

Een kwestie van taak

Door de toepassing van ict kan informatie steeds gemakkelijker door steeds meer medewerkers worden ingezien. Goed autorisatiebeheer is daarom belangrijk. Aandacht voor de taakverdeling tussen de vele partijen binnen de zorginstelling levert daarbij de meeste winst op.



Auteurs: Berend de Vries en Jaap van der Wel
Illustratie: Tjeerd Royaards

Toen in oktober vorig jaar George Clooney na een motorongeluk in een Amerikaans ziekenhuis belandde, bleken 27 medewerkers die niets met de behandeling te maken hadden, in zijn medisch dossier te hebben gekeken. Iets dergelijks was in Nederland al eerder gebeurd. “Agenten azen op dossier Van Persie”, kopte RTL-nieuws op 12 oktober 2005. Hier betrof het geen zorgdossier maar het procesverbaal met betrekking tot een vermeende verkrachttingszaak, toch ook wel privacygevoelig. Deze nieuwsberichten roepen de vraag op hoe vaak persoonlijke dossiers worden ingezien, zonder dat het ontdekt wordt.

Door de toepassing van ict kan informatie steeds gemakkelijker door steeds meer medewerkers worden ingezien. Belangrijk, want dat spaart werk en voorkomt fouten. De keerzijde is echter dat meer aandacht nodig is voor toegangsbeveiliging om te zorgen dat personeel correct om blijft gaan met patiëntgegevens. Leverde vroeger de geheimhoudingsplicht van de zorgverlener afdoende garanties, door de toenemende toegankelijkheid van informatie wordt het steeds belangrijker om goed in beeld te hebben wie met welke gegevens mag omgaan en waarom.

Iedereen in de zorg ziet het belang van autorisatiebeheer. Toch komt fatsoenlijk autorisatiebeheer in de praktijk maar moeizaam van de grond. Dit heeft te maken met een combinatie van factoren. Allereerst is er de lastig te beheren ict-techniek. Daarnaast is er vaak sprake van een suboptimale samenwerking tussen de ict-afdeling en zorgafdelingen. En dan is er nog de vage privacyregelgeving die nog maar aan het begin staat van aanpassing aan het geautomatiseerde tijdperk.

Het beheer van de ict-techniek is lastig omdat zorginstellingen een groot aantal informatiesystemen hebben. Een ziekenhuis heeft gewoonlijk tussen de 50 en de 200 informatiesystemen waarin medische informatie is opgeslagen. In omvang variëren deze van het centrale ziekenhuissysteem dat op iedere afdeling wordt gebruikt tot kleine systemen specifiek voor een specifieke afdeling. Voor de grotere systemen zijn de procedures voor de toegangscontrole gewoonlijk wel in orde maar verreweg de meeste van de

Te vaak worden rechten niet ingetrokken

kleinere systemen kennen nauwelijks formele procedures. Daarmee onttrekt de autorisatie van het leeuwendeel van de privacygevoelige medische informatie zich aan de formele bevoegdheden van de medisch directeur.

Het autorisatiebeheer is bovendien arbeidsintensief doordat de meeste applicaties eigen lijsten van gebruikers en rechten hebben en een aparte inlogprocedure. Dit is lastig voor de behandelaar die meerdere gebruikersnamen en passwords moet onthouden. Het is helemaal lastig als de behandelaar op meerdere plekken werkt en het inloggen in de systemen één of meer minuten bedraagt. Men moet dan ook niet verbaasd zijn dat iemand op een afdeling ‘s ochtends inlogt waarna andere medewerkers van die afdeling de rest van de dag gebruik maken van die ingelogde terminal.

Foutgevoelig

Wanneer een medewerker verandert van afdeling moeten meerdere systemen worden aangepast, hetgeen foutgevoelig is en geregeld wordt vergeten. Medewerkers die daarvoor geen toegang hebben maar wel gegevens nodig hebben, zorgen er wel voor dat de rechten goed gezet worden. Te vaak echter worden rechten niet ingetrokken waardoor een medewerker onterecht toegang blijft houden tot te veel informatie. Het komt zelfs voor dat bij het verlaten van de dienst de rechten niet meteen ingetrokken worden. Tal van zorgprofessionals zien de problemen van autorisatiebeheer wel maar kunnen daaraan niet veel doen omdat zij in de praktijk niet betrokken zijn bij het beheer. De ict-afdeling, die de rechten meestal instelt, ziet gewoonlijk wel dat het rechtenbeheer verbetering behoeft. Zij probeert daar iets aan te doen door bijvoorbeeld in te gaten te houden welke medewerkers van afdeling veranderen om dan

taakverdeling



spontaan rechten in te trekken. Ict-medewerkers trekken daarmee verantwoordelijkheden naar zich toe die bij de afdelingshoofden behoren te blijven, de wereld op zijn kop.

Tenslotte dwingt de regelgeving weinig af. De Wet bescherming persoonsgegevens en de Wet geneeskundige behandelovereenkomst maken op zich wel duidelijk dat vertrouwelijke informatie niet ter beschikking mag komen aan personen die de informatie niet nodig hebben, maar de verdere uitwerking in de praktijk is onduidelijk.

Informatiesystemen hoeven niet aan standaarden te voldoen en hebben ieder een eigen autorisatiebeheer waardoor het voor een zorginstelling lastig is om instellingsbreed toegangsbeheer goed vorm te geven.

Personeelspas

Het verduidelijken van de weinig specifieke regelgeving is een maatschappelijk issue, geen taak voor directies van zorginstellingen.

gen. Voor hen staan twee andere wegen open: het verbeteren van de ict en vooral het verbeteren van de organisatie.

Er zijn in de ict tal van betaalbare en bruikbare mogelijkheden om de identiteit van gebruikers vast te stellen. De vele verschillende gebruikersnamen en wachtwoorden kunnen tegenwoordig worden samengevoegd in een personeelspas samen met bijvoorbeeld functies voor de toegang tot het parkeerterrein en het betalen in de kantine. De alternatieven voor pasjes hebben in de praktijk nog veel nadelen.

Vingerafdrukherkenning kent nog veel te veel onterechte afwijzingen of is lastig bij het dragen van handschoenen en irisscan is te duur en te omslachtig in de dagelijkse praktijk van de zorg.

In een enkele zorginstelling wordt al geëxperimenteerd met een centraal systeem voor autorisatiebeheer en 'single-signon'. Een dergelijk systeem voert inlogprocedures automatisch uit op de gevraagde applicatie.

Hoe interessant de technische mogelijkheden ook zijn, naar onze mening levert aandacht voor de taakverdeling tussen de vele partijen binnen de zorginstelling de meeste winst op. Afdelingshoofden moeten hun verantwoordelijkheid gaan nemen en moeten daarvoor het inzicht in en het overzicht over de uitgegeven rechten hebben. De ict-afdeling zal zich moeten beperken tot uitvoering van het rechtenbeheer. De afdeling personeelszaken is de juiste afdeling om identiteiten, ook digitale identiteiten, te beheren. Dit is immers de afdeling waar de identiteit van de nieuwe medewerker wordt getoetst en waar men als eerste op de hoogte is van wijziging van dienstverband of uitdiensttreding. Ook beheert deze afdeling de functiebeschrijvingen waarop de rechten voor toegang tot het informatiesysteem worden gebaseerd.

Tenslotte is deze afdeling op de hoogte van het komen en gaan van tijdelijk personeel.

De organisatie van het rechtenbeheer krijgt gestalte in een vaste commissie die bestaat uit materiedeskundigen, applicatiebeheerders en

it'ers. Binnen deze groep worden gegevens naar gevoeligheid geclassificeerd, taken in functies gegroepeerd en deze twee indelingen gecombineerd in een autorisatieschema.

Opdrachtgever van dit geheel is de medisch directeur. Handhaven van een standaard voor functies en toegangsrechten beperkt het onderhoudswerk en daarmee het risico van fouten in de praktijk. De invoering van een dergelijke aanpak start met de belangrijkste applicaties waarna ook andere toepassingen in de schema's opgenomen worden.

Tot slot is geregelde evaluatie nodig. 'Met en

Personeelszaken is de juiste afdeling om identiteiten te beheren

is weten' want daarmee komen tekortkomingen aan het licht. Een uitstekend instrument hiervoor is de norm voor informatiebeveiliging in de zorg, NEN 7510. In de norm wordt gesteld dat een gegevensclassificatie en een autorisatietabel aantoonbaar aanwezig moeten zijn. Daarnaast wordt gesteld dat iedere medewerker eenduidig identificeerbaar moet zijn. En er wordt gesteld dat het onwenselijk is dat procedures omzeilt kunnen worden. In de praktijk valt het niet mee aan deze strenge norm te voldoen. Toch is het zeker niet juist de norm alleen als checklist te hanteren. Om de norm werkelijk te implementeren zijn veranderingen in organisatie en cultuur een voorwaarde en hierin kunnen slechts kleine stapjes worden gemaakt. <

Berend de Vries en Jaap van der Wel maken beiden deel uit van Comfort-IA (www.comfort-ia.nl) dat zich toelegt op informatiebeveiliging in de zorg. Van der Wel is auteur van het boek *Informatiebeveiliging in de zorg*.