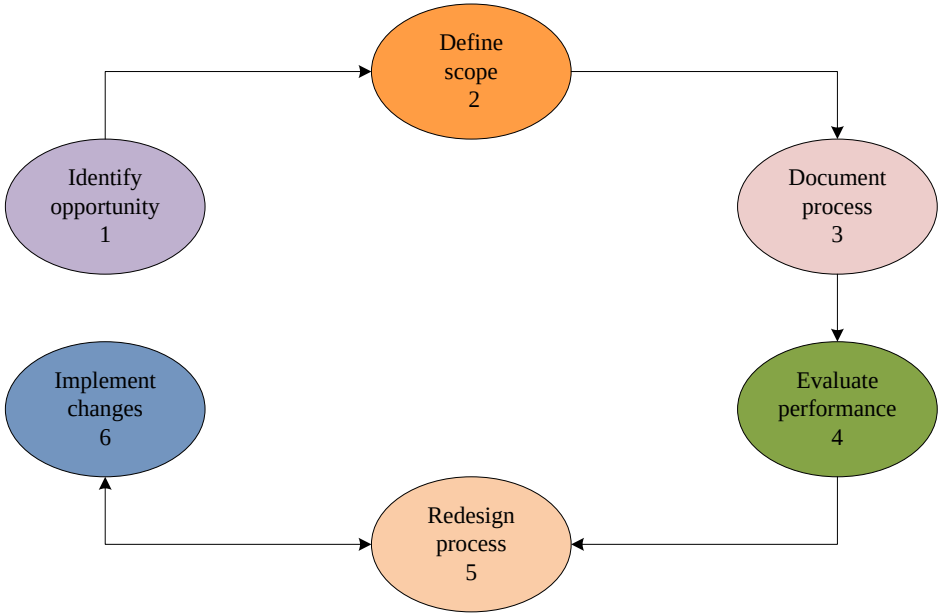
Procesdocumentatie
Het ontwikkelen van oplossingen gaat volgens de methodes van het boek Operations Management. (Krajewski, L. 2007: 153) Dit is een methode om processen opnieuw in te richten. Er worden globaal zes stappen onderscheden die doorlopen moeten worden om tot een herinrichting van het proces te komen. Deze zes stappen zijn de volgende:

1. Identify opportunity
2. Define the scope
3. Document the process
4. Evaluate performance
5. Redesign the process
6. Implement changes

Voor elke stap worden er hulpmiddelen gegeven op het doel te bereiken. De methode moet worden gezien als extra handvat om het onderzoek aan op te hangen. Stap 1: 'Identify opportunity' is gezet door het UMCG zelf. Zij zagen kansen tot verbetering in de huidige situatie. In het traject voor het daadwerkelijke onderzoek is vastgelegd wat er precies onderzocht ging worden. Dit is stap 2: 'Define scope'. Stap 3, 4 en 5 worden in dit rapport behandeld. Voor stap 6: 'Implement Changes' wordt alleen een plan geschreven.

BPM/One
Met behulp van het programma BPM/One; het programma wat het UMCG gebruikt om haar processen te documenteren; worden de processen in kaart gebracht.

Interviews
Voor het in kaart brengen van de problematiek, de huidige situatie en de mogelijke oplossingen daarvoor, zijn er medewerkers geïnterviewd. Er is gebruik gemaakt van het half



Figuur 3 Blueprint for Process Analysis.

gestandaardiseerd interview. Dit is de beste manier van interviewen in deze situatie omdat allerlei procedures en systemen in het begin nog onbekend waren. In een half gestandaardiseerd interview ligt alleen het thema en een aantal onderwerpen vast. Het is het nuttig gebleken om met een combinatie van open vragen en concretiseringen deze onderwerpen beter door te lichten. (Gramsbergen-Hoogland, Y.H. 2005: 61) Er zijn interviews gehouden om het proces in kaart te brengen. Met dit in kaart gebrachte proces werd duidelijk welke sleutelfiguren er betrokken waren bij de processen. Hierna kon er gericht verder gegaan worden met interviewen van de juiste betrokken mensen. Bepaalde geïnterviewden prefereerden het om anoniem te blijven terwijl anderen naamsvermelding geen probleem vonden. De meeste gebruikte gespreksinformatie is ondertekend door de verstrekker en inzage in deze ondertekende documenten is mogelijk bij de opdrachtgever. Ook zijn er ondervraagden die de gespreksverslagen niet hebben ondertekend. Deze personen staan anoniem vermeld wanneer zij geen goedkeuring voor het gebruik van de naam en tekst hebben gegeven. Informatie uit deze gesprekken is niet gecontroleerd op juistheid waardoor er voorzichtiger is omgegaan met conclusies trekken uit die verslagen. Er zijn gespreksverslagen die het gehele gesprek verwoorden, maar ook zijn er gespreksverslagen die na wens van de vestrekker enkel zaken die relevant zijn voor ons onderzoeksonderwerp bevatten.

1.4 Vooruitblik

De problemen die voorkomen zijn hiervoor in *§ 1.2: Problematiek* aangestipt. In *Hoofdstuk 2: Probleemschets* is de problematiek nader uitgewerkt en zijn er kritische succes factoren opgesteld waaraan een nieuwe situatie gemeten kan worden. Daarop volgend in *Hoofdstuk 3: Probleemanalyse* zijn de bevindingen en analyse van het probleem beschreven. In *Hoofdstuk 4: Conclusie en Aanbevelingen* wordt er een eindconclusie getrokken en er staan aanbevelingen voor een verbetersituatie. Tot slot wordt er in *Hoofdstuk 5: Implementatie* een implementatieplan voorgesteld

2 Probleemschets

2.1 UMCG

2.1.1 Kerntaken[1]

Kerntaak: Zorg
Patiënten komen in het UMCG voor 'gewone' ziekenhuiszorg, maar ook voor zeer specialistische diagnostiek, onderzoek of behandeling. Alle patiënten uit Noord-Nederland met gecompliceerde of zeldzame aandoeningen worden uiteindelijk naar het UMCG verwezen. Voor sommige zeer complexe behandelingen is het UMCG zelfs het enige ziekenhuis in Nederland. Goede zorg is altijd gebaseerd op de nieuwste inzichten. Veiligheid en kwaliteit staan daarbij voorop, vanzelfsprekend met oog voor de wensen van de patiënten. Zorg houdt voor het UMCG niet op bij de ziekenhuismuren. Het UMCG werkt daarom nauw samen met huisartsen, verloskundigen, thuiszorg en tal van andere zorginstellingen.

Kerntaak: onderwijs
De Groningse opleidingen staan zeer hoog aangeschreven en bieden tal van uitdagende extra's: zo wordt de bachelor Geneeskunde ook in het Engels aangeboden en kunnen excellente geneeskundestudenten een extra opleiding volgen, die gericht is op het doen van wetenschappelijk onderzoek, de Junior Scientfic Masterclass (JSM), of al tijdens hun studie promoveren.
In het UMCG worden ongeveer 3400 studenten opgeleid tot arts, tandarts of bewegingswetenschapper en ruim 450 artsen opgeleid tot medisch specialist. Het UMCG heeft alle opleidingen tot specialist in huis. Ook verzorgt het UMCG tal van (zorg)opleidingen op HBO- en MBO-niveau.

Kerntaak: onderzoek
Het UMCG doet onderzoek naar nieuwe technieken en behandelingen, nieuwe medicijnen en nieuwe vormen van zorg waarbij de focus ligt op 'gezond en actief ouder worden'. Hierbij wordt nauw samen gewerkt met de Rijksuniversiteit Groningen. Het fundamenteel en klinisch onderzoek van het UMCG behoort tot de internationale wetenschappelijke top. De aanwezigheid van unieke biobanken en state-of-the-art onderzoeksfaciliteiten trekt wetenschappers uit de hele wereld.

2.1.2 Structuur

De ziekenhuisorganisatie is opgebouwd rondom patiëntenzorg. De directe patiëntenzorgactiviteiten worden verricht door de afdelingen en de ondersteunende voorzieningen voor de patiëntenzorg zijn ondergebracht in zorgfaciliteiten. Het UMCG bestaat uit zes sectoren. Deze kunnen gezien worden als afzonderlijke ziekenhuizen. Elke sector heeft bijvoorbeeld haar eigen sectordirectie. In bijlage 1 zijn de organogrammen te vinden van het UMCG, een sector en een medische afdeling. De afdelingen zijn op basis van erkende medische specialismen geordend in de sectoren. Elke afdeling heeft de vrijheid om de afdeling naar eigen inzichten in te richten. Dit betreft onder andere de aanwending van personele en financiële middelen. Het afdelingshoofd is belast met de algemene leiding van de afdeling en wordt ondersteund door een drietal functionarissen: een (coördinerend) Chef de Clinique, een manager Bedrijfsvoering en/of manager Zorg. Gezamenlijk vormen deze functionarissen met het afdelingshoofd het Dagelijks Bestuur (DB) van de afdeling, dat verantwoordelijk is voor de dagelijkse leiding van de afdeling.

De structuur van het UMCG kan aangeduid worden als een 'divisiestructuur'. Een divisie bestaat uit een 'hoofdkantoor', het UMCG, en een aantal 'dochters', de sectoren. De sectoren zijn verantwoordelijk wat de uitvoering van hun eigen taken betreft. Maar het UMCG bepaalt de randvoorwaarden. Dat wil zeggen: de overallstrategie: wat de sectoren uiteindelijk moeten bereiken en de speelruimte waarbinnen dit gebeurt. (Noomen, J.L., 2004: 422-423)

2.1.3 Cultuur

Organisatiecultuur is het geheel aan opvattingen over bijvoorbeeld waarden, normen, doelstellingen en verwachtingen, dat dominant is binnen de organisatie, en het daaruit resulterende gedrag van de medewerkers.

[1] Intranet UMCG

Een belangrijke slaagfactor van veranderprocessen is het tijdig aanleren van een nieuwe attitude, kennis en vaardigheden door betrokken medewerkers en ook werkelijk in de praktijk toepassen. Dit betekent dat medewerkers zich voor een deel een nieuwe waarde en normenpatroon eigen moeten maken. Veel veranderprocessen blijken na verloop van tijd alsnog te mislukken omdat er onvoldoende rekening is gehouden met de bedrijfscultuur van de betrokken organisatiedelen. Het is dan ook belangrijk zicht te hebben op de dominante cultuur van de organisatie.

De organisatiecultuur van de bij het onderzoek betrokken organisatiedelen in het UMCG karakteriseert zich als een taakcultuur. Bij deze cultuur is de hoogste waarde dat het werk zo goed mogelijk wordt gedaan. Men is pragmatisch ingesteld en men laat zich wat betreft de coördinatie leiden door de eisen die het werk stelt. Deskundigheid weegt zwaar en men werkt samen in teams als dat tenminste bijdraagt aan de kwaliteit en effectiviteit van het werk. In een taakcultuur worden ad hoc gevormde werkgroepen gevormd die problemen aanpakken op het moment dat ze zich voordoen. (Kleijn, H. Rorink, F. 2009: 92-100) Deze eigenschappen zijn aan het licht gekomen en terug gevonden bij de afdelingen (ICT, FGB) tijdens dit onderzoek binnen het UMCG. Er zijn werkgroepen aangesteld door leidinggevenden die zich focussen op problemen en deze projectmatig proberen op te lossen. Voor het verlenen van specifieke zorg weegt deskundigheid zwaar en moet de kwaliteit zo hoog mogelijk zijn wat tevens aansluit bij een taakcultuur.

2.2 IGZ Audit

De Inspectie voor Gezondheidszorg heeft alle ziekenhuizen in Nederland opdracht gegeven in 2010 een onafhankelijke, externe, audit te laten uitvoeren op de implementatie van de NEN7510. Deze audit heeft uitgewezen dat het UMCG op bepaalde punten niet aan de NEN7510 voldoet, één van deze punten is het proces rondom bevoegdhedenverstrekking. Met het niet voldoen aan NEN 7510-normering neemt het UMCG ook risico's. Een slechte informatiebeveiliging kan bijvoorbeeld leiden tot een lagere kwaliteit zorgverlening aan de patiënt. Wanneer patiënteninformatie niet goed beveiligd is, is het denkbaar dat door onbevoegden bijvoorbeeld de medicatievoorschriften voor een patiënt aanpast worden wat ernstige gevolgen kan hebben voor de gezondheid van de patiënt. Of wanneer patiënteninformatie uitlekt, kan dit leiden tot claims van gedupeerden tegen het UMCG. Het imago van de organisatie kan aangetast worden wat zorgt voor verlies van marktaandeel ten opzichte van concurrenten die wel aan de normering voldoen. Om die redenen wil het UMCG voldoen aan de gestelde wet- en regelgeving.

Tijdens dit onderzoek zijn de plannen voor het EPD veranderd. De Eerste Kamer heeft tegen de verplichte aansluiting op het EPD gestemd. Wel wordt er nu gekeken of via versterking van andere wetten de privacy en bescherming van patiënten verbeterd kan worden. De prioriteit om aan wet en regelgeving te voldoen blijft dus ondanks de onzekerheid van het verplichte landelijke EPD hoog. In bijlage 7 is het bericht van de website van het landelijke EPD terug te vinden.

2.2.1 Juridische kaders

De gestelde wet- en regelgeving, die van toepassing is op het onderzochte probleem wordt hieronder kort toegelicht zodat er bepaald kan worden wat het UMCG moet doen om toch aan de gestelde normering te voldoen.

- NEN7510
- NEN7511
- NEN7512
- Wet bescherming persoonsgegevens

Het IGZ en CBP (College Bescherming Persoonsgegevens) zijn toezichthoudende instanties die beide de informatiebeveiliging scherp op het vizier hebben staan. In het verleden hebben het IGZ en het CBP nauw met elkaar samengewerkt. Het rapport *"Informatiebeveiliging in ziekenhuizen voldoet niet aan de norm"* bijvoorbeeld, beschrijft een onderzoek wat in 2007 is uitgevoerd door het IGZ en het CBP. Dit geeft aan dat er goede controle is op naleving van de gestelde eisen. Het IGZ en CBP voeren nog altijd controles uit om te kijken of de informatiebeveiliging van ziekenhuizen aan de eisen voldoen. Alle ziekhuizen zijn in 2010 verplicht door IGZ om een externe audit te laten uitvoeren om te toetsen of zij aan de norm voor informatiebeveiliging (NEN7510) voldoen.

De norm **NEN 7510** gaat over informatiebeveiliging binnen de zorgsector. Onder informatiebeveiliging in de zorg wordt verstaan: het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van alle informatie die benodigd is om patiënten verantwoorde zorg te kunnen bieden. Naast het borgen van deze kwaliteitscriteria vereist deze norm ook dat de informatiebeveiligingsmaatregelen op controleerbare wijze zijn ingericht voordat kan worden gesproken over adequate informatiebeveiliging. De norm kan beschouwd worden als een kader. Binnen dit kader kan elke proceseigenaar de voor zijn/haar proces relevant geachte informatiebeveiliging specificeren, inclusief de daarbij behorende maatregelen.[2]

Een overzicht van de op het onderzoek toepasbare wet- en regelgeving uit de NEN7510 is terug te vinden in bijlage 4.

De **NEN7511** is een uitwerking van de algemene norm NEN7510. De **NEN 7512** is een aanvulling op de richtlijnen die in de NEN7510 gesteld worden. De **Wet bescherming persoonsgegevens** (Wbp) regelt, ter bescherming van de privacy, wat er allemaal wel en niet mag met gebeuren met persoonsgegevens. De Wbp is de opvolger van de Wet persoonsregistraties (Wpr).

De audit IGZ-2010 heeft uitgewezen dat het UMCG niet volledig aan de NEN7510 normering voldoet. In de audit komt naar voren wat er mis gaat met de informatiebeveiliging in het UMCG.

Verschillende problemen worden vermeld in de proefaudit en bevestigd tijdens de oriënterende interviews. Accounts van medewerkers blijken bijvoorbeeld lang actief te blijven als medewerkers niet meer werkzaam zijn bij het UMCG. Daarnaast zijn er medewerkers met teveel of juist te weinig bevoegdheden. Medewerkers lenen accounts ook uit aan elkaar. Ook is het niet eenduidig hoe het proces van bevoegdheidverstrekking precies verloopt, wie daar op welk moment verantwoordelijkheid in heeft en hoe daarbij de informatiebeveiliging wordt gewaarborgd. Hoe vaak de genoemde problemen zich voordoen is onduidelijk doordat inzage in de audit beperkt is. Omdat het om de veiligheid en bescherming van patiënten gaat is elke fout, één fout te veel.

De problemen die voorkomen staan hieronder in willekeurige volgorde in Tabel 1 weergegeven.

Nr.	Probleem
1	Medewerkers lenen accounts uit aan elkaar.
2	Bij het wijzigen van afdeling blijven oude bevoegdheden staan.
3	Medewerkers met teveel of juist te weinig bevoegdheden

Tabel 1 Problemen genoemd in de proefaudit en oriënterende interviews.

Om te bewerkstelligen dat het UMCG aan alle normen voldoet moeten de problemen die hierboven zijn genoemd dus opgelost worden.

2.3 Beleid

Het ICT-beleid van het UMCG wordt onder andere afgeleid van de in de zorg geldende wet en regelgeving.
In het document *"Van beleid naar naleving"* (Krogt, van der, L., 2006) van het UMCG wordt de vertaalslag van deze regelgeving naar de naleving hiervan toegelicht. Daarnaast werkt de afdeling ICT-Beheer volgens een kwaliteitshandboek waarin al haar processen abstract staan beschreven.

2.4 McKinsey

UMCG heeft zich in november/december 2010 door strategisch consultancybureau McKinsey laten adviseren over de te volgen strategie in het kader van de noodzakelijke bezuinigingen. Hier zijn een aantal adviezen uit voort gekomen. Deze adviezen zijn breed toepasbaar en niet alleen specifiek voor het onderwerp waar het in dit onderzoek over gaat maar het geeft wel aan welke nieuwe koers het UMCG wil varen. Als gevolg van bezuinigingen en om in de toekomst ook betaalbare zorg te kunnen leveren heeft het UMCG als doel gesteld om de doelmatigheid van algemene en medische ondersteuning in de komende jaren te verhogen. Hierbij adviseerde McKinsey om processen meer te standaardiseren om de efficiëntie te verhogen en om UMCG brede standaard werkwijzen te gebruiken. Een sa-

[2] www.nen7510.org

menvatting van het adviesrapport van McKinsey is terug te vinden in bijlage 3.

2.5 Kritische succes factoren

Aan de hand van de problemen die in de audit gesteld zijn en de adviezen van McKinsey over de nieuwe koers van het UMCG kunnen de onderstaande kritische succes factoren, waar een nieuwe, gewenste situatie aan gemeten wordt, worden opgesteld.

Nr	KSF
1	Medewerkers gebruiken hun account uitsluitend voor zichzelf
2	Gebruikers moeten uitsluitend toegang kunnen krijgen tot diensten, systemen en gegevens waarvoor zij zijn geautoriseerd.
3	UMCG breed standaard werkwijze gebruiken
4	Meer standaardisatie nodig om efficiëntie te vergroten

Tabel 2 Kritische succes factoren.

3 Probleemanalyse

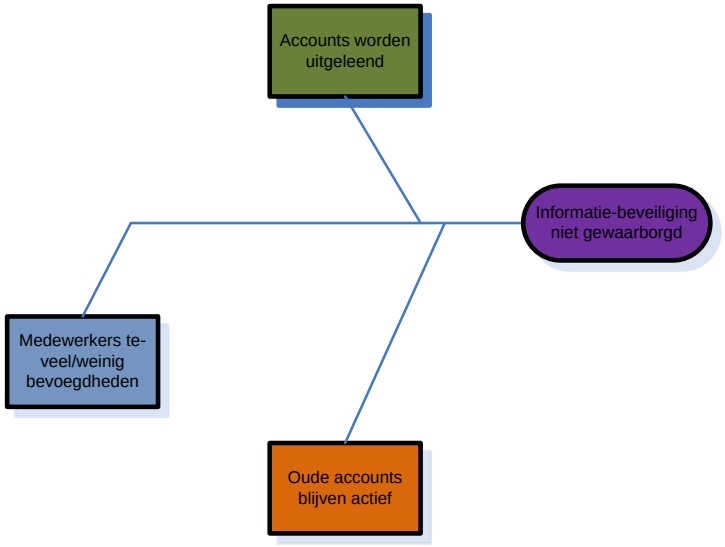
De drie problemen die ten grondslag liggen aan het niet waarborgen van de informatiebeveiliging zijn in dit hoofdstuk geanalyseerd om de onderliggende oorzaken aan het licht brengen. Door middel van een Ishikawa diagram, ook wel een visgraat diagram genoemd, worden de relaties tussen problemen en oorzaken weergegeven. De eerder, in

§2.2.1, genoemde problemen en het gevolg zijn in figuur 3 weergegeven. Door middel van interviews met sleutelfiguren, (zie tabel 5) is achterhaald wat de oorzaken zijn van de problemen. Elk van de problemen wordt nu nader beschreven. Aan het einde van dit hoofdstuk worden de oorzaken van de problemen ingevuld in de Ishikawa diagram.

3.1 Processen

Allereerst is er gekeken hoe de huidige situatie eruit ziet. In het model 'Blueprint for Process Analysis' (zie §1.3.7) is dit stap 3 'Document the process'. De huidige situatie wordt beschreven door de processen in kaart te brengen die van belang zijn. Op deze manier wordt het duidelijk welke sleutelfiguren er betrokken zijn bij het toekennen, muteren en intrekken van bevoegdheden voor ICT applicaties en kan er onderzocht worden waar de genoemde problemen precies uit ontstaan. De processen die te maken hebben met bevoegdhedenverstrekking zijn:

- het aanstellen van een medewerker bij het UMCG,
- het toekennen of muteren van bevoegdheden en
- het intrekken van bevoegdheden.



Figuur 4 Ishikawa met de drie hoofdproblemen.

Het is binnen het UMCG niet algemeen bekend hoe deze processen precies verlopen en wie op welk moment verantwoordelijk is.

In het kader van marktgericht werken, kwaliteitsverbetering, efficiëntieverhoging, organisatieverplatting en delegatie van taken verantwoordelijkheden en bevoegdheden moeten processen transparant en beheerst zijn. Dit niet

alleen om bijvoorbeeld ieders bijdrage aan een activiteit, proces en een integrale kostprijs te bepalen, maar ook om als management processen effectief te kunnen aansturen. Bedrijfsprocessen hebben betrekking op alle activiteiten binnen en direct samenhangend met het primaire proces van de organisatie. (Kleijn, H. Rorink, F. 2009:102-104)

3.1.1 Aanstelling medewerker

Het eerste proces wat is onderzocht is dat van de aanstelling van de medewerker. Wanneer een nieuwe medewerk

er in dienst komt, treedt er een proces in werking waarin formulieren worden verzameld en contracten opgesteld. Dit proces vindt hoofdzakelijk plaats op de P&O afdeling van een sector. De stappen gemaakt in dit proces zijn hier-

onder beschreven in tabel 3, in bijlage 2 is het stroomschema te zien.

De afhandeling van de aanstelling van de medewerker door de P&O afdeling duurt normaal gesproken rond de 21 werkdagen (circa 4 weken). De aanvraag van het netwerkaccount en de daarbij behorende bevoegdheden kan van start gaan als de medewerker in PEOPLESOFT (het personeelsinformatiesysteem) is geregistreerd. Er is dan een personeelsnummer beschikbaar die noodzakelijk is voor het aanvragen van bevoegdheden.

3.1.2 Toekennen of muteren van bevoegdheden

Het tweede proces wat beschreven wordt is het proces van het toekennen of het muteren van bevoegdheden. De medewerker is nu aangesteld en heeft bevoegdheden nodig of de medewerker wisselt van functie of afdeling en heeft nieuwe bevoegdheden nodig. Elke afdeling en elke sector hebben mensen die tekenbevoegd zijn. Zij mogen bevoegdheden aanvragen voor medewerkers die dat nodig hebben.

Stap	Omschrijving	Doorlooptijd (cumulatief) werkdagen	Verantwoordelijkheid
1	Start aanstellingstraject door inlevering aanstellingsdocumenten	0(0)	Leidinggevende
2	Invoeren gegevens in Oscar en inplannen A&G aanstellingsonderzoek en arbeidsvoorwaardengesprek	1(1)	P&O
3	Uitvoeren aanstellingsonderzoek en arbeidsvoorwaardengesprek	7(7)	A&G en P&O
4	Opmaken aanstellingscontract	2(-)	P&O
5	Tekenen aanstellingsformulieren	2(-)	P&O adviseur
6	Tekenen aanstellingsbesluit	2(-)	Sectordirecteur
7	Uitslag medische keuring	5(12)	A&G
8	Opsturen contract en retour ontvangen	7(19)	Nieuwe medewerker
9	Complete administratieve afhandeling	1(20)	P&O
10	Invoering nieuwe medewerker in PEOPLESOFT	1(21	PSA
11	Controle op de invoer en aanmelden voor bevoegdheden	1(21)	PSA

Tabel 3 Aanstellingstraject.

Een Tekenbevoegde krijgt opdracht van de leidinggevende van een medeweker of van de PSA medewerker om een aanvraag in te dienen. Een dergelijke aanvraag wordt op de afdeling ICT een Service Request genoemd en dat kan gaan om het toekennen of muteren van bevoegdheden. Een aanvraag kan op twee manieren ingediend worden door de Tekenbevoegde. Via IDS (ICT Digitale Service) of via ISS (ICT Self Service). ISS is een nieuwe methode voor aanvragen van bevoegdheden maar is nog niet geïntegreerd op

alle afdelingen en werkt (voorlopig) ook niet met elk soort aanvraag.

Een aanvraag met ISS werkt zonder tussenkomst van personen en wordt vrijwel meteen behandeld en teruggekoppeld aan de FNB'er of Tekenbevoegde. Bepaalde aanvragen zijn niet mogelijk om via ISS door te zetten, deze worden via IDS aangevraagd. Een dergelijke aanvraag komt binnen bij Bevoegdhedenbeheer in het programma CLIENTELE (CLIENTELE heeft tijdens de onderzoeksperiode het oudere VEGASUITE vervangen) waarna bevoegdhedenbeheer de realisatie daar tot stand brengt. Voor sommige applicaties is een licentie vereist. Dit wordt door Licentiebeheer gecontroleerd en toebedeeld. Als het om een aanvraag gaat voor toegang tot een systeem waar de gegevensbeheerder van het desbetreffende systeem eerst toestemming voor moet geven (bijvoorbeeld X/Care) dan wordt de aanvraag doorgezet naar Functioneel Gegevens Beheer. Uiteindelijk is het Bevoegdhedenbeheer die de behandelde aanvraag terugkoppelt naar de Tekenbevoegde.

In tabel 4 zijn de stappen weergegeven die plaatsvinden bij het aanvragen van bevoegdheden. In bijlage 2 is het stroomschema te zien. Voor het aanvragen van bevoegdheden wordt een doorlooptijd van 5 dagen gehanteerd.

3.1.3 Beëindiging arbeidsrelatie - Intrekken bevoegdheden

Het proces voor het intrekken van de bevoegdheden verloopt op vrijwel dezelfde manier als het toekennen of wijzigen van bevoegdheden. Wanneer het netwerkaccount is verwijderd kan de medewerker meteen ook niet meer bij zijn email en andere applicaties. De tekenbevoegde moet opdracht krijgen, van de leidinggevende van de uitdienst tredende medewerker, tot het indienen van een verzoek tot verwijdering. Bevoegdhedenbeheer verwijdert dan vervolgens het netwerkaccount.

Eens per half jaar wordt er een automatisch script uitgevoerd die alle oude netwerkaccounts verwijderd. Op deze manier zijn de netwerkaccounts, die men vergeten is op te

Stap	Omschrijving	Doorlooptijd (cumulatief) werkdagen	Verantwoordelijkheid
1	Initiatie proces door P&O of leidinggevende		P&O of leidinggevende
2	Aanvraag mutatie		Tekenbevoegde
3	Aanvraag mogelijk via ISS? ja=stap8 nee=stap4		Tekenbevoegde
4	Aanvraag via IDS		Tekenbevoegde
5	Behandeling door bevoegdhedenbeheer		Bevoegdhedenbeheer
6a	Licentie benodigd? ja=stap7a nee=stap8		Bevoegdhedenbeheer
7a	Uitgave licentie door Licentiebeheer >stap 9		Licentiebeheer
6b	Autorisatie benodigd? ja=stap7b nee=stap8		Bevoegdhedenbeheer
7b	Autorisatie door FGB >stap 9b		FGB
8	Aanvraag via ISS		Tekenbevoegde
9a	Automatische realisatie		Systeem
9b	Realisatie bevoegdhedenbeheer		Bevoegdhedenbeheer
10	Terugkoppeling naar FNB of Tekenbevoegde		Bevoegdhedenbeheer, systeem
11	Terugkoppeling naar medewerker	Norm: 5 dagen	Tekenbevoegde

Tabel 4 Toekennen of muteren van bevoegdheden.

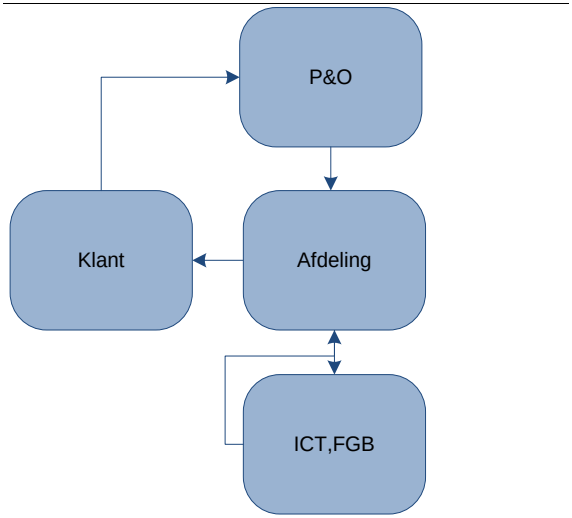
zeggen op het moment dat een medewerker uit dienst ging, niet meer bruikbaar.

Wanneer een netwerkaccount wordt opgezegd kan een medewerker niet meer bij zijn email en niet meer inloggen op de computers in het UMCG. Toegangsrechten binnen applicaties blijven wel bestaan maar zijn niet meer bruik-

baar omdat deze applicaties niet meer benaderbaar zijn. Dit zorgt voor 'vervuiling' in de systemen maar is geen risico voor de informatiebeveiliging.

3.1.4 Afdelingen en sleutelfiguren

Bij het verstrekken van ICT bevoegdheden spelen verschillende afdelingen en figuren een rol. De afdeling, waar de medewerker werkzaam is die bevoegdheden nodig heeft, zorgt voor de aanvraag van bevoegdheden. Daarnaast spelen de afdeling ICT, en bureau Functioneel- & gegevensbeheer een rol. Zij zorgen voor de realisatie van de bevoegdheden. Voordat bevoegdheden kunnen worden verstrekt moet de medewerker eerst in dienst zijn. Het aanstellingstraject wordt uitgevoerd door de afdeling P&O van de sector waarin de nieuwe medewerker wordt aangenomen. De Personeels- en salarisadministratie en Arbeid & Gezondheid spelen in dit traject ook een kleine rol.



Figuur 5 De relaties tussen afdelingen bij het bevoegdheidsproces.

Afdeling	Rol	Verantwoordelijkheid
ICT	Security Officer	Waarborging informatiebeveiliging, voldoen aan wet & regelgeving etc.
	Coördinator ICT bevoegdhedenbeheer	Coördineren werkzaamheden BHB
	Bevoegdhedenbeheerder	Behandelen van bevoegdheidsaanvragen
	Licentiebeheerder	Toekennen van licenties
FGB	Hoofd FGB / Opdrachtgever	Coördineren werkzaamheden FGB
	Functioneel Beheerder	Waarborging continuïteit en kwaliteit van een informatiesysteem
	Functioneel Gegevens Beheerder	Beheer van gegevens, data en informatie van een informatiesysteem
Sector medewerker	Sectordirecteur	Eindverantwoordelijke van een sector
Afdeling medewerker	Leidinggevende	Opdracht aan Tekenbevoegde voor aanvragen bevoegdheden
	Tekenbevoegde	Aanvragen bevoegdheden bij bevoegdhedenbeheer
	Nieuwe medewerker	
P&O	P&O medewerker	Uitvoeren van aanstellingstraject
PSA	PSA medewerker	Verwerken van mutaties op het gebied van personeels- en salarisadministratie.
A&G	A&G medewerker	Uitvoeren arbeidsvoorwaardengesprek

Tabel 5 Sleutelfiguren.

Hiernaast zijn drie processen omschreven. Het aanstellen van de medewerker, het toekennen of wijzigen van bevoegdheden en het intrekken van bevoegdheden. In §3.2 worden de processen en de eerder genoemde problemen geanalyseerd.

3.2 Bevindingen

Stap 3 van het model "Blueprint for proces analysis" (zie §1.3.7) is voltrokken in de vorige paragraaf. In deze paragraaf wordt stap 4: "Evaluate performance" uitgevoerd. Per probleem worden de gedane bevindingen beschreven.

3.2.1 Accounts worden uitgeleend

Een van de problemen die leiden tot een verminderde informatiebeveiliging in het UMCG is het uitlenen van accounts. Het uitlenen van accounts zorgt ervoor dat er niet meer te traceren is wie op welk moment toegang heeft tot gevoelige informatie. Gevoelige informatie kan in handen komen van onbevoegden, wat natuurlijk niet de bedoeling is.

Het uitlenen van accounts aan collega's blijkt voor te komen wanneer een nieuwe medewerker niet tijdig de juiste bevoegdheden heeft om zijn werk goed uit te kunnen voeren. Om dan toch de werkzaamheden te kunnen verrichten wordt er tijdelijk een account van een collega geleend.

Uit de oriënterende interviews en de resultaten van de audit is gebleken dat hier klaarblijkelijk erg gemakkelijk mee omgegaan wordt. De audit meldt dat er onvoldoende informatiebeveiligingsbewustzijn bij de medewerkers is waardoor zaken als het uitlenen van account gegevens te gemakkelijk plaatsvinden. Vanaf het moment dat een medewerker in dienst komt bij het UMCG wordt het belang van een goede informatiebeveiliging niet gecommuniceerd.

Het is dus enerzijds nodig om het informatiebeveiligingsbewustzijn bij de medewerkers te vergroten zodat toegangsrechten enkel gebruikt worden door de persoon die ze toegewezen heeft gekregen. Anderzijds is het belangrijk om te onderzoeken hoe bevoegdheden tijdig beschikbaar kunnen zijn. De bevoegdheden staan idealiter klaar op de dag van indiensttreding van de medewerker. Op deze manier wordt het uitlenen van accounts onnodig.

Tijdig klaarstaan bevoegdheden

Om na te gaan hoe bevoegdheden kunnen klaarstaan op de dag dat de nieuwe medewerker begint is onderzocht waardoor het komt dat dit niet altijd het geval is. Eerder is het proces van de aanstelling van de medewerker in kaart gebracht en vervolgens het aanvragen van de bevoegdheden.

Aanstellingstraject

Het proces van het aanvragen van bevoegdheden kan pas beginnen wanneer het aanstellingstraject is afgerond omdat aan het einde van het aanstellingstraject een personeelsnummer gegenereerd wordt die essentieel is bij het aanvragen van bevoegdheden. De systemen in het UMCG zijn afhankelijk van elkaar. Het aanstellingstraject is echter een traject waar veel partijen bij betrokken zijn. Afwezigheid door ziekte kan er voor zorgen dat het traject uitloopt. Daarnaast wordt er gemeld dat nieuwe medewerkers niet altijd tijdig het juiste papierwerk opleveren (denk aan diploma's, etc.). Tijdens het aanstellingstraject wordt PEOPLESOFT gebruikt als checklist om te kijken of de juiste papieren zijn opgeleverd.

Afdeling van nieuwe medewerker

Wanneer dit traject is afgesloten moet een Tekenbevoegde van de desbetreffende afdeling de bevoegdheden gaan aanvragen. Een Tekenbevoegde krijgt de opdracht tot zo'n aanvraag niet op een uniforme manier binnen. De opdracht kan komen van een leidinggevende, collega, P&O medewerker of de werknemer zelf. Aanvragen komen telefonisch, per mail, of worden mondeling gedaan.

3.2.2 Medewerkers met te veel of te weinig bevoegdheden

Een tweede probleem dat leidt tot een verminderde informatiebeveiliging is dat er medewerkers zijn in het ziekenhuis met te veel of juist te weinig bevoegdheden en toegangsrechten. Het hebben van teveel bevoegdheden en toegangsrechten resulteert in het feit dat de medewerker bij in informatie kan waar hij onbevoegd voor is. Het probleem van het hebben van te weinig bevoegdheden is dat de medewerker een manier gaat zoeken om toch zijn taken uit te kunnen voeren. Wat weer kan resulteren in het lenen

van een account van een collega die wel toegang heeft tot de benodigde informatie. Dit is in strijd met de wet- en regelgeving en kan een gevaar vormen voor de informatiebeveiliging en daarmee patiëntveiligheid.

Er zijn meerdere oorzaken voor het probleem dat medewerkers te veel of juist te weinig bevoegdheden hebben. Wanneer een medewerker bijvoorbeeld van afdeling wisselt of van functie verandert, heeft hij/zij vaak een ander pakket met bevoegdheden nodig. Het aanvragen hiervan gaat op de manier beschreven in §3.1.2. In dit proces gaat er iets mis. Van afdeling veranderde medewerkers hebben vaak nog de toegangsrechten van de oude afdeling of van hun oude functie. De tekenbevoegde van de nieuwe afdeling krijgt wel opdracht tot het aanvragen van de nieuwe bevoegdheden. Er wordt vaak echter geen opdracht gegeven tot het verwijderen van bevoegdheden.

Een andere oorzaak is dat het niet altijd duidelijk is voor de Tekenbevoegde wat er precies aangevraagd moet worden. Het aanvragen van bijvoorbeeld ZIS bevoegdheden kan erg complex zijn. Vaak worden dan bevoegdheden van een collega met een soortgelijk takenpakket gekopieerd. Die collega kan weer net andere bevoegdheden hebben dan de medewerker nodig heeft waardoor het bevoegdhedenpakket niet klopt.

3.2.3 Oude accounts blijven actief

Het derde probleem dat leidt tot een verminderde informatiebeveiliging is dat accounts actief blijven wanneer een medewerker uit dienst gaat. In de praktijk gebeurt het intrekken van bevoegdheden wanneer een medewerker uit dienst gaat, niet altijd. Hierdoor blijven toegangsrechten en netwerkaccounts actief wanneer de medewerker uit dienst treedt. Gebleken is dat de tekenbevoegde niet altijd opdracht krijgt voor het indienen van een verzoek tot het intrekken van bevoegdheden bij ICT.

3.3 Analyse

In deze paragraaf worden de bevindingen nader geanalyseerd.

3.3.1 Processen

De processen die van toepassing zijn op dit onderzoek kenmerken zich als secundaire of ondersteunende processen. In veel nieuwe literatuur wordt er, in tegenstelling tot de klassieke standaardwerken waar nauwelijks aandacht wordt besteed aan processen, juist wel aandacht geschonken aan processen. In veel organisaties zijn er spanningsvelden tussen organisatiestructuur en de bedrijfsprocessen. Wanneer er in organisatiestructuren gedacht wordt, ontstaat er een verticale organisatie. Medewerkers richten zich veel op hun eigen functie. De afdeling is heilig en problemen worden vaak over de muur van een andere afdeling geworpen in plaats van bij de rechtstreekse collega van een andere afdeling. De organisatiestructuur en de processtructuur dienen als een geheel te zijn ontworpen. Door te denken in processtructuur wordt deze hokjesgeest doorbroken. Er staat een dynamischere structuur die meer gericht is op klantwaarde en resultaten. (Kleijn, H. Rorink, F. 2009:102-104)

Het proces van het aanvragen van bevoegdheden, was binnen het UCMG, vóór het schrijven van dit rapport, niet transparant. Hierdoor is het niet duidelijk voor medewerkers binnen het proces wat precies het einddoel is en hoe hun gedeelte van het proces bijdraagt aan het geheel. Gemaakte fouten worden op deze manier minder snel herkend waardoor processen minder efficiënt verlopen.

3.3.2 Accounts worden uitgeleend

Informatiebeveiligingsbewustzijn van medewerkers in het UMCG laat te wensen over. Vanaf het moment dat een medewerker het UMCG binnenkomt wordt het belang van een goede informatiebeveiliging niet duidelijk gecommuniceerd. Binnen het UMCG komt het belang van een goede informatiebeveiliging van gebruikersaccounts en bevoegdheden onvoldoende naar voren. De werkgever moet ervoor zorgen dat je medewerkers hun werk naar wens doen. De werkgever is namelijk verantwoordelijk voor de daden van werknemers ook al zijn deze daden tegen de instructies in. (Roest, van der. O.A.P., 2006: 171-173) Daar komt nog bij dat je uit ethisch oogpunt als verantwoordelijke, de veiligheid en het welzijn van je klanten moet waarborgen. (Flederman, C.B.,2008: 68-72)

Het tijdig klaarstaan van bevoegdheden is essentieel voor een goede informatiebeveiliging en werkt efficiënter. Het uitlenen van accounts aan collega's wordt minder noodzakelijk waardoor dit niet zo vaak meer voor zal gaan komen. Redenen van het niet tijdig beschikbaar staan van bevoegdheden beginnen al in het aanstellingstraject.

Aanstellingstraject
Het is van belang dat het aanstellingstraject goed verloopt. De onderlinge afhankelijkheid van systemen zorgt er namelijk voor dat voordat er een netwerkaccount en andere bevoegdheden aangevraagd kunnen worden er een aantal zaken vereist zijn:
1. Personeelsnummer
2. Naam leidinggevende
3. Functienaam
4. Afdelingsnaam

Hierdoor is een goede afhandeling van de registratie van de medewerker door de P&O afdeling een pre. In §3.1.1 staan de stappen in het proces voor de aanstelling beschreven met de tijdsduur. De tijdsduur daarbij vermeld is gebaseerd op ervaringen. Het aanstellingsproces neemt 21 werkdagen in beslag. Na deze termijn kan de leidinggevende een opdracht geven aan de tekenbevoegde voor het aanvragen van bevoegdheden.

Men moet veel papierwerk afhandelen alvorens een medewerker in PEOPLESOFT ingeboekt staat en de rest van het traject kan beginnen. Het niet tijdig door de medewerker opleveren van de juiste documenten zorgt voor vertraging in dit proces. Doordat men PEOPLESOFT gebruikt als checklist om te kijken of alle documenten compleet zijn kan men niet eerder beginnen met aanvragen van bevoegdheden.

Een lopend ICT project binnen het UMCG heeft betrekking op dit gedeelte van het traject. Op dit moment is het zo dat in PEOPLESOFT uitsluitend personen zijn geregistreerd die daadwerkelijk in dienst zijn. Door het lopende project is het binnenkort is het mogelijk om een 'Person of Interest' in PEOPLESOFT in te voeren. Het is dan mogelijk een werknemer tot 40 dagen voor zijn indiensttreding in te voeren. Het aanvragen van bevoegdheden kan dan eerder starten.

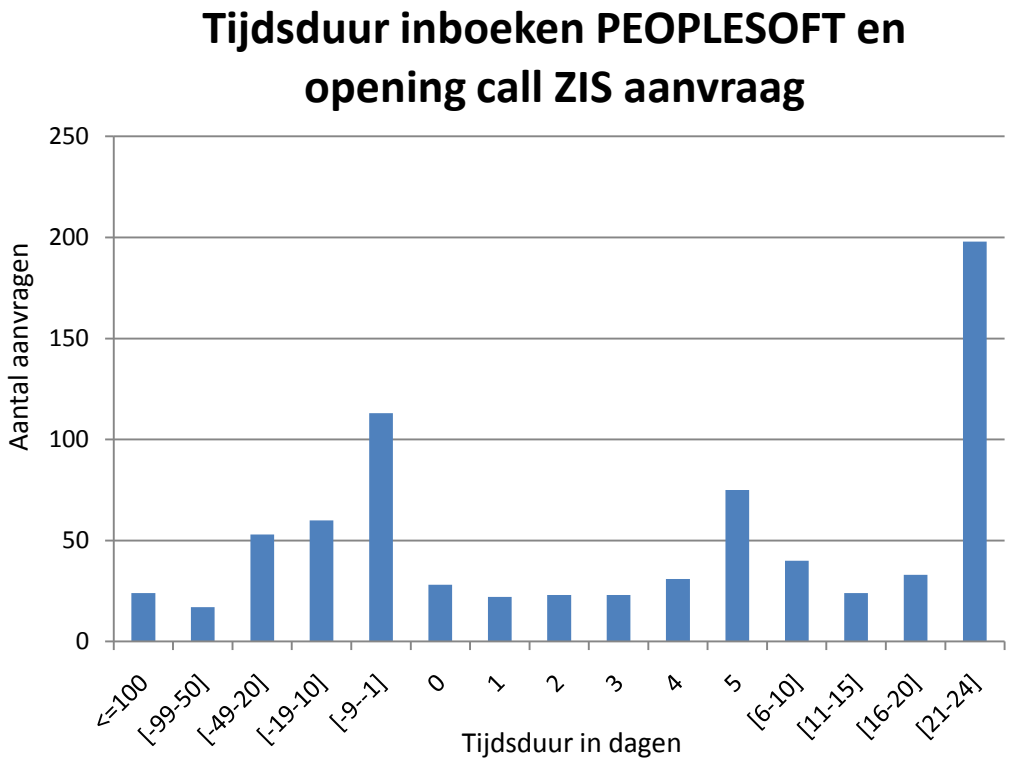
Als de medewerker eenmaal is ingeboekt moet de Tekenbevoegde opdracht krijgen voor het aanvragen van bevoegdheden. Via de systemen die in het UMCG is het gelukt datums te onttrekken die meer inzicht in geven in de tijdsduur tussen inboeken van de medewerker in PEOPLESOFT en het aanvragen van bevoegdheden door de Tekenbevoegde. De aanvragen van alle ZIS accounts over de periode 2010 zijn onderzocht. Dit account geeft toegang tot het ZIS systeem, is de basis voor veel zorgapplicaties en is voor medisch personeel een belangrijk account.

Figuur 6 geeft het tijdsbestek aan tussen het inboeken van de medewerker in PEOPLESOFT en het aanvragen van een ZIS account door de tekenbevoegde. Men noemt een aanvraag een 'call' De x-as betreft de intervallen van de duur van de aanvraag, de y-as hoe vaak een interval voor komt.

Er zijn negatieve waarden te zien in de grafiek. Dit kan meerdere oorzaken hebben. Ten eerste is het mogelijk een call eerder te plaatsen dan dat de medewerker ingeboekt is oftewel voordat hij feitelijk in dienst is. Men doet dit soms om zeker te zijn dat bevoegdheden geregeld zijn wanneer de medewerker in dienst gaat. Dit heet de workaround en is door sommige afdelingen niet gewenst. De prikkeling tot het verbeteren van de normale procedure wordt daarmee namelijk weggehaald. Een tweede mogelijkheid is dat een medewerker al langer in dienst is en gebruikt maak van ZIS maar van afdeling is gewijzigd. De inboekdatum in PEOPLESOFT is dan de wijzigingsdatum.

Een hoge positieve waarde kan eenvoudig verklaard worden. Een medewerker heeft in het begin wellicht geen ZIS account nodig en een aanvraag wordt pas later gedaan dan zijn indiensttreding. De hoge positieve waardes geven dus niet perse aan dat het proces ergens vertraging oploopt.

Zonder workaround of vertragingen in het proces wordt een ZIS call geopend op dezelfde dag als de inboekdatum in PEOPLESOFT. Gebleken is echter dat tussen deze twee het proces niet gestructureerd verloopt. Aanvragen bij de Tekenbevoegde komen telefonisch, per mail, of worden mondeling gedaan. De bevinding van McKinsey (zie Bijlage 3) dat processen in het UMCG niet altijd gestandaardiseerd zijn en dit ten koste gaat van de efficiëntie is hier dus zeker van toepassing.



Figuur 6 Tijdshiaat PEOPLESOFT en openen call (ZIS).

ICT/FGB

Een aanvraag wordt ingediend bij de afdeling ICT. ICT hanteert een norm voor het behandelen van aanvragen van 5 dagen. Op de afdeling ICT wordt er gebruik gemaakt van een helpdeskprogramma waarin aanvragen binnenkomen. De datum waarop de aanvraag binnenkomt en de datum waarop de aanvraag volbracht is zijn vergeleken.

De grafiek in figuur 7 geeft het tijdsbestek aan tussen de opening van een call voor de aanvraag van een ZIS account en het sluiten van die call daarvan. Dit proces is afhankelijk van de bevoegdhedenbeheerder en functioneel gegevens beheerder. Bij bepaalde niet gestandaardiseerde ZIS aanvragen gaat er namelijk een opdracht naar het bureau Functioneel- en gegevensbeheer. Nadat deze is verwerkt gaat de call weer terug naar bevoegdhedenbeheer. Standaard ZIS account aanvragen hoeven niet langs de Functioneel Gegevens Beheerder. Bevoegdhedenbeheer heeft een aantal profielen klaar staan die ze meteen kunnen koppelen aan de medewerker.

Op de x-as zijn de intervallen van de duur van de aanvragen weergegeven. De y-as geeft weer hoe vaak een interval voorkomt. ICT hanteert een norm van vijf dagen doorlooptijd voor het aanvragen van bevoegdheden. Zoals te zien in de grafiek vallen ze meestal ruim binnen de norm. 90,3% van de calls is binnen 5 dagen behandeld. 8,5% is binnen 10 dagen behandeld. Dan zijn er nog een paar uitschieters, die

Figuur 7 Tijdshiaat openen call en sluiten call (ZIS).

hebben soms als oorzaak dat een aanvraag gekoppeld wordt aan een specifieke datum waarop het ZIS account geactiveerd moet worden. De call wordt dan vaak pas gesloten op die datum, dit geeft dus een iets vertekend beeld.

Een voorbeeld van de database waaruit de gegevens zijn gehaald is te zien in bijlage 8: ZIS aanvragen.
Voor de aanvraag van een ADS netwerkaccount is het helaas niet mogelijk om, zoals bij het ZIS account, de inboekdatum van de medewerker in PEOPLESOFT te koppelen aan de aanvraagdatum. Dit komt omdat het personeelsnummer van de medewerker niet in een ADS call bekend is. Hierdoor is voor de aanvraag van een netwerkaccount enkel de aanvraag en sluitdatum van de aanvraag bekend (zie figuur 8).

De rode staafgrafiek is het totaal van alle aanvragen. Zoals te zien is, is iets meer dan 40% van alle aanvragen dezelfde dag nog behandeld. De blauwe grafiek geeft de aanvragen voor nieuwe netwerkaccounts weer. Groen is een aanvraag voor het wijzigen van een netwerkaccount. De reden dat de aanvragen opgesplitst zijn in categorieën is dat de aanvragen in categorie 'overig' veelal een gewenste ingangsdatum hebben. Het weergeven van deze aanvragen tussen de andere aanvragen zou een vertekend beeld geven.

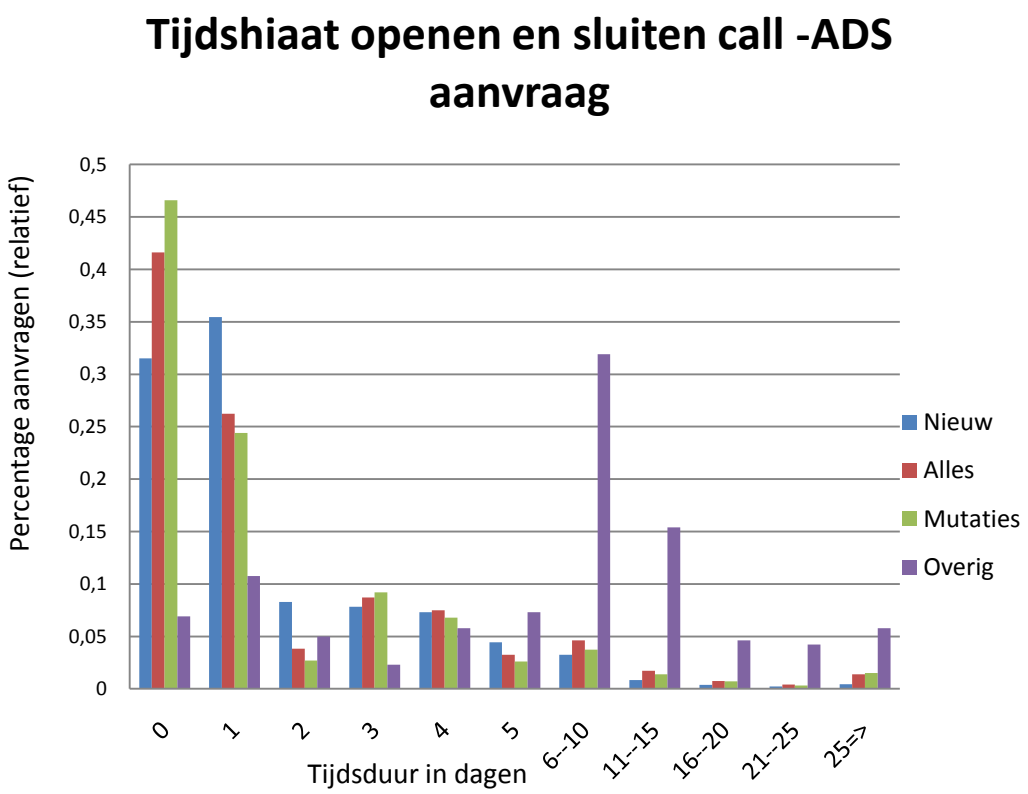
Slechts 5,13% van de aanvragen voor een nieuw netwerkaccount valt buiten de gehanteerde norm. Voor een aanvraag voor een mutatie van een netwerkaccount valt 7,67% buiten de gehanteerde norm. De overige aanvraag duren in bijna 62% van de gevallen, langer dan 5 dagen. Maar zoals eerder vermeldt zijn dit aanvragen met een specifieke ingangsdatum voor het aanmaken of muteren van een netwerkaccount. Een voorbeeld van de database waaruit de gegevens zijn gehaald is te zien in bijlage 9: ADS aanvragen.

3.3.3 Medewerkers met te veel of te weinig bevoegdheden

Door verschillende redenen (zie §3.2.2) zijn er in het UMCG medewerkers met te veel of te weinig bevoegdheden. Te veel bevoegdheden is in strijd met de wet- en regelgeving. Die meldt namelijk: “Gebruikers moeten uitsluitend toegang kunnen krijgen tot diensten, systemen en gegevens waar voor zij zijn geautoriseerd.”

Te weinig bevoegdheden kan leiden tot het onderling uitlenen van accounts wat ook weer in strijd is met bovenstaande regel.

Rolonduidelijkheid is een oorzaak van medewerkers met een onjuist bevoegdhedenpakket. Interne communicatieprocessen, geïnitieerd door het management, vinden plaats om de organisatiemedewerkers voor interne, maar ook externe, ontwikkelingen te informeren. Interne communicatie



Figuur 8 Tijdshiaat opening call en sluiten call (ADS).

vindt ook plaats om de rol, en de taken daarbinnen, van de medewerkers te verduidelijken en hun activiteiten te coördineren. Dit moet medewerkers in staat stellen beter de verantwoordelijkheid voor hun eigen functioneren te nemen. Hierbij wordt, voor zover dat mogelijk is, rekening gehouden met de normen, waarden, verwachtingen, doelstellingen en wensen van de medewerkers. (Kleijn, H. Rorink, F. 2009: 91)
Een veel voorkomend communicatie- en informatieprobleem is: "Gebrek aan taakinformatie en de bijbehorende verantwoordelijkheden en bevoegdheden bij organisatiemedewerkers"
Bovenstaand lijkt ook het geval te zijn in het UMCG. Waarom dat zo is wordt verder toegelicht:

Voor een goede, adequate uitoefening van taken is het noodzakelijk dat de medewerker beschikt over informatie met betrekking tot zijn rol en de daarbij behorende taken. Dit betreft de inhoud van de taken en de daarbij bijbehorende verantwoordelijkheden. Als dit onvoldoende gebeurt, ontstaat na verloop van tijd conflicten tussen medewerkers onderling, tussen leidinggevenden onderling en tussen medewerkers enerzijds en leidinggevende anderzijds. Dit verschijnsel wordt rolonduidelijkheid genoemd. Gaat dit gebrek gepaard met slecht/onvoldoende leidinggeven dan krijgen medewerkers de kans om een eigen 'toko te runnen', met als gevolg een ondergraving van het functioneren van het afdelingsteam en misschien de totale organisatie. (Kleijn, H. Rorink, F. 2009: 91)

Werknemers die tekenbevoegd zijn doen dat werk er extra bij naast hun andere takenpakket. Tekenbevoegdheid is een rol die een medewerker op zich neemt en geen functie op zich. Tijdens het onderzoek is naar voren gekomen dat er geen training of inwerk periode is voor Tekenbevoegden. Doordat men niet ingewerkt wordt, weet men niet altijd wat de huidige procedures zijn en gaat iedereen het werk op zijn eigen manier doen. Er ontstaat onduidelijkheid in wat er precies aangevraagd moet worden en op wat voor manier dit moet gebeuren. De manier waarop de Tekenbevoegden toegangsrechten aanvragen verandert ten opzichte van elkaar en er ontstaat een waaier van verschillende werkwijzen binnen de muren van het UMCG. Adviesbureau McKinsey heeft het UMCG geadviseerd (zie §2.4) om, desondanks de opdeling in sectoren, toch UMCG brede werkwijzen aan te houden. Door structurering van processen verlopen deze efficiënter en zijn ze beter controleerbaar.

Het aanvragen van een ZIS account is erg lastig. Er zijn een aantal standaard bevoegdhedenpakketten of profielen aangemaakt die gekoppeld kunnen worden aan bepaalde functies. Wat vaak gebeurd is dat bevoegdheden van een collega met een soortgelijk takenpakket gekopieerd worden. Hier kunnen bevoegdheden bij zitten die toegang geven tot systemen waar een medewerker niet bij zou mogen komen.

Niet alleen voor Tekenbevoegden is er sprake van rolonduidelijkheid maar ook voor leidinggevenden. Het is niet altijd duidelijk waar de grenzen van verantwoordelijkheid liggen waardoor van afdeling of functie wisselende medewerkers niet ontnomen worden van de oude bevoegdheden en toegangsrechten.

Leidinggevenden weten blijkbaar niet goed dat zij eindverantwoordelijk zijn voor de acties van hun ondergeschikten en dat zij er zorg voor moeten dragen dat informatie van hun afdeling enkel toegankelijk is voor de juiste personen. Zij zijn degene die opdracht moeten geven aan de Tekenbevoegde om bevoegdheden te ontnemen. (Roest, van der. O.A.P., 2006:171-173)

Het is ook niet altijd even duidelijk welke toegangsrechten een medewerker heeft. Wanneer de Tekenbevoegde dus toch een opdracht krijgt tot het intrekken van bevoegdheden is het erg lastig te bepalen wat er precies ingetrokken moet worden.

3.3.4 Oude accounts blijven actief

Bij het beëindigen van de arbeidsrelatie van een medewerker is het noodzakelijk dat de bevoegdheden van de desbetreffende medewerker worden ingetrokken. Als dit niet gebeurt, kan een kwaadwillende ontslagen medewerker patiëntgegevens inzien of zelfs veranderen. De verantwoordelijkheid voor het intrekken van bevoegdheden ligt zou moeten liggen bij de leidinggevende, al is dit niet eenduidig vast gelegd. De leidinggevende is verantwoordelijk voor de toegangsrechten die zijn medewerkers hebben. De leidinggevende moet de opdracht tot intrekken van be-

voegdheid geven aan de Tekenbevoegde van de afdeling. Dat dit noodzakelijk is, wordt vergeten of is niet bekend.

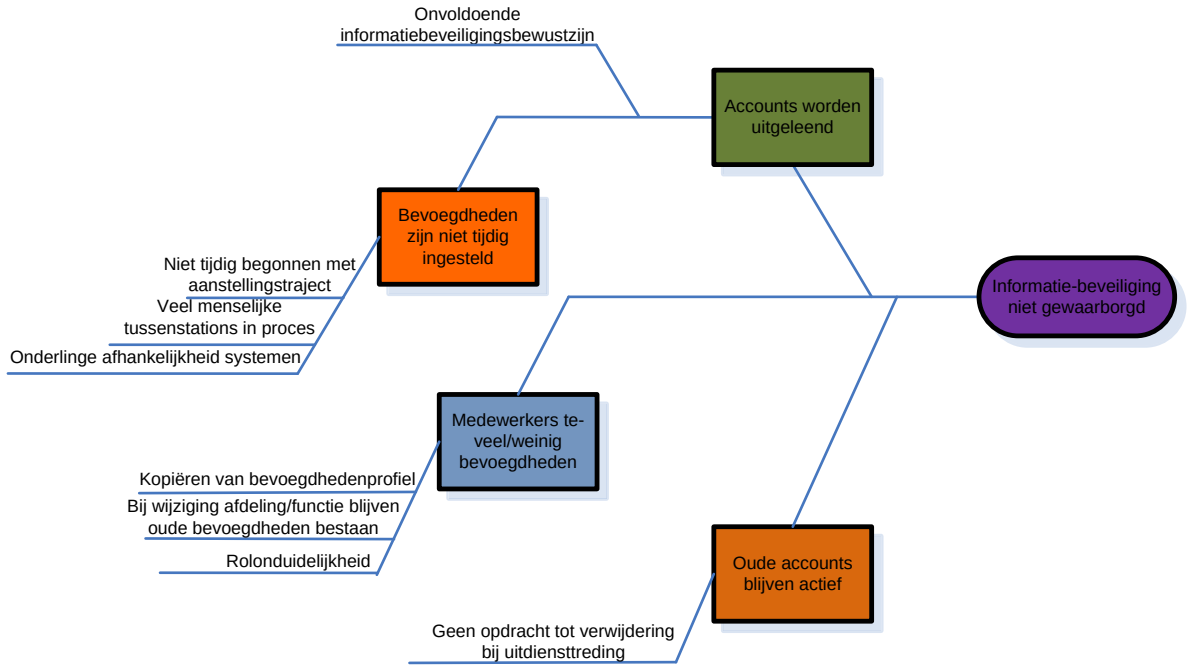
Accounts die een lange tijd niet gebruikt zijn worden op inactief gezet. Dit wordt gedaan om accounts van medewerkers die inmiddels uit dienst zijn te verwijderen. Hier wordt het probleem echter niet mee opgelost. Tegenwoordig kun je met WOA (Werkplek Op Afstand) blijven inloggen op je webmail waardoor het account actief blijft en bevoegdheden dus aanblijven.

Identity Access Management is een project dat op moment van schrijven uitgevoerd wordt. Dit project koppelt het personeelsbestand aan het ADS. Makkelijker gezegd: persoonsgegevens en inloggegevens worden gekoppeld. Voor het intrekken van bevoegdheden houdt dit in dat zodra een medewerker uit dienst gaat, hij/zij automatisch ook niet meer kan inloggen op het netwerk. Tot voor kort was het zo dat wanneer een medewerker uit dienst ging, het netwerkaccount handmatig opgezegd moest worden. ZIS bevoegdheden blijven echter nog wel actief.

3.3.5 Ishikawa met hoofdproblemen en oorzaken

Aan de hand van de analyse hierboven is de in figuur 8 weergegeven Ishikawa diagram ingevuld. Een uitgebreid overzicht van de problemen met oorzaken is terug te vinden in bijlage 5: Oorzaken uitgebreid

Dit hoofdstuk begon met het aanstippen van de drie hoofdproblemen rond het verstrekken van bevoegdheden die zorgen voor een verminderde informatiebeveiliging. De problemen zijn stuk voor stuk behandeld en geanalyseerd. Vervolgens zijn de oorzaken van de problemen aangewezen. Figuur 9 geeft de problematiek overzichtelijk weer. In bijlage 5 zijn de uitgewerkte problemen met oorzaken te vinden.



Figuur 9 Ishikawa met de drie hoofdproblemen en oorzaken daarvan.

4 Conclusie en aanbevelingen

4.1 Conclusie

Hokjesstructuur
Accounts worden tussen collega's onderling uitgeleend doordat bevoegdheden niet tijdig of volledig beschikbaar zijn. De processen van het aanstellen van een nieuwe medewerker en het aanvragen van zijn/haar bevoegdheden zijn niet transparant en duidelijk voor sleutelfiguren in het proces. In het kader van marktgericht werken, kwaliteitsverbetering, efficiëntieverhoging, organisatieverplatting en delegatie van taken verantwoordelijkheden en bevoegdheden moeten processen transparant en beheerst zijn. (Kleijn, H. Rorink, F. 2009:102-104) Doordat dit niet het geval is, is er een hokjesstructuur ontstaan die niet zozeer gericht is op resultaat. Voor medewerkers binnen het proces is niet duidelijke wat precies het einddoel is en hoe hun gedeelte van het proces bijdraagt aan het geheel. Gemaakte fouten worden op deze manier minder snel herkend waardoor processen minder efficiënt verlopen dan mogelijk en wenselijk zou zijn.

Ongestructureerd en bottlenecks in het proces
Onderlinge afhankelijkheid van systemen zorgt ervoor dat er bottlenecks ontstaan in het systeem. Voordat bevoegdheden kunnen worden aangevraagd dient namelijk het aanstellingstraject eerst afgerond te zijn. De vele stappen en menselijke tussenstations in dit traject kunnen allemaal voor vertraging zorgen. Omdat PEOPLESOFT gebruikt wordt als checklist om te controleren of het benodigde papierwerk verzameld is staat het traject stil tot al het papierwerk compleet is.

Het aanstellingstraject duurt doorgaans 21 dagen. Dan kan er van start gegaan worden met het aanvragen van bevoegdheden. De norm daarvoor is 5 dagen. Voor verwerking door de tekenbevoegde en terugkoppeling naar de medewerker wordt 2 dagen gesteld. Afgerond naar boven duurt het dus ongeveer 6 weken voordat een medewerker administratief verwerkt is in het UMCG. Wanneer er dus zes weken van te voren begonnen wordt met het aanstellingstraject kan de medewerker tijdig beschikken over zijn bevoegdheden.

Op dit moment is het zo dat in PEOPLESOFT uitsluitend personen zijn geregistreerd die daadwerkelijk in dienst zijn. Door een lopend ICT project is het binnenkort is het mogelijk om een 'Person of Interest' in PEOPLESOFT in te voeren. Het is dan mogelijk een werknemer tot 40 dagen voor zijn indiensttreding in te voeren. Het aanvragen van bevoegdheden kan dan al van start gaan als nog niet al het papierwerk rond is. Op deze manier kunnen bevoegdheden tijdig klaargezet worden. Werknemers kunnen op dag van indiensttreding direct aan het werk en de noodzaak om accounts onderling uit te lenen verdwijnt.

Rolonduidelijkheid
Gebrek aan taakinformatie en de bijbehorende verantwoordelijkheden en bevoegdheden bij organisatiemedewerkers is een veelvoorkomende fout binnen organisaties. (Kleijn, H. Rorink, F. 2009: 91) Dit fenomeen wordt rolonduidelijkheid genoemd. Door rolonduidelijkheid is het niet transparant welke bevoegdheden er aangevraagd moeten worden. Verkeerde bevoegdheden worden dan aangevraagd of door het kopiëren van het bevoegdhedenpakket van een collega met een soortgelijk takenpakket krijgt een medewerker onjuiste bevoegdheden toegekend. Door rolonduidelijkheid verandert ook de manier waarop de Tekenbevoegden toegangsrechten aanvragen ten opzichte van elkaar. Er ontstaat hierdoor een waaier van verschillende werkwijzen binnen de muren van het UMCG. Wanneer een medewerker de afdeling verlaat of van functie verandert, dienen zijn oude bevoegdheden ontnomen te worden. Leidinggevenden weten vaak niet dat zij hiervoor verantwoordelijk zijn of deze processtap wordt simpelweg vergeten door gebrek aan een gestructureerd proces.

Tekenbevoegden krijgen niet altijd opdracht tot verwijdering van bevoegdheden wanneer een medewerker uit dienst treedt. Dit wordt vergeten door leidinggevenden of is helemaal niet bekend. Hierdoor blijven accounts actief nadat de medewerker uit dienst is. Een lopend project binnen het UMCG heeft als doel het koppelen van het personeelsinformatiesysteem PEOPLESOFT aan het ADS. Wanneer een medewerker dan uit dienst gaat en uit

PEOPLESOFT wordt gehaald, dan verdwijnt automatisch zijn netwerkaccount. Toegang tot overige systemen is hiermee onmogelijk.

De werkwijzen omtrent het bevoegdheidverstrekkingsproces zijn niet UCMG breed gelijk. Ook verlopen bepaalde stappen in het proces niet gestructureerd waardoor er fouten ontstaan. Het gebrek aan een UMCG breed, gestandaardiseerd proces komt meer voor in het UMCG en is ook wat McKinsey is opgevallen. Doelmatigheid en efficiëntie hebben hieronder te leiden.

4.2 Aanbevelingen

In deze paragraaf worden aanbevelingen gegeven voor het verbeteren van het bevoegdheidverstrekkingsproces om daarmee de problemen omtrent informatiebeveiliging op te lossen. In het model 'Blueprint for process analysis' (zie §1.3.7) is dit stap 5: 'Redesign the process'.

De kritische succes factoren waaraan de situatie zou moeten voldoen zijn opgesteld in §2.2.1 en worden hieronder nog een keer aangehaald.

Nr	KSF
1	Medewerkers gebruiken hun account uitsluitend voor zichzelf
2	Gebruikers moeten uitsluitend toegang kunnen krijgen tot diensten, systemen en gegevens waarvoor zij zijn geautoriseerd.
3	UMCG breed standaard werkwijze gebruiken
4	Meer standaardisatie nodig om efficiëntie te vergroten

Tabel 2 Kritische succes factoren.

De aanbevelingen zijn gecategoriseerd in technische, organisatorische en sociaalbeleidsmatige aanbevelingen.

4.2.1 Technische aanbevelingen

Aanbeveling-1: Person of Interest
Door te werken naar de mogelijkheid van de 'Person of interest' in PEOPLESOFT wordt het mogelijk gemaakt om een personeelsnummer te genereren alvorens de medewerker in dienst is. Het proces van het aanvragen van bevoegdheden hoeft dan niet te wachten op gereed stelling van alle benodigde papieren. De medewerker blijft als ´Person of Interest´ geregistreerd staan totdat al het papierwerk compleet is. Op deze manier wordt de vertraging omzeild die veroorzaakt wordt doordat PEOPLESOFT als checklist gebruikt wordt. Het netwerkaccount van de medewerker hoeft dan alleen nog maar geactiveerd te worden op de dag van indiensttreding. . Als accounts van werknemers tijdig klaar staan is er geen reden meer voor het lenen van accounts van collega's.

Aanbeveling-2: Identity Access Management
Door gebruik te maken van Identity Access Management worden PEOPLESOFT en ADS gekoppeld. Een netwerkaccount wordt dan automatisch aangemaakt bij de registratie in PEOPLESOFT en automatisch verwijderd bij uitdiensttreding. Het probleem van oude accounts die actief blijven worden op deze manier aangepakt. Ook zal het aanvragen van een ADS netwerkaccount sneller verlopen. Dit project loopt op het moment al maar is cruciaal gebleken voor het oplossen van het probleem van het aanblijven van accounts na uitdiensttreding. Het UMCG wordt aanbevolen om dit project te prioriteren en UMCG breed uit te rollen zodat de informatiebeveiliging op dit punt versterkt wordt.

Aanbeveling-3: Automatiseren
Gebruik maken van Identity Access Management voor ZIS. Identity Access Management zorgt voor een koppeling tussen PEOPLESOFT en ADS. Ideaal zou zijn als ZIS ook soortgelijk gekoppeld wordt. Wanneer een medewerker wordt ingeboekt in PEOPLESOFT wordt de medewerker direct gekoppeld aan een afdeling, functiegroep en rol. Automatisch worden dan de juiste bevoegdheden gekoppeld die de medewerker nodig heeft om op zijn afdeling in zijn functiegroep en met zijn rol goed te kunnen functioneren. Op deze manier hoeft de Tekenbevoegde enkel de aanvraag te controleren en door te voeren. Op deze manier worden ook alle ZIS bevoegdheden bij uitdiensttreding verwijderd Automatiseren zorgt voor minder risico op menselijke fouten in het proces en snellere doorlooptijden. Bevoegdheden zijn zo eerder en juister ingesteld. Er is minder reden voor het uitlenen van accounts en medewerkers hebben het bevoegdhedenpakket die bij hun functie, rol en afdeling past.

Aanbeveling-4: Logboek
Binnen het UMCG zorgen voor een logboek waar de loopbaan qua bevoegdheden van iedere medewerker in staat vermeld. Op deze manier wordt inzicht gecreëerd in de ooit toegekende bevoegdheden en kan altijd gezien worden welke bevoegdheden op het moment toegewezen zijn. Op deze manier kan gekeken worden of de toegekende bevoegdheden terecht zijn toegekend en of bij mutaties de oude bevoegdheden wel zijn ingetrokken. De Tekenbevoegden en leidinggevenden van medewerkers zouden toegang tot deze database moeten hebben.

Aanbeveling-5: Verzamelen gegevens
De taak van het verzamelen van gegevens, benodigd voor het indienen van een aanvraag, ontnemen van de Tekenbevoegden. Afdelingsmanagers of personeelsadministratie medewerkers moeten zorgen dat de juiste complete gegevens bij de Tekenbevoegde terecht komen. Dit door middel van een digitaal aanvraag formulier dat vereist dat alle velden zijn ingevuld voor verzending. ISS moet als het ware een niveau omhoog getild worden.

4.2.2 Organisatorische aanbevelingen

Aanbeveling-6: Auditeren
Periodiek auditeren op naleving van de gestelde wet- en regelgeving omtrent informatiebeveiliging. Niet alleen verhoogt dit het informatiebeveiligingsbewustzijn, het beleid wordt ook getest en kan, waar nodig, aangescherpt worden. Dit bevordert het verandertraject. Bij het periodiek auditeren controleren of de sleutelfiguren in de processen voldoen aan de gestelde maximale werktijd eisen. Op deze manier wordt het verantwoordelijkheidsgevoel gestimuleerd.

Aanbeveling-7: Rolonduidelijkheid verbeteren
De taken van alle medewerkers binnen het proces moeten duidelijk worden. Gedecentraliseerde medewerkers zoals Tekenbevoegden en leidinggevenden hebben een opfriscursus ICT bevoegdheden nodig. Wanneer tekenbevoegdheid wordt overgedragen op een andere medewerker dan dient deze ingewerkt te worden. Verder dient er een handleiding beschikbaar te zijn op het Intranet over het aanvragen van bevoegdheden.

Aanbeveling -8: Transparant maken van processen
Door het transparant maken van processen worden sleutelfiguren in het proces gestimuleerd om te denken in resultaten in plaats van niet verder te kijken dan het eigen takenpakket. Voor de start van het onderzoek was er niet algemeen bekend hoe de processen precies liepen. In dit onderzoek zijn de processen in kaart gebracht met behulp van BPM/One. Door het communiceren van de processen richting de medewerkers wordt het voor hen duidelijk waar fouten kunnen ontstaan en bij welke personen het proces stil ligt. Communicatie verloopt dan sneller zodat incidenten worden voorkomen of eerder zijn opgelost. Vertragingen in het proces komen zo minder vaak voor waardoor bevoegdheden ook weer eerder klaar staan.

Aanbeveling-9: UMCG brede gestandaardiseerde werkwijzen
Door het UMCG heen gestandaardiseerde werkwijzen gebruiken. Op dit moment gaan niet alle stappen in het traject op eenzelfde manier. Hierdoor verlopen aanvragen rommelig. Een voorbeeld hiervan is om één manier van indienen van aanvragen bij een Tekenbevoegde instellen om de kans op fouten te verkleinen. Dit zou moeten gebeuren met een digitaal aanvraag formulier. Op deze manier is de kwaliteit van het werk van de Tekenbevoegden ook te meten.

4.2.3 Sociaalbeleidsmatige aanbevelingen

Aanbeveling-10: Informatiebeveiligingsbewustzijn verhogen
Medewerkers op de hoogte brengen van de gevaren van het niet voldoen aan de informatiebeveiligings wet- en regelgeving. Medewerkers weten namelijk niet wat de gevolgen zijn en zien de gevaren dus ook niet.
Aanleveren van gebruikersnaam en wachtwoord in een gesloten envelop met beveiligingsinstructies. Hierdoor krijgt een nieuwe medewerker direct een goed beeld van het belang van veiligheid. Met een verhoogd informatiebeveiligingsbewustzijn lenen medewerkers accounts minder snel aan elkaar uit. Ook wordt er beter gelet op welke bevoegdheden en toegangsrechten een medewerker krijgt. Ook wordt er dan beter gelet opdat gebruikers uitsluitend toegang kunnen krijgen tot diensten, systemen en gegevens waarvoor zij zijn geautoriseerd.

4.2.4 Mogelijk vervolg onderzoek

Exacte tijden aanstellingstraject
In het onderzoek is gekeken naar de doorlooptijden van het bevoegdheden aanvraag proces. Hierbij is gekeken of ICT voldeed aan de gestelde eisen. Ook is er gekeken hoe lang de tijd bedroeg tussen het invoeren van een nieuwe medewerker in PEOPLESOFT tot dat de aanvraag van de Tekenbevoegde naar ICT werd doorgevoerd. De tijd van de aanvraag van de invoer in PEOPLESOFT totdat de aanvraag bij de tekenbevoegde terecht kwam is niet gemeten. Dit komt doordat er niet één universele manier is voor een bevoegdheden aanvraag bij de Tekenbevoegde. Ook kan hierdoor niet de tijd dat de aanvraag bij de Tekenbevoegde ligt gemeten worden. Wel zou er gekeken kunnen worden wat de data zijn van het aanstellingsgesprek en deze koppelen aan de data van de invoer in PEOPLESOFT. De exacte tijd van de start van het proces tot de invoer in PEOPLESOFT kan dan gemeten worden. Op deze manier kan berekend worden hoe lang het proces bij P&O/PSA ligt. De doorlooptijd in tabel 3 is namelijk gebaseerd op schattingen en inzicht van geïnterviewde medewerkers. Uit de exacte data komen misschien redenen naar voren die een optimalisatie van het aanstellingstraject verantwoorden.

Standaard profielen.
Voor het automatiseren van het bevoegdheidsproces zou er onderzoek uitgevoerd moeten worden naar het standaardiseren van profielen zodat in PEOPLESOFT snel het juiste bevoegdhedenpakket ingesteld kan worden.
Er moeten standaardbevoegdheden komen voor afdelingen, functies en rollen.

In dit hoofdstuk zijn conclusies getrokken uit de geconstateerde problematiek. Vervolgens zijn er aanbevelingen aan het UMCG gedaan die de problematiek moeten aanpakken. In hoofdstuk 5: Implementatie wordt er beschreven hoe de aanpassingen het best doorgevoerd kunnen worden.

5 Implementatie

5.1 Stappenplan

Om succesvol de implementatie van de gegeven adviezen door te kunnen voeren wordt aangeraden om hier een werkgroep voor op te zetten. Ter voorbereiding van deze implementatie wordt een mogelijk stappenplan gegeven.

Hier in is vermeld wat, wanneer gedaan moet worden. Hierin is ook te zien wie eindverantwoordelijk is voor de gezette stap. Aan het einde van het schema kan afgevinkt worden welke stappen zijn volbracht of afgerond.
Onder het stappenplan is in te zien welke actie welke adviezen implementeert.

Actie nummer	Actie	Sep.	Okt.	Nov.	Dec.	Jan.	Eindverantwoordelijk
1	Opstellen Implementatiegroep die de implementatie van de aanbevelingen ter verbetering van de informatiebeveiliging gaat doorvoeren.	X					Opdrachtgever
2	IAM	X					Implementatiegroep
3	Opstellen UMCG brede werkwijze Tekenbevoegden	X					Implementatiegroep
4	Invoeren UMCG brede werkwijze Tekenbevoegden			X			Implementatiegroep
5	Aanvraag formulier aanmaken voor Tekenbevoegden	X					Implementatiegroep
6	Invoeren gebruik aanvraag formulier Tekenbevoegden			X			Implementatiegroep
7	ZIS en PEOPLESOFT applicatiebeheerders en bouwers samen brengen om de mogelijkheden van de koppeling te bespreken	X					Implementatiegroep
8	Koppeling ZIS en PEOPLESOFT					X	Implementatiegroep
9	Aanmaken logboek bevoegdheden medewerkers	X					Implementatiegroep
10	Start gebruik logboek bevoegdheden		X				Implementatiegroep
11	Inwerkcursus Tekenbevoegden opstarten	X					Implementatiegroep
12	Huidige Tekenbevoegden de cursus ter opfrissing laten volgen			X			Implementatiegroep
13	Document aanmaken met gestelde eisen aan Tekenbevoegden met vermelding van werkwijzen	X					Implementatiegroep
14	Nieuwsbrief opstellen en versturen om medewerkers op de hoogte te brengen van de gevaren omtrent informatiebeveiliging	X					Implementatiegroep
15	Starten controles informatiebeveiliging en werktijden.			X			Implementatiegroep
16	Person of Interest mogelijkheid realiseren	X					Implementatiegroep
17	Duidelijk in kaart brengen en houden van de processen omtrent bevoegdheden afgifte, mutaties en afnamen. Alle mogelijkheden overzichtelijk hebben.			X			Implementatiegroep

Tabel 6 Implementatiestappenplan

5.2 Acties en Adviezen

Actienummer	Adviesnummer	Advies
1		Aanbevelingen invoeren (implementatie)
2	3	Aanbeveling-3: Identity Access Management
3,4	6	Aanbeveling-6: UMCG brede gestandaardiseerde werkwijzen
5,6	6, 10	Aanbeveling-6: UMCG brede gestandaardiseerde werkwijzen Aanbeveling-10: Verzamelen gegevens
7,8	4	Aanbeveling-4: Automatiseren
9,10	9	Aanbeveling-9: Vastleggen van bevoegdheden
11,12,13	5	Aanbeveling-5: Rolonduidelijkheid verbeteren
14	7	Aanbeveling-7: Informatiebeveiligingsbewustzijn verhogen
15	8	Aanbeveling-8: Auditeren
16	2	Aanbeveling-2: Person of Interest
17	1	Aanbeveling -1: Transparant maken van processen

Tabel 7 Acties en adviezen

5.3 Prioriteit

Actienummer	Prioriteit: Laag	Gemid-deld	Hoog	Zeer hoog	Verklaring/Omschrijving
1				X	Informatiebeveiliging moet gewaarborgd worden.
2				X	Medewerkers die uit dienst zijn getreden mogen nooit daarna nog toegang hebben tot gegevens.
3		X			Proces optimalisatie
4		X			Proces optimalisatie
5		X			Proces optimalisatie
6		X			Proces optimalisatie
7			X		Proces optimalisatie, deze stap is nodig voor Actie 8
8			X		Proces optimalisatie, wachttijden verkorten.
9		X			Controle document
10		X			Controle document
11			X		Sleutelfiguren moet weten wat ze doen
12			X		Sleutelfiguren moet weten wat ze doen
13			X		Sleutelfiguren moet weten wat ze moeten doen
14				X	Informatiebeveiligings bewustzijn moet zo snel mogelijk worden verhoogd.
15	X				Eerst moeten er aanpassingen gedaan worden voordat je kunt meten of deze aanpassingen effect hebben gehad.
16			X		Proces optimalisatie. Wachttijden verkorten
17		X			Door dit onderzoek zijn de processen: afgifte, mutaties en afname pas in kaart gebracht

Tabel 8 Prioriteiten

Literatuurlijst

Ondersteunende literatuur

Grit, R. (2005) Project Management. Groningen. Uitgeverij: Wolters Noordhoff

Kempen, P. Keizer, J. (2010). Competent afstuderen en stagelopen. Een advieskundige benadering. Groningen. Uitgeverij Wolters Noordhoff

Mertens, J. (2008) Praktijkonderzoek voor bachelors. Bussum. Uitgeverij Coutinho

Verschuren, P. Doorewaard, H., (2003). Het ontwerpen van een onderzoek. Utrecht. Uitgeverij LEMMA BV.

Literatuur

CBP, IGZ., (2008) Informatie beveiliging in ziekenhuizen voldoet niet aan de norm, Den Haag

Fledderman, C.B. (2008) Engineering Ethics. Upper Saddle River, New Jersey

Gramsbergen-Hoogland, Y.H. Molen, van der, H.T., (2005) Gesprekken in organisaties. Groningen. Uigeverij Wolters Noordhoff

Kleijn, H. Rorink, F. (2009) Verandermanagement. Amsterdam. Uitgeverij Pearson Education

Krajewski, L. Ritzman, L. Malhotra, M., (2007) Operations Management. Processes and Value Chains. Upper Saddle River, New Jersey

Krogt, van der, L., (2006) Van beleid naar naleving. Groningen, UMCG.

McKinsey&Company. (2010) Samenvatting: Klaar voor de toekomst, Algemene en medische ondersteuning, Groningen

Nederlands Normalisatie Instituut, 'NEN7510', http://www.nen7510.org, 15 juni 2011
Rijksoverheid, 'NEN7510 en het EPD', 12 juni 2011

Roest, van der, O.A.P. (2006) Basisboek Recht. Groningen/Houten. Uitgeverij Wolters-Noordhoff

Informatiepunt landelijk EPD, 'Landelijk EPD niet verplicht'. http://www.infoepd.nl 15 juni 2011

Begrippenlijst

Functies

Bevoegdhedenbeheerders
De bevoegdhedenbeheerders behandelen de aanvraag van de Functioneel netwerkbeheerders en zetten deze aanvraag door naar de juiste persoon.

Functioneel Beheerder
Functioneel beheer is verantwoordelijk voor de continuïteit en de kwaliteit van de ondersteuning van de bedrijfsprocessen door informatievoorzieningen. Ze doet dat in opdracht van de procesverantwoordelijken in de gebruikersorganisatie, de zogenaamde proceseigenaren.

Functioneel Gegevens Beheerder
Beheert de gegevens, data en informatie van de applicaties op een overzichtelijke manier.

Functioneel Netwerk Beheerder
Een Functioneel Netwerk Beheerder (FNB-er) is een Tekenbevoegde die tevens een aanspreekpunt op een afdeling of sector is voor als klanten iets willen op ICT gebied.

Gebruikers/Klanten
De gebruikers/klanten zijn bijvoorbeeld doktoren of andere medewerkers die gebruik maken van ICT systemen in het ziekenhuis.

Personeel en Organisatie Medewerkers
Personeel en Organisatie Medewerkers (P&O-ers) zijn betrokken bij de verwerking van de gegevens van medewerkers in het personeelsbestand. P&O zorgt bij aanstelling van een medewerker dat de juiste documenten op tijd binnen zijn.

Personeel- en salarisadministratie (PSA)
PSA voert na ontvangst van alle benodigde gegevens van nieuwe medewerkers, deze nieuwe medewerkers in PEOPLESOFT in.

Proceseigenaar
Zij zijn verantwoordelijk, moeten toezien op een toegewezen proces en zorgen dat dit goed verloopt.

Security Officer
De Security Officer is verantwoordelijk voor onder ander de informatiebeveiliging. Andere aspecten in zijn vakgebied zijn niet relevant voor dit onderzoek. Hij wijst ook de risico's aan die zich kunnen voltrekken.

Tekenbevoegde
Een tekenbevoegde is gemachtigd om bevoegdheden aan te vragen voor personeel bij de afdeling ICT maar heeft niet de rest van de verantwoordelijkheden van een Functioneel Netwerk Beheerder.

Systemen

ADS
Active Directory System. Dit is een database met inloggegevens van gebruikers voor bijvoorbeeld de toegang tot Windows.

CLIENTELE
CLIENTELE is het nieuwe callverwerkingsprogramma van de ICT afdeling. Dit is de opvolger van VEGASUITE

IDS
ICT Digitale Service. Digitaal bevoegdheden aanvraag formulier, gebruikt door bevoegdheden beheer en tekenbevoegden.

Intranet UMCG
Intranet UMCG is de plek waar de interne communicatie verloopt. Hier worden ziekenhuisbrede nieuwsaankondigingen neergezet maar ook afdelingen en sectoren hebben vaak een portal waar veel informatie te vinden is.

ISS
ICT Self Service. Digitaal bevoegdheden aanvraag formulier, gebruikt door Tekenbevoegden. Wijst automatisch en direct bevoegdheden en direct toe zonder tussenkomst van personen. Niet alle afdelingen werken al met ISS. Niet ge-

schikt voor het aanvragen van bevoegdheden binnen applicaties of het aanvragen van een ZIS account.

PEOPLESOFT
PEOPLESOFT is het personen en personeelsinformatiesysteem voor het UMCG. In PEOPLESOFT worden van alle medewerkers de benodigde gegevens vastgelegd voor o.a. het correct kunnen betalen van de maandelijkse salarissen, de ziekte melding en de voortgang in het beter wordt geregistreerd ten einde een goede begeleiding van de medewerker door de leidinggevende mogelijk te maken, de keuzes voor verhoogd en extra persoonlijk budget registreren, het kunnen vervaardigen van overzichten zoals de Norm en Standlijst, een actueel ziekte overzicht, het maken van RPF'en (rechtspositieformulieren) etc. PEOPLESOFT is op het gebied van persoon en personeelgegevens de bron voor vele andere informatiesystemen in het UMCG.1

POLIPLUS
POLIPLUS is de aanzet voor het EPD (elektronisch patiëntendossier) van het UMCG. Het is een webapplicatie die oorspronkelijk ontwikkeld is in het AMC en patiëntgegevens snel en eenvoudig bereikbaar maakt. Een webapplicatie wordt opgestart in een zogenaamde webbrowser (bijv. Internet Explorer). Het gedraagt zich min of meer zoals een internetpagina. Iemand die bevoegd is om POLIPLUS te gebruiken, kan het op ieder moment en op iedere geschikte PC opstarten. Tevens kunnen er meerdere gebruikers op hetzelfde moment naar dezelfde gegevens kijken.1

VEGASUITE
VEGASUITE is het callverwerkingsprogramma van de ICT afdeling.

X-CARE
X-CARE is een digitale agenda om patiënten afspraken te maken.

ZIS
ZIS staat voor ziekenhuisinformatiesysteem en dit is de basis van het elektronisch patiënten dossier (POLIPLUS, niet verwarren met het landelijke EPD) van het UMCG. Het ZIS is de bron van een groot deel van de patiëntgegevens. Het ZIS bestaat uit verschillende aan de Zorg gerelateerde onderdelen.

WOA
Werkplek Op Afstand. Bied de mogelijkheid toegang te krijgen tot bepaalde systemen van buiten het UMCG.

Overige

Audit
Visitatie en beoordeling door een panel op grond van vastgestelde criteria. Deze criteria zijn meestal ontleend aan een kwaliteitskader of- model, zoals het accreditatiekader, het EFQM model of het ISO model.

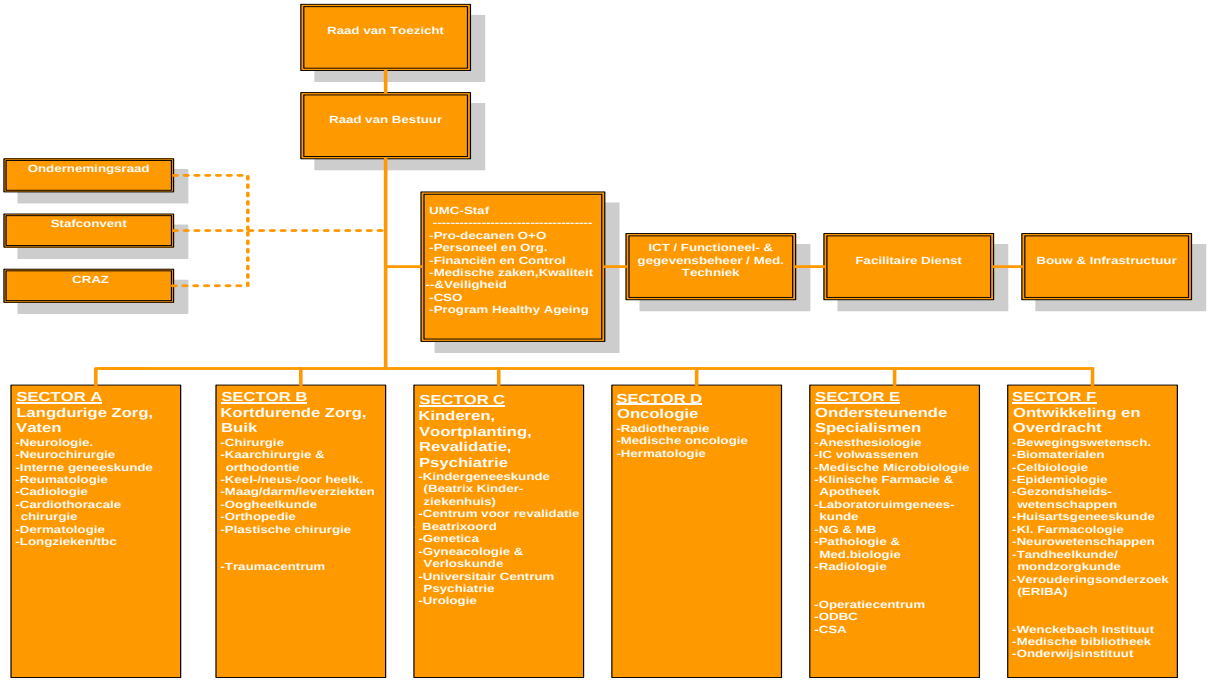
CBP
Het CBP houdt toezicht op de naleving van wetten die het gebruik van persoonsgegevens regelen. Het CBP houdt dus toezicht op de naleving en toepassing van de Wet bescherming persoonsgegevens (Wbp), de Wet politiegegevens (Wpg) en de Wet gemeentelijke basisadministratie (Wet GBA). (www.cbp.nl)

IAM
Identity Acces Management is een lopend ICT project in het UCMG. Het personeelssysteem PEOPLESOFT en het ADS worden hiermee gekoppeld aan elkaar.

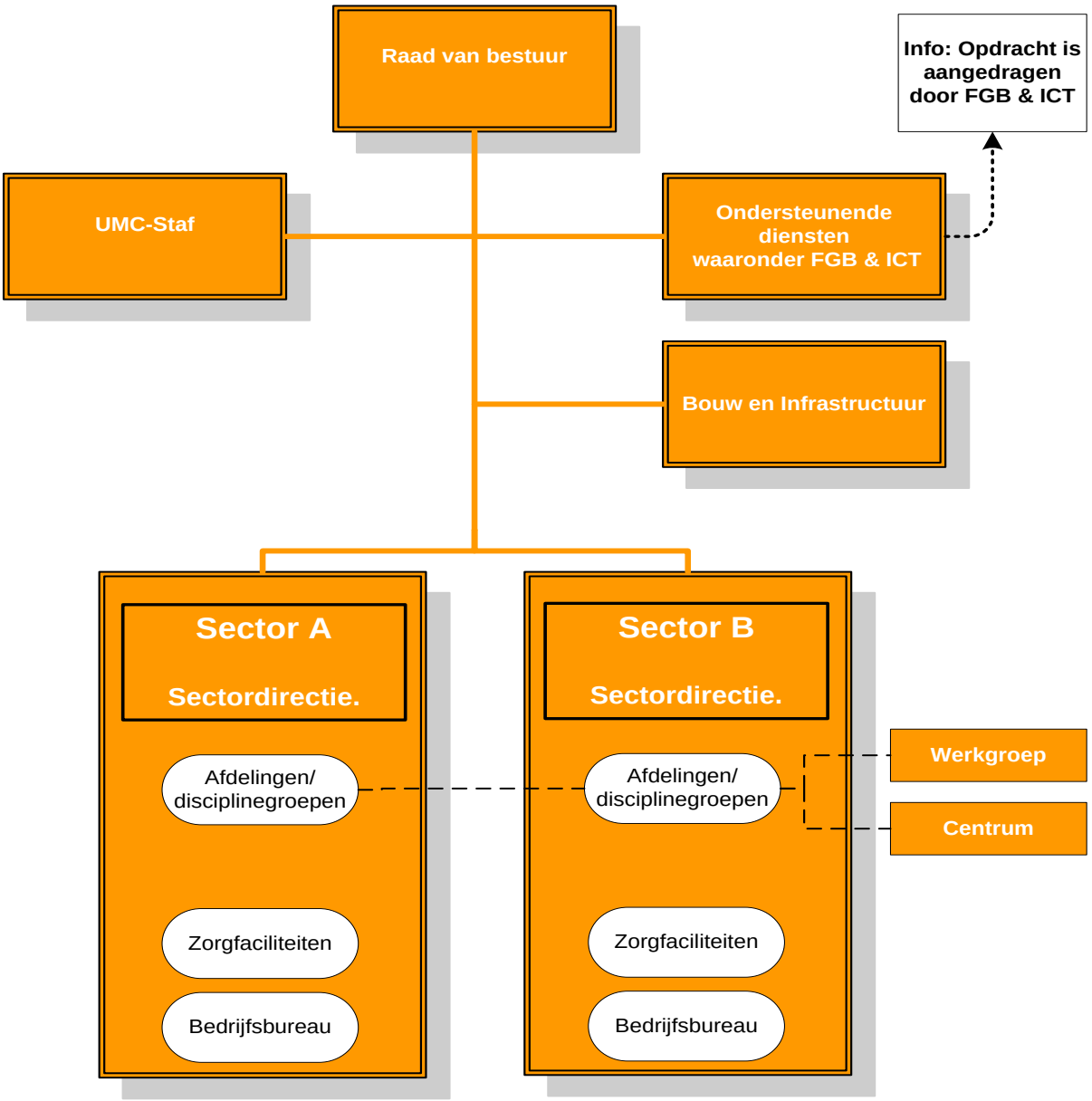
IGZ
De Inspectie voor de Gezondheidszorg (IGZ) bevordert de volksgezondheid door effectieve handhaving van de kwaliteit van zorg, preventie en medische producten. De inspectie adviseert de bewindspersonen en maakt ten opzichte van de zorgaanbieders gebruik van advies, stimulans, drang en dwang als bijdrage aan verantwoorde zorg. De inspectie onderzoekt en oordeelt onpartijdig, deskundig, zorgvuldig en onafhankelijk van politieke kleur of heersend zorgstelsel. (www.igz.nl/organisatie)

Person of interest
Door een lopend ICT project is het nu mogelijk om niet alleen mensen in PEOPLESOFT te zetten die op de loonlijst staan maar ook mensen die niet in dienst zijn van het UMCG. Deze mensen worden dan als Person of Interest in PEOPLESOFT gezet. Dit maakt het mogelijk om bevoegdheden aan te vragen voor werknemers waarvan het aanstellingstraject nog niet is afgerond.

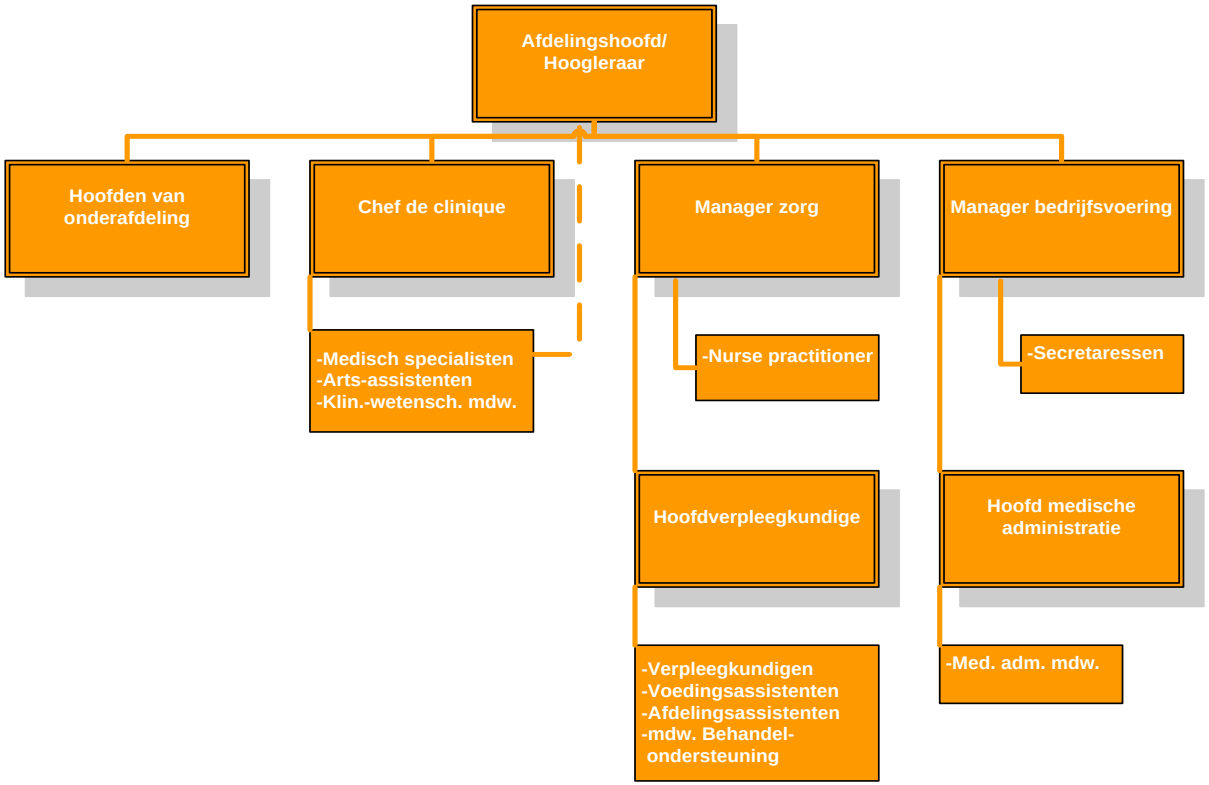
Bijlage 1 Organogrammen



Organigram UMCG



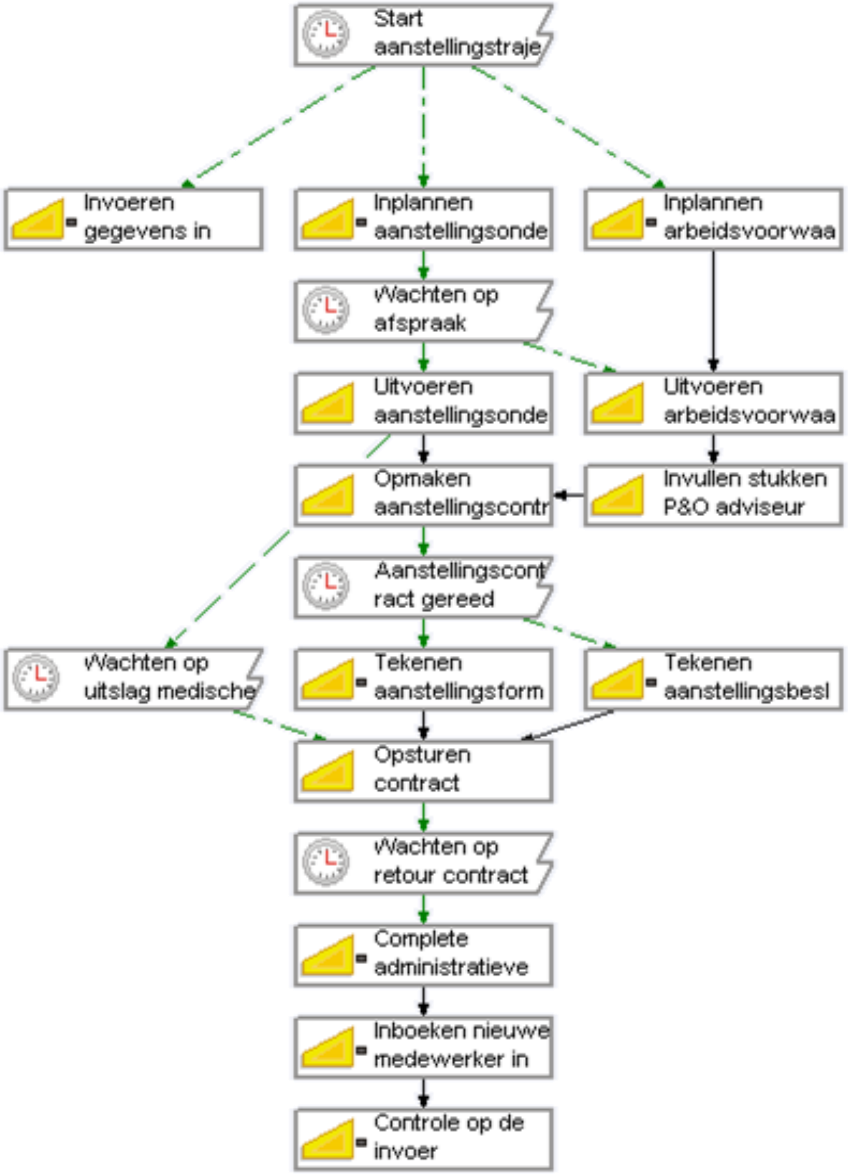
Organigram UMCG sector[1]



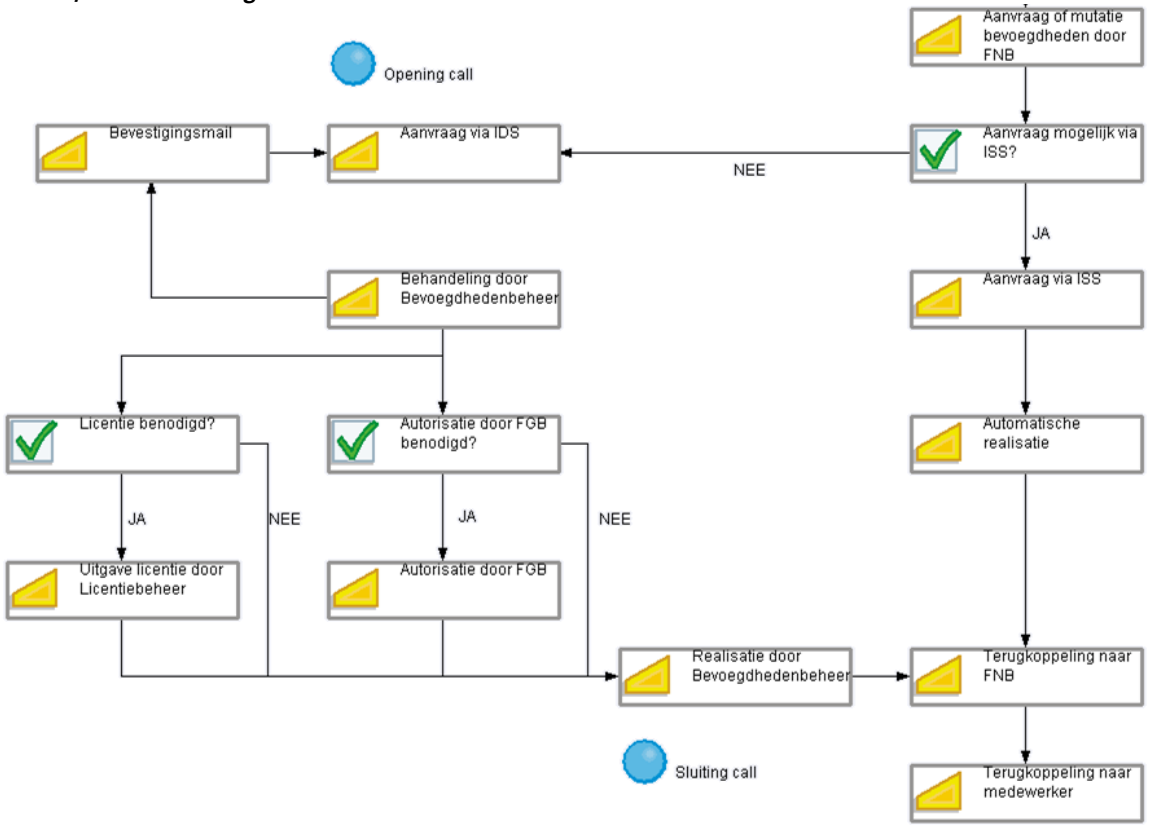
Organigram Sectorspecifiek

Bijlage 2 Processen

Aanstelling medewerker



Toekennen/muteren bevoegdheden



Bijlage 3 McKinsey

Aanbevelingen McKinsey die relevant zijn op het onderzoek.

- Voor bepaalde functies een UMCG breed verbeteringsplan uitwerken.
- Voor bepaalde functies standaard werkwijzen en resultaatratio's gebruiken
- Meer standaardisatie is nodig om de efficiëntie te verhogen.
- Het vergroten van het leiderschap en verantwoordelijkheid gevoel.

Als gevolg van bezuinigingen en om in de toekomst ook betaalbare zorg te kunnen leveren heeft het UMCG als doel gesteld om de doelmatigheid van algemene en medische ondersteuning in de komende jaren te verhogen.

Om de doelmatigheid te verhogen zijn er 3 thema's naar voren gebracht.

- Kundige medewerkers met sterke intrinsieke motivatie en verantwoordelijkheidsgevoel; meer aandacht gewenst voor ontwikkeling en stimuleren van talent.
- Aanpassen van de stijl van leiderschap, gericht op effectievere en transparantere besluitvorming, duidelijke taakstellingen en verantwoordelijkheden, stimulering van medewerkers tot hogere prestaties en samenwerking over de grenzen van organisatieonderdelen heen
- Coördinatie en controle versterken: consequent transparant maken van de voortgang en resultaten van projecten en resultaatverbeteringmaatregelen en waar nodig daarop bijsturen

Bijlage 4 Relevante informatie NEN7510

Relevante informatie uit de NEN7510

Er moet aandacht worden besteed aan het beschermen van de integriteit van elektronisch gepubliceerde informatie, om ongeoorloofde wijzigingen te voorkomen die de reputatie van de instelling zou kunnen schaden.

Toegangsbeveiliging moet ervoor zorgen dat de toegang tot voorzieningen en gegevens wordt veleend aan gebruikers die daartoe gerechtigd zijn en wordt geweigerd aan anderen. Het doel ervan is te waarborgen dat het lezen, toevoegen, wijzigen en verwijderen van gegevens en programmatuur slechts gecontroleerd kan plaatsvinden. Dit is zeker voor de gezondheidszorg een essentiële eis aan de informatievoorziening. Het beland en de wensen van de patiënt moeten hierin worden betrokken. Toegang tot gegeven moet worden beperkt met het oog op integriteit en vertrouwelijkheid

Een instelling moet regels en rechten voor toegang opstellen en onderhouden voor elke gebruiker of groep gebruikers. Op basis hiervan moet toegangsbeveiliging worden geconcretiseerd in beheersmaatregelen en procedures. De eisen waaraan de toegangsbeveiliging moet voldoen, moeten duidelijk worden gemaakt aan gebruikers en beheerders van de middelen voor de informatievoorziening.

Voor toegang tot het geven van medische opdrachten ligt de vereiste zekerheid van de identiteit van de gebruiker zeer hoog.

De toegang tot informatiesystemen en -diensten moet worden beheerst via een geformaliseerde gebruikersregistratie.

Alle geregistreerde gebruikers moeten ene unieke gebruikersidentificatie hebben voor persoonlijk gebruik. De instelling moet procedures voor het toewijzen van gebruikersidentificaties vaststellen.

Gebruikers moeten goede beveiligingsgewoontes in acht nemen bij het kiezen en gebruiken van wachtwoorden en ervoor zorgen dat anderen hun wachtwoord en/of authenticatiemiddel niet kunnen gebruiken.

Gebruikers moeten alleen toegang kunnen krijgen tot diensten, systemen en gegevens waar voor zij zijn geautoriseerd.

De instelling moet procedures en regels vaststellen voor de toekenning en intrekking van bevoegdheden.

Toepassingen, systemen en netwerkvoorzieningen moeten zodanig worden ingericht dat toegang alleen mogelijk is in overeenstemming met geldige bevoegdheden.

Om de toegang tot gegevens en informatiediensten effectief te beheersen, moet de verantwoordelijke op gezette tijden een procedure uitvoeren om de uitgegeven toegangsrechten te controleren.

Zaken waar het beleid aandacht aan moet schenken met betrekking tot het gebruik van netwerkdiensten.

- De netwerken en netwerkdiensten waartoe men toegang heeft
- De autorisatieprocedures om te bepalen wie toegang heeft tot welke netwerken en netwerkdiensten
- Beheersmaatregelen en -procedures om de toegang tot netwerkverbindingen en netwerkdiensten te beveiligen.

Bijlage 5 Oorzaken uitgebreid

Accounts worden uitgeleend
Er is gebleken dat medewerkers hun accounts uitlenen aan collega's wanneer deze nog geen beschikking hebben over een eigen account. Kortom, er zijn twee hoofdoorzaken:

- Een nieuwe medewerker zijn account is niet tijdig beschikbaar.
- De lenende medewerker is zich niet bewust van de mogelijke gevaren van het uitlenen van zijn account.

Niet aanleveren gegevens door medewerker.
Het niet aanleveren van de juiste documenten aan P&O door de nieuwe medewerker zorgt voor het stilliggen van het proces. Als niet alle juiste documenten, contracten en formulieren bij P&O aanwezig zijn, dan voert PSA de nieuwe medewerker niet in, in PEOPLESOFT. Ook al is het proces tijdig gestart maar worden de juiste gegevens niet doorgegeven dan ligt het proces stil.

Niet overkomen van gegevens van een aanvraag bij de Tekenbevoegde
Als de aanvraag voor een account voor een nieuwe medewerker niet overkomt bij de Tekenbevoegde dan ligt het proces daar stil. Er zijn meerdere mogelijkheden waarom de aanvraag niet bij de Tekenbevoegde verwerkt wordt.

Situatie 1	In de praktijk komt het regelmatig voor dat nieuwe medewerkers hun bevoegdheden niet tijdig hebben omdat het bevoegdheidsaanvraag proces niet goed is verlopen.
Oorzaak	– Niet aanleveren van gegevens door nieuwe medewerker waardoor PSA het proces stil laat liggen. – Niet overkomen van gegevens van een aanvraag bij de Tekenbevoegde – Afwezigheid van sleutelfiguur in het proces. – Onjuiste aanvraag door de Tekenbevoegde – FNB weet niet wat exact wat hij aan moet vragen en moet eerst informeren. – Verschillende werkwijzen per sector. ICT moet met verschillende werkwijzen omgaan wat meer tijd kost en niet efficiënt is. – Afhankelijkheid van applicaties en programma's onderling. Geen personeelsnummer? Geen ZIS. – Te laat starten van het proces.
Gevolg	– Het niet tijdig aan het werk kunnen op de eigen account van werknemers resulteert in het gebruik maken van een account van een collega. – Door het gebruik van accounts van collega's wordt er niet voldaan aan de NEN7510 en dus niet aan het beleid. – Door het gebruik van accounts van collega's kan de patiënt veiligheid en privacy niet worden gegarandeerd. – Het imago en de kwaliteit van de zorg leiden onder het niet voldoen aan de NEN7510. Niet voldoen aan de NEN7510 zorgt er voor dat er niet mee gewerkt kan worden aan het landelijk EPD en in ernstige gevallen word het verlenen van bepaalde zorg geweigerd. – Het gebruik maken van accounts van collega's is in strijd met de NEN7510 er is namelijk niet terug te koppelen wie wat op welk moment gedaan heeft hier door. – Het gebruik van accounts van collega's kan er toe leiden dat de lenende werknemer door het gebruik van een account van een ander meer in kan zien dan hij zou mogen. Hier lekt de beveiliging.

1.Medewerker P&O/PSA is ziek/vakantie
In het proces zijn vaak te weinig vervangers voor medewerkers waardoor bij ziekte of afwezigheid de werkzaamheden van deze persoon niet worden opgepakt door een collega. Er wordt niet waargenomen of de waarnemer behandelt niet oude aanvragen.
2.Medewerker P&O/PSA vergeet de gegevens door te geven
Medewerkers van P&O en PSA vergeten hun taken soms uit te voeren. Dit is mogelijk ook een oorzaak van het feit dat er geen controle en consequenties zijn voor het niet volbrengen van je taken binnen het UMCG

3.Tekenbevoegde is ziek/vakantie
Het niet aanwezig zijn van de FNB'er veroorzaakt het stil vallen van het proces. FNB'ers hebben vaak hun eigen werkwijze waardoor waarneming er lastig is. Dit is het gevolg van het feit dat er niet één UMCG brede werkwijze voor FNB is.

4.FNB is de aanvraag vergeten(door vage doorgave van gegevens)
Doordat er niet één universele manier is om een aanvraag in te dienen bij FNB kan het voorkomen dat aanvragen vergeten worden omdat deze niet terug te vinden zijn. De volgende mogelijkheden zijn er.
Aanvragen:
1. Per mail
2. Telefonisch
3. Gedelegeerd via P&O met behulp van een infopath formulier
4. Via secretaresses
5. Via collega's
6. Soms mailen/bellen mensen ook zelf als ze nog geen bevoegdheden hebben

Met name telefonisch en mondelinge aanvragen zijn niet meer na te zien.
Problemen door meerdere manieren van aanvragen:
- Inefficiënt werken
- Storingsgevoelig
- Meer werk dan nodig.

Deze problemen zijn ontstaan door
- Het ontbreken van UMCG breed beleid.

5.P&O/PSA geeft wel een aanvraag door maar er missen gegevens.
Het doorgeven van een aanvraag naar FNB kan doordat er niet één universele manier gehanteerd wordt gemakkelijk foutief plaatsvinden. Dit kan er toe leiden dat er gegevens missen en de FNB'er de aanvraag niet kan voltooien.

Afwezigheid van sleutelfiguur.
Doordat het proces afhankelijk is van vele menselijke schakels is de kans op vertraging groot. Bij de afwezigheid van één van de sleutelfiguren ligt het proces al tijdelijk stil.

Onjuiste aanvraag door FNB
Doordat FNB'ers niet worden ingewerkt is niet altijd duidelijk wat er bij bepaalde aanvragen moet gebeuren. Dit resulteert in verkeerde aanvragen.

Onduidelijkheid bij FNB'er
Doordat FNB'ers niet worden ingewerkt is niet altijd duidelijk wat exact de taken zijn van een FNB'er en wat hoe deze taken uitgevoerd moeten worden. Dit resulteert in het feit dat FNB'ers de ICT helpdesk gaan bellen en dat is niet efficiënt. Deze niet efficiënte vorm van werken kost meer tijd waardoor het proces langer duurt dan nodig.

Verschillende werkwijzen per Sector
Er is geen UMCG brede werkwijze voor FNB. Het resultaat is dat Sectoren allemaal hun eigen werkwijze zijn gaan ontwikkelen. ICT krijgt te maken met verschillende werkwijzen wat lastig kan zijn maar vooral ook frustrerend. Ook hier wordt niet efficiënt gewerkt en verschillende manieren van aanvragen nemen meer tijd in beslag dan nodig.
Problemen:
- Er kan lastig toezicht gehouden worden op werkwijzen binnen het UMCG omdat er verschillende werkwijzen zijn die verschillend gecontroleerd moeten worden.
- Bij ziekte kan niet de FNB'er van de ene Sector het werk van de andere Sector zomaar waarnemen omdat de werkwijzen verschillend zijn.
- Sectoren doen dubbel werk omdat ze onderling niet communiceren.
- Frustrerend voor ICT
- Inefficiënt

Deze problemen zijn ontstaan door
- De opdeling in Sectoren(kleine ziekenhuisjes) heeft er voor gezorgd dat elke Sector zijn eigen werkwijze heeft gecreëerd.
- Er wordt van hoger af niet één werkwijze verplicht.
- FNB'ers worden niet ingewerkt waardoor eigen werkwijzen ontstaan

Afhankelijkheid van applicaties en programma's onderling.
Het proces omtrent bevoegdhedenaanvragen moet stap voor stap worden doorlopen. Zodra bij P&O bekend is dat een nieuwe medewerker voor zijn aanstaande functie ZIS nodig heeft kan niet direct ZIS voor deze medewerker aangemaakt worden. Voor ZIS is namelijk PEOPLESOFT nodig. Wordt om een om andere reden geen PEOPLESOFT aangemaakt dat kan er ook geen ZIS aangemaakt worden. Deze afhankelijkheid zorgt er voor dat het proces te veel tijd in beslag neemt.

Te laat starten van het proces.
Het bevoegdhedenaanvraag proces neemt normaliter 28 werkdagen in beslag. Korter dan 28 werkdagen voor de eerste werkdag van de nieuwe medewerker starten resulteert in het niet tijdig beschikbaar zijn van de bevoegdheden.

Situatie 2	Laag informatiebeveiligings- bewustzijn
Oorzaak	– Geen gevolgen voor medewerkers. – Geen controle op het aan blijven houden van accounts. – Er wordt geen bewustzijn gecreëerd binnen het UMCG. De werkelijke gevolgen van het nonchalant omgaan met bevoegdheden zijn niet bekend.
Gevolg	– Verkeerde personen behouden de verkeerde bevoegdheden. – De verkregen bevoegdheden worden niet enkel voor eigen gebruik behouden.

Geen consequenties.
Het uitlenen van accountgegevens heeft geen consequenties waardoor de voordelen opwegen tegen de nadelen.

Geen controle
Al zouden er consequenties zijn dan is er ook nog eens geen controle op het uitlenen van accountgegevens. Afdelingshoofden voeren geen controles uit om het uitlenen te voorkomen.

Onbekendheid gevolgen nonchalante werkwijze.
Doordat er niet bekend is wat de gevolgen zijn van het uitlenen van accountgegevens zien medewerkers ook de gevaren er niet van in.

Medewerkers met teveel of juist te weinig bevoegdheden.
Er is gebleken dat in de er in praktijk medewerkers zijn met teveel en ook met te weinig bevoegdheden.

Hier onder zijn deze situaties met de oorzaken en de gevolgen hiervan weergegeven
Afdelingsmanagers geven de verkeerde aanvraag door aan FNB
Doordat FNB'ers niet ingewerkt worden en niet altijd weten wat ze aan moeten vragen gebeurd dit ook op vertrouwen van de afdelingsmanagers. Vraagt de afdelingsmanager dan het verkeerde aan, dan zal dit ook zo doorgevoerd worden door de FNB'er

FNB vraagt verkeerde bevoegdheden aan.
Doordat FNB'ers niet worden ingewerkt is niet altijd duidelijk wat er bij bepaalde aanvragen moet gebeuren. Dit resulteert in verkeerde aanvragen.

Kopiëren van bevoegdheden
Bij bepaalde aanvragen wordt er gebruik gemaakt van het zogenoemde 'kopiëren'. Een nieuwe werknemer krijgt dezelfde bevoegdheden als een collega met dezelfde functie. Al kan deze collega ook speciale bevoegdheden hebben die

de nieuwe werknemer niet zou moeten krijgen maar op de manier wel verkrijgt.

Mutaties
Bij mutaties komt het binnen het UMCG regelmatig voor dat de oude afdeling de oude bevoegdheden niet intrekt. Op deze manier kan de medewerker gebruik blijven maken van de oude bevoegdheden. Dit probleem komt deels voort uit het feit dat FNB'ers niet worden ingewerkt en er niet wordt gemeld dat zij de oude bevoegdheden bij een mutatie van een medewerker van hun afdeling in moeten trekken.

Ontslag
Bij het ontslag van medewerker worden niet altijd de oude bevoegdheden ingetrokken doordat het vergeten wordt of als onbelangrijk gezien wordt.

Niet doorgeven van het vertrek van een medewerker.
P&O geeft niet altijd door dat een medewerker met ontslag of ontslagen is. Hierdoor weet FNB niet dat bevoegdheden moeten ingetrokken waardoor ze aanblijven.

Geen overzicht toegewezen bevoegdheden.
Bij het vertrek van een medewerker is door de FNB'er niet in een bestand in te zien wat de ooit toegekende bevoegdheden van de medewerker zijn. De FNB'er weet dan dus ook niet wat hij exact in moet trekken.

Situatie 1	In de praktijk komt het regelmatig voor dat medewerkers toegang hebben tot gegevens en applicaties die ze niet zouden moeten hebben
Oorzaak	– Afdelingsmanager geeft de verkeerde aanvraag aan FNB door. – FNB vraagt verkeerde bevoegdheden aan. – Door kopiëren van bevoegdheden kan het voorkomen dat ook niet standaard bevoegdheden mee worden gekopieerd. – Bij mutaties neemt de oude sector/afdeling de oude bevoegdheden niet af waardoor ze beschikbaar blijven voor de medewerker. – Bij ontslag niet verwijderen van de account. – Bij vertrek van een medewerker niet doorgeven door P&O/leidinggevende aan ICT en FNB dat deze medewerker uit dienst gaat. – Geen goede inzage door FNB in de bevoegdheden waardoor niet gezien wordt wat precies afgenomen moet worden bij een mutatie.
Gevolg	– Verkeerde mensen kunnen bij de verkeerde informatie. De kans op problemen en fouten neemt toe. – De patiëntveiligheid en privacy kunnen niet worden gewaarborgd. – Niet voldoen aan de NEN7510 – Niet voldoen aan het beleid.

Situatie 2	In de praktijk komt het regelmatig voor dat medewerkers niet de toegang hebben tot gegevens en applicaties die ze niet zouden moeten hebben
Oorzaak	– Afdelingsmanager geeft de verkeerde aanvraag aan FNB door. – FNB vraagt verkeerde bevoegdheden aan. – Door kopiëren van bevoegdheden worden specifieke bevoegdheden niet toegewezen.
Gevolg	– Medewerkers kunnen hun taken niet voldoende uitvoeren. – De kans op het zoeken naar mogelijkheden om toch hun werk uit te kunnen voeren neemt toe. (lenen van accounts)

Afdelingsmanagers geven de verkeerde aanvraag door aan FNB
Doordat FNB'ers niet ingewerkt worden en niet altijd weten wat ze aan moeten vragen gebeurd dit ook op vertrouwen van de afdelingsmanagers. Vraagt de afdelingsmanager dan het verkeerde aan, dan zal dit ook zo doorgevoerd worden door de FNB'er

FNB vraagt verkeerde bevoegdheden aan
Doordat FNB'ers niet worden ingewerkt is niet altijd duidelijk wat er bij bepaalde aanvragen moet gebeuren. Dit resulteert in verkeerde aanvragen.

Kopiëren van bevoegdheden
Bij bepaalde aanvragen wordt er gebruik gemaakt van het zogenoemde 'kopiëren'. Een nieuwe werknemer krijgt dezelfde bevoegdheden als een collega met dezelfde functie. Het kan zijn dat de nieuwe medewerker dezelfde functie heeft als zijn collega waar van gekopieerd wordt maar ook speciale bevoegdheden nodig heeft die op deze manier niet worden toegewezen

Oude accounts blijven actief
Er is gebleken dat in de er in praktijk na ontslag oude accounts actief blijven. Oud medewerkers kunnen nog steeds bij informatie terwijl dit niet zou moeten.
Hier onder is deze situatie met de oorzaken hiervan en de gevolgen weergegeven.

Niet doorgeven door P&O dat een medewerker met ontslag of ontslagen is.
P&O geeft niet altijd door dat een medewerker met ontslag of ontslagen is. Hierdoor weet FNB niet dat bevoegdheden moeten ingetrokken waardoor ze aanblijven.

Bevoegdheden worden niet ingetrokken door laksheid.
Het feit dat er geen controle en consequenties zijn voor het niet volbrengen van je taken worden bepaalde taken laks uitgevoerd.

Gevolgen zijn onbekend.
Het is bij medewerkers niet bekend wat de gevolgen zijn van het niet intrekken van bevoegdheden. Hierdoor zien de medewerkers hier de gevaren ook niet van in.

Situatie	Bij uitdiensttreding verdwijnen niet altijd de toegangsrechten.
Oorzaak	– Er wordt niet altijd door P&O/leidinggevende doorgegeven dat een medewerker met ontslag of ontslagen is. – Bevoegdheden worden gewoon niet ingetrokken.(laksheid) – Bewustzijn van de gevaren is onvoldoende waardoor niet altijd gezien wordt dat bevoegdheden afgenomen moeten worden.
Gevolg	– Verkeerde mensen kunnen bij de verkeerde informatie. – Niet voldoen aan de NEN7510 – Niet voldoen aan beleid

Bijlage 6 Gespreksverslagen

Oriënterende interviews

Om inzicht te krijgen in de situatie binnen het UMCG betreffende het bevoegdheden aanvraag proces, zijn oriënterende interviews gehouden. Deze gesprekken hebben inzicht gegeven in probleem situaties, de taken van een FNB'er, inzicht in beleid en vele andere cruciale onderwerpen voor het succesvol volbrengen van dit onderzoek. Hiernaast zijn er om gedetailleerde informatie over specifieke onderwerpen te verkrijgen diepte interviews gehouden.

Bepaalde geïnterviewden prefereerden het om anoniem te blijven terwijl anderen naamsvermelding geen probleem vonden. Alle gebruikte gespreksinformatie is ondertekend door de verstrekker en inzage in deze ondertekende documenten is mogelijk bij het UMCG. Ook zijn er ondervraagden die na meerdere verzoeken niet gereageerd hebben, hier zijn geen handtekeningen van beschikbaar. Uit deze gesprekken worden enkel bevonden problemen gebruikt omdat de informatie niet gecheckt is en fouten kan bevatten. Uit veiligheid worden deze persoon anoniem vermeld.

Er zijn gespreksverslagen die het gehele gesprek verwoorden, maar ook zijn er gespreksverslagen die na wens van de vertrekker enkel die zaken die relevant voor ons onderzoeksonderwerp zijn bevatten.

Overzicht ondertekende gespreksverslagen

Gesprek nummer	Persoon	Functie/rol/afdeling
1	Ymte de jager	Coördinator ICT Beheer Bevoegdheden
2	Frans Erich	Stafmedewerker ICT Sector C
3	Frans Erich, Teun Modderman, Peter Wagenaar	Stafmedewerker ICT en FNB'ers Sector C
4	Anoniem	FNB
5	Anoniem	FNB
6	Frank de Vries	FNB Sector A
7	Stanley Wikkeling	FNB Sector D
8	Sandra Brugge	FGB en FNB
9	Piet van der Veen	FGB en FNB
10	Anoniem	FGB
11	Henri Vegter	FGB ZIS
12	Mense Bakker	Bevoegdheden beheer
13	Anoniem	Lean Six Sigma Blackbelt
14	Corrina Argus	Stafadviseur (rollen o.a. Opdrachtgever, Projectmanager/leider, Ketenvoorzitter).

Overzicht niet ondertekende gespreksverslagen

Gesprek nummer	Persoon	Functie/rol/afdeling
15	Anoniem	FNB Sector F
16	Anoniem	Functioneel netwerk beheerder Sector B en ICT medewerker
17	Rob Lohr	Bevoegdheden beheer.

Bijlage 7 Status EPD

Eerste Kamer stemt tegen landelijk elektronisch patiëntendossier
5 april 2011
De Eerste Kamer heeft dinsdag tegen de wet gestemd die de verplichte aansluiting op het landelijk elektronisch patiëntendossier (EPD) regelt. Daarnaast heeft de Eerste Kamer minister Schippers van Volksgezondheid, Welzijn en Sport gevraagd om niet meer mee te werken aan de ontwikkeling van het landelijk EPD. De minister brengt op dit moment in kaart wat de gevolgen zijn voor het landelijk EPD.
De Tweede Kamer stemde begin 2009 in met de wet, maar door de beslissing van de Eerste Kamer is de wet nu van de baan. De minister onderzoekt of via versterking van andere wetten de privacy en bescherming van patiënten kan worden verbeterd.

Bijlage 8 ZIS aanvragen

wrk_ingdat	usr_ingdat	usr_mutdat	werknemer eigennaam	Call_open	Call_close	Personeelsnummer	Duur aanvraag	Verschil indienst en aanvraag	Verschil call close en usr_ingdat	Verschil PS ZIS ing	Verschil PS ZIS mut	Verschil Close call en mutdat
1-2-2011	2-2-2011	2-2-2011	XXXX	23-3-2010	23-3-2010	0	0	-308	309	1	1	309
1-12-2010	8-2-2010	19-12-2010	XXXX	3-2-2010	8-2-2010	0	5	-298	0	-293	18	311
1-12-2010	16-2-2010	19-12-2010	XXXX	15-2-2010	16-2-2010	0	1	-286	0	-285	18	303
1-1-2011	31-3-2010	17-1-2011	XXXX	30-3-2010	31-3-2010	0	0	-271	0	-270	16	287
1-1-2011	25-1-2011	25-1-2011	XXXX	19-4-2010	21-4-2010	0	2	-252	274	24	24	274
1-1-2011	12-5-2010	17-1-2011	XXXX	11-5-2010	12-5-2010	0	1	-230	0	-229	16	245
1-9-2010	9-2-2010	22-9-2010	XXXX	9-2-2010	9-2-2010	0	0	-202	0	-202	21	223
1-9-2010	16-2-2010	17-1-2011	XXXX	16-2-2010	16-2-2010	0	0	-195	0	-195	136	331
1-12-2010	30-11-2010	19-12-2010	XXXX	28-5-2010	31-5-2010	0	3	-183	180	-1	18	199
6-9-2010	16-11-2010	16-11-2010	XXXX	10-3-2010	10-3-2010	0	0	-176	246	70	70	246
1-1-2011	8-7-2010	17-1-2011	XXXX	6-7-2010	8-7-2010	0	2	-175	0	-173	16	189
1-1-2011	18-11-2010	17-1-2011	XXXX	6-7-2010	8-7-2010	0	2	-175	130	-43	16	189
1-9-2010	15-3-2010	21-11-2010	XXXX	11-3-2010	15-3-2010	0	4	-170	0	-166	80	246
18-10-2010	4-5-2010	7-11-2010	XXXX	4-5-2010	4-5-2010	0	0	-164	0	-164	19	183
1-11-2010	19-5-2010	7-11-2010	XXXX	18-5-2010	19-5-2010	0	1	-163	0	-162	6	168
1-7-2010	4-3-2008	15-7-2010	XXXX	25-1-2010	26-1-2010	0	1	-156	-682	-837	14	169
1-7-2010	15-10-2009	15-7-2010	XXXX	25-1-2010	26-1-2010	0	1	-156	-101	-256	14	169
1-7-2010	26-1-2010	15-7-2010	XXXX	25-1-2010	26-1-2010	0	1	-156	0	-155	14	169
1-12-2010	13-7-2010	19-12-2010	XXXX	12-7-2010	13-7-2010	0	1	-139	0	-138	18	156
1-10-2010	17-5-2010	17-10-2010	XXXX	14-5-2010	17-5-2010	0	3	-137	0	-134	16	150

Bijlage 9 ADS aanvragen

	werknemer eigennaam	Call_open	Call_close	Verschil open en close call
		30-dec-2010	30-dec-2010 13:55:24	0
		30-dec-2010	30-dec-2010 14:08:17	0
		28-dec-2010	28-dec-2010 10:10:47	0
		27-dec-2010	28-dec-2010 9:40:14	1
		27-dec-2010	28-dec-2010 9:35:00	1
		27-dec-2010	29-dec-2010 9:25:53	2
		24-dec-2010	27-dec-2010 10:07:34	3
		23-dec-2010	27-dec-2010 11:11:22	4
		22-dec-2010	27-dec-2010 10:12:25	5
		22-dec-2010	22-dec-2010 12:44:37	0
		21-dec-2010	22-dec-2010 9:48:46	1
		21-dec-2010	22-dec-2010 9:14:00	1
		21-dec-2010	22-dec-2010 9:08:36	1
		21-dec-2010	22-dec-2010 9:05:27	1
		21-dec-2010	22-dec-2010 9:02:59	1
		21-dec-2010	22-dec-2010 9:00:00	1
		21-dec-2010	21-dec-2010 12:09:52	0
		21-dec-2010	22-dec-2010 8:57:34	1
		21-dec-2010	22-dec-2010 8:50:16	1
		21-dec-2010	22-dec-2010 8:47:44	1