Uw dossiers, het ziekenhuis en het EPD:

Vertrouwelijkheid en betrouwbaarheid van patiëntgegevens in het ziekenhuis, in het kader van de invoering van het nationale EPD.

Document: masterscriptie
Versienummer: 1.1 (final)
Datum: 29 juli 2009

ing. Kevin M. J. Kluijtmans
Studentnummer: s0717703
Afstudeernummer: 95 IK

Radboud Universiteit Nijmegen
Faculteit Natuurkunde, Wiskunde en Informatica
Opleiding: master Information Science
Begeleiding: prof. dr. ir. Th.p. van der Weide
dr. W.G. Teepe

Externe organisatie:
PricewaterhouseCoopers
Begeleiding: ir. C. Wullems-Beister RE

Voorwoord

Met deze masterscriptie sluit ik mijn studie Information Science aan de Radboud Universiteit Nijmegen af. Deze scriptie is geschreven na aanleiding van het nationale Elektronisch Patiënten Dossier (EPD), een 'hot-topic'. Het nationale EPD is een complex en uitdagend project in wording, met vele interessante onderdelen welke vanuit vele gezichtspunten belicht kunnen worden. Deze scriptie richt zich op de vertrouwelijkheids- en betrouwbaarheidsaspecten van de registratie, het gebruik en uitwisseling van patiëntgegevens. Met name het aspect vertrouwelijkheid kan in de communicatie rondom het nationale EPD en in de media rondom het project op veel aandacht rekenen. Dit is niet onterecht, tekortkomingen ten aanzien van vertrouwelijkheid maar zeker ook betrouwbaarheid van patiëntgegevens kan negatieve gevolgen hebben voor verschillende partijen. We kaderen ons onderzoek verder in door ons te richten op de registratie, gebruik en uitwisseling van patiëntgegevens in het ziekenhuis. Wij richten ons in dit onderzoek niet op de communicatie tussen het ziekenhuis en derden. Overigens vormt het nationale EPD, gericht op nationale uitwisseling van patiënt-/cliëntgegevens tussen zorgaanbieders, wel de achtergrond tegen welke we dit onderzoek uitvoeren. De via het nationale EPD uitgewisselde patiëntgegevens komen immers in het ziekenhuis terecht na uitwisseling.

Deze scriptie is het beste te lezen voor personen met een IT-achtergrond. Dit onderzoek is met name interessant voor personen welke zich professioneel bezighouden met de informatisering van die processen in het ziekenhuis welke gebruik maken van patiëntgegevens.

Dit onderzoek beantwoord doormiddel van een zorgvuldige analyse de vraag welke risico's spelen bij de registratie, gebruik en uitwisseling van patiëntgegevens in het ziekenhuis en maatregelen om deze risico's te beheersen. Deze analyse start in *hoofdstuk 2* met een beschrijving van het domein, het ziekenhuis, voor zover relevant voor ons probleemgebied. *Hoofdstuk 3* brengt die bepalingen uit relevante wet- en regelgeving en een norm in kaart welke een impact hebben op de registratie, gebruik en uitwisseling van patiëntgegevens in het ziekenhuis. Op basis van deze twee hoofdstukken brengen we in *hoofdstuk 4* de belangrijkste risico's in kaart welke verbonden zijn aan de registratie, gebruik en uitwisseling van patiëntgegevens in het ziekenhuis. In *hoofdstuk 5* leggen we een basis voor de maatregelen om deze risico's te beheersen. Doelstelling is het ziekenhuis inzicht te geven in waar het voor hen 'mis' kan gaan waar het gaat om vertrouwelijkheid en betrouwbaarheid van patiëntgegevens binnen de organisatorische grenzen en aanknopingenpunten te geven hoe men deze risico's kan beheersen.

Ik ben in de eerste plaats veel dank verschuldigd aan mijn begeleiders van PricewaterhouseCoopers en de Radboud Universiteit Nijmegen. Chantalle Wullems-Beister (PricewaterhouseCoopers) en Theo van der Weide (Radboud Universiteit Nijmegen) vanwege hun uitstekende inhoudelijke adviezen en begeleiding van het proces. Wouter Teepe wil ik bedanken voor zijn hulp bij de afronding van de scriptie. Ook wil ik alle collega's bij PricewaterhouseCoopers bedanken voor hun goede adviezen en hulp. Ten slotte wil ik mijn vriendin en familie bedanken voor hun steun bij dit intensieve maar bijzonder leerzame proces.

Uden
27 juli 2009
Kevin Kluijtmans

Verkorte inhoudsopgave

Inhoudsopgave

Samenvatting

Centraal in dit onderzoek staat de vraag:
"Wat zijn de risico's ten aanzien van en welke beheersmaatregelen moet het ziekenhuis nemen voor vertrouwelijkheid en betrouwbaarheid van patiëntgegevens bij de digitale registratie, gebruik en uitwisseling van deze gegevens binnen het ziekenhuis?"

Het nationale Elektronisch Patiënten Dossier (nationale EPD) wordt op korte termijn ingevoerd. Het is een complex project, met vele interessante facetten. In dit onderzoek richten wij ons op de vertrouwelijkheid en betrouwbaarheid bij registratie, gebruik en uitwisseling van patiëntgegevens in het ziekenhuis, tegen de achtergrond van het nationale EPD.

Vertrouwelijkheid en betrouwbaarheid van patiëntgegevens is uiterst belangrijk. Is de vertrouwelijkheid (in de ogen van de patiënt) onvoldoende gewaarborgd dan zal hij of zij minder open zijn richting de medewerkers in het ziekenhuis, wat directe gevolgen voor de kwaliteit van de geboden zorg. Waarborgt het ziekenhuis of haar medewerkers de vertrouwelijkheid niet dan schendt de medewerker mogelijk de (afgeleide) geheimhoudingsplicht die hem of haar vanuit de wet is opgelegd. Wordt de betrouwbaarheid (bestaande uit de waarden tijdigheid, juistheid, volledigheid) van patiëntgegevens onvoldoende geborgd dan kan dit ernstige gevolgen hebben voor de te leveren zorg, bijvoorbeeld als belangrijke patiëntgegevens niet tijdig op de juiste plek beschikbaar zijn. Medische fouten, imagoschade en negatieve financiële gevolgen kunnen bijvoorbeeld resulteren uit tekortkomingen ten aanzien van de betrouwbaarheid van patiëntgegevens in het ziekenhuis.

Het ziekenhuis is een veeleisend domein, onder meer omdat men samenwerkt met regelmatig van samenstelling wisselende, gespecialiseerde teams in een informatie-intensieve omgeving. Ook de patiënt en maatschappij zijn veeleisend. Het operationele zorgproces bestaat uit een significant aantal activiteiten waarbij verschillende typen patiëntgegevens worden gebruikt. De competenties en autorisaties ten aanzien van dit proces en de daarbij betrokken registraties (in het bijzonder de registratie van de patiënt en medische dossiers) zijn duidelijk verdeeld over het grote aantal actoren welke erbij betrokken zijn. Ook zijn er verschillende ondersteunende activiteiten waarbij patiëntgegevens (kunnen) worden gebruikt. We hebben dit domein kunnen beschrijven in een aantal modellen.

Om de risico's te bepalen ten aanzien van de vertrouwelijkheid en betrouwbaarheid van patiëntgegevens is enkel een 'ziekenhuismodel' echter onvoldoende. Wet- en regelgeving en normen hebben invloed op de registratie, gebruik en uitwisseling van patiëntgegevens in het ziekenhuis. Met name de Wet bescherming persoonsgegevens (Wbp) en Wet op de geneeskundige behandelovereenkomst (Wgbo) en de norm NEN 7510 heeft een brede en sterke invloed op de registratie, gebruik en uitwisseling van patiëntgegevens in het ziekenhuis. Deze bepalingen stellen enkele specifieke en minder specifieke vereisten aan het probleemgebied.

Op basis van het 'ziekenhuismodel' en de vereisten vanuit Wbp, Wgbo en NEN 7510 kijken we naar de risico's van de digitale registratie, opslag en uitwisseling van patiëntgegevens in het ziekenhuis. De risico's hebben we in het onderzoek geabstraheerd tot een aantal risicogroepen, te weten:

1. 'Benodigde patiëntgegevens zijn niet of onvolledig geregistreerd in deelsysteem'.

   Patiëntgegevens welke een zeker doel dienen binnen activiteiten van het ziekenhuis ontbreken, bijvoorbeeld omdat ze verwijderd zijn binnen de wettelijke bewaartermijn of formulieren onvolledig zijn en de gebruiker niet vragen om alle noodzakelijke informatie. Onvolledige patiëntgegevens kunnen resulteren in fouten en het ziekenhuis / de zorgprofessional kan daardoor in gebreken zijn waar het gaat om verplichten opgelegd door de Wbp. Ook NEN 7510 vereist beheersmaatregelen t.b.v. een volledige invoer van patiëntgegevens (waar het gaat om het invoeren van gevraagde informatie).

2. 'Patiëntgegevens zijn niet (tijdig) beschikbaar voor niet-registrerende gebruikers'.

Patiëntgegevens welke beschikbaar zouden moeten zijn, bijvoorbeeld omdat een gebruiker ze vereist voor de uitvoer van een activiteit, zijn niet beschikbaar. Dit kan bijvoorbeeld gebeuren wanneer patiëntgegevens niet tijdig worden geregistreerd door de professional in de zorg. Dit kan tot gevolgen hebben dat er fouten worden gemaakt bij de behandeling van de patiënt, bijvoorbeeld omdat relevante informatie ontbrak bij de uitvoer van medische handelingen.

3. 'Gebruikers kunnen ongewenste acties uitvoeren op patiëntgegevens'.

   Gebruikers kunnen acties uitvoeren op patiëntgegevens waartoe zij op basis van identiteit/functie/rol in de behandeling van de betreffende patiënt niet toe geautoriseerd zijn. Ook kan het zo zijn dat patiëntgegevens worden gebruikt voor doelen waar zij eigenlijk niet voor gebruikt dienen te worden. Dit kan gevolgen hebben voor de juistheid en volledigheid van de patiëntgegevens. Ook kan het zijn dat het ziekenhuis / de zorgprofessional de door de Wgbo en Wbp opgelegde geheimhoudingsplicht schendt. Ook NEN 7510 stelt bepaalde vereisten aan toegangscontrole.

4. 'Irrelevante patiëntgegevens zijn vastgelegd in deelsysteem'.

   Patiëntgegevens welke geen valide doel dienen binnen de activiteiten van het ziekenhuis worden wel vastgelegd door gebruikers. Het ziekenhuis / de zorgprofessional kan hierdoor in gebreken zijn waar het gaat om verplichten opgelegd door de Wbp.

5. 'Acties van gebruikers op patiëntgegevens zijn niet controleerbaar'.

   Dit maakt het voor controlerende partijen lastig toe te zien op een correcte omgang met patiëntgegevens. Dit kan op haar beurt gevolgen hebben voor zowel vertrouwelijkheid als betrouwbaarheid.

6. 'Patiëntgegevens zijn gekoppeld aan de verkeerde patiënt'.

   Dit kan bijvoorbeeld tot gevolg hebben tot in principe ongeautoriseerde gebruikers toegang krijgen tot de medische dossiers of de professionals in de zorg bij een volgende behandeling het dossier niet onder ogen krijgen. Kortom fouten kunnen worden verwacht.

7. 'Patiëntgegevens zijn onvoldoende bruikbaar voor de niet-registrerend gebruiker'.

   Patiëntgegevens zijn niet interpreteerbaar voor de gebruiker of context noodzakelijk voor een juiste interpretatie ontbreekt. Zorgprofessionals worden hierdoor onvolledig geïnformeerd of maken fouten.

8. 'Actualiteit/bron van patiëntgegevens is onduidelijk voor de gebruiker'.

   De betreffende patiëntgegevens kunnen niet 'op waarde worden ingeschat'. Mogelijk ziet de zorgprofessional patiënttoevoegingen aan voor patiëntgegevens afkomstig van de specialist of gebruikt de professional een verouderde kopie van een dossier. Dit kan resulteren in medische fouten.

9. 'Patiëntgegevens zijn onvoldoende bruikbaar voor de niet-registrerend gebruiker'

   Wanneer patiëntgegevens worden beschreven in een formaat welke niet bruikbaar is voor een gebruikers welke de gegevens verkrijgt van een andere gebruiker kan het zijn dat hij, zij of het de patiëntgegevens niet juist kan interpreteren of misschien zelfs verkeerd begrijpt. Ook kan het zijn dat noodzakelijke context ontbreekt. Ook dat kan leiden tot fouten.

10. 'Deeldossiers zijn onvindbaar voor gebruiker'.

De gebruiker kan hierdoor niet tijdig beschikken over benodigde patiëntgegevens of ziet patiëntgegevens over het hoofd, dit kan fouten in activiteiten tot gevolg hebben.

11. 'Patiëntgegevens kunnen redundant worden geregistreerd / zijn vastgelegd in deelsysteem'.

    Er kan hierdoor onduidelijkheid bestaan over de juistheid van patiëntgegevens of de gebruiker krijgt een onvolledig overzicht van de beschikbare patiëntgegevens, met bijvoorbeeld medische fouten tot gevolg of fouten bij de financiële verwerking van de behandeling.

12. 'Patiëntgegevens zijn niet toegankelijk voor professional in geval van nood'.

    In geval van nood kunnen reguliere autorisaties niet worden doorbroken. Dit kan medische gevolgen hebben voor de patiënt en hiermee ook negatief uitpakken voor het ziekenhuis, bijvoorbeeld omdat het imagoschade lijdt als gevolg van negatieve media aandacht.

13. 'Beheer van IT-systeem leidt tot problemen voor de vertrouwelijkheid en betrouwbaarheid van patiëntgegevens'

    Ook het beheer van het IT-systeem vraagt wat extra's in het ziekenhuisdomein. Onzorgvuldig beheer kan leiden tot problemen ten aanzien van vertrouwelijkheid en betrouwbaarheid van patiëntgegevens.

Om deze risicogroepen te beheersen leggen we in dit onderzoek de basis voor enkele beheersmaatregelen. We gebruiken hiervoor primair beheersmaatregelen welke geautomatiseerd zijn en we gebruiken organisatorische maatregelen ter aanvulling, om de effectiviteit van de beheersing te verhogen. Soms zijn de beheersmaatregelen eenvoudig van aard en soms zijn ze complex van aard. Helaas is het niet mogelijk alle beheersmaatregelen op een zinvolle wijze op te sommen zonder te vervallen in een volledige beschrijving van alle details rondom de maatregelen. Toch zullen we puntsgewijs enkel voorbeelden noemen om een indruk te geven van de verschillende beheersmaatregelen:

- Het gebruik van workflow management om een tijdige beschikbaarheid van patiëntgegevens te bewerkstelligen.
- Het registreren van acties op patiëntgegevens in een logboek.
- Het vastleggen van statische en dynamische werkrelaties tussen specialisten en andere (zorg)professionals.
- Het koppelen van een deeldossier aan andere deeldossiers zodat bij uitwisseling van het deeldossier de andere deeldossiers ook onder ogen komen van de zorgprofessional.

1 Introductie

1.1 Probleemstelling

Nederland staat aan de vooravond van een landelijke elektronisch medisch dossier [1][2], het zogenaamde nationale Elektronisch Patiënten Dossier, kortweg EPD[1]. Gepland is een voorziening die het mogelijk maakt om patiënt-/cliëntgegevens te delen op een nationaal niveau [3], met één 'virtueel dossier'[2] dat een keur aan medische gegevens bevat over Nederlandse patiënten/cliënten. Bij de ingebruikname van het EPD worden medicatiegegevens (via het Elektronisch Medisch Dossier (EMD)) en huisartswaarnemingen (via het WaarnemingsDossier Huisartsen (WDH)) uitgewisseld [4], maar er worden voorbereidingen getroffen om ook andersoortige informatie, zoals declaratiegegevens en gegevens over de gezondheid van kinderen, te delen middels het EPD [5].

Het EPD is een complex samenspel van techniek en organisatie, met een brede groep aan stakeholders. In potentie zijn er voordelen te behalen. Ter illustratie sommen we hier een aantal voorbeelden van voordelen van het Elektronisch Medicatie Dossier (EMD), als zijnde een concrete toepassing van het EPD [3], op:

- Het verminderen van de kans op medische fouten.
- Zorgverleners inlichten over het medicijngebruik van de patiënt/cliënt.
- De patiënt/cliënt hoeft niet met iedere zorgverlener zijn of haar medicatiegebruik door te nemen.
- De waarnemend huisarts kan de eigen huisarts informeren middels het EPD.

De kern van de argumenten voor de invoering van het EPD is het verhogen van de kwaliteit van de zorg en het verhogen van kostenefficiëntie [6]. Ook het verhogen van de patiënt-/cliëntveiligheid speelt een rol. [6]

Wij richten ons in dit onderzoek op het ziekenhuis welke als zorgaanbieder geconfronteerd wordt met het EPD. Traditioneel is het ziekenhuis een plaats waar patiëntgegevens worden geregistreerd, gebruikt en uitgewisseld. Toch vormt het EPD een prima aanleiding om het probleem onder de loep te nemen. Gegevens worden op grote schaal uitgewisseld en bovendien staat de zorg, als domein, niet stil.

Vertrouwelijk en betrouwbaarheid van medische gegevens zijn belangrijke aandachtspunten binnen het EPD project. Er is onder meer aandacht voor vragen als: wie heeft er toegang [7] en is de privacy van de patiënt/cliënt gewaarborgd [8]. Een onderzoek van TNS NIPO [38] onderstreept de gevoelige positie van privacy in dit project. Van de respondenten welke bezwaar hebben gemaakt tegen deelname aan het EPD noemde 48% van de respondenten als belangrijkste redenen voor hun bezwaar privacy. De op één en twee na meest genoemde bezwaren zijn respectievelijk de bezwaren: iedereen kan gegevens inzien/wijzigen (47%) en beveiliging/veiligheid van het systeem (32%). 6% Van alle burgers heeft bezwaar gemaakt tegen deelname aan het project [38]. Ook artsen staan niet onverdeeld positief tegenover de invoer van het EPD. Ter illustratie hiervan een quote uit een eerder onderzoek van TNS NIPO [10]: "Inmiddels heeft al 3 procent van de burgers het 'bezwaarformulier EPD' ingevuld. Onder hen een opvallend hoog aantal artsen." Het vertrouwelijkheidvraagstuk laat het ziekenhuis, het domein van ons onderzoek, dan ook niet ongemoeid. Het wordt geconfronteerd met een kritische patiënt, medewerker en publiek.

[1] Voor redenen van leesbaarheid refereren we in deze scriptie met de term EPD aan het nationale EPD.
[2] De dossiers blijven opgeslagen bij de individuele zorgaanbieders, omdat echter in potentie alle dossiers relatief eenvoudig toegankelijk zijn voor zorgaanbieders zou men kunnen spreken van één 'virtueel dossier'.

Naast vertrouwelijkheid speelt ook de betrouwbaarheid[3] een belangrijke rol bij registratie, gebruik en uitwisseling van patiëntgegevens in het ziekenhuis. Er is een evidente noodzaak voor tijdige, juiste en volledige patiëntgegevens. Bedenk bijvoorbeeld wat er gebeurt wanneer men bij een operatie uitgaat van de onjuiste gegevens of een belangrijk dossier ongemerkt niet is meegenomen bij de voorbereiding van de operatie. Het ziekenhuis kan hier negatieve gevolgen van ervaren, zeker wanneer er structurele problemen bestaan.

Centraal in dit onderzoek staat de volgende onderzoeksvraag:

"Wat zijn de risico's ten aanzien van en welke beheersmaatregelen moet het ziekenhuis nemen voor vertrouwelijkheid en betrouwbaarheid van patiëntgegevens bij de digitale registratie, gebruik en uitwisseling van deze gegevens binnen het ziekenhuis?"

We voeren ons onderzoek uit tegen de achtergrond van de invoering van het EPD. Het onderzoek richt zich echter op het algemenere probleem van de registratie, gebruik en uitwisseling van patiëntgegevens in het ziekenhuis. Nader onderzoek zou zich kunnen richten op hoe in het EPD vertrouwelijkheid en betrouwbaarheid garandeert. In *bijlage A* hebben we daarom een beschrijving van het EPD opgenomen.

De termen en concepten uit de onderzoeksvraag worden als volgt gedefinieerd:

Risico
'Gevaar voor schade of verlies, de gevaarlijke of kwade kans of kansen die zich bij iets voordoen.' [11]

Beheersmaatregelen
Maatregelen om de kans op voorkomen van een incident en/of de impact die van een incident uitgaat te verlagen.

Ziekenhuis
'Inrichting voor onderzoek, behandeling en verpleging van zieken' [11].

Vertrouwelijkheid.
Alleen daartoe geautoriseerde partijen hebben toegang tot de betreffende patiëntgegevens.

Betrouwbaarheid
Valt uiteen in de waarden tijdigheid, juistheid en volledigheid.

Tijdigheid
Patiëntgegevens zijn beschikbaar op het moment dat een (mogelijke) gebruiker de gegevens nodig heeft (of kan hebben) voor de uitvoer van een taak, met inbegrip van noodzakelijke buffers, of wet- en regelgeving en/of normen vereisen dat de patiëntgegevens beschikbaar zijn.

Juistheid
De correctheid van patiëntgegevens, zoals vastgelegd, is op het niveau noodzakelijk voor een correct verloop van activiteiten in het ziekenhuis.

Volledigheid
Alle patiëntgegevens welke nodig zijn voor de uitvoer van bepaalde activiteiten zijn aanwezig.

Patiëntgegevens
'Een patiënt is een natuurlijke persoon die zorgdiensten ontvangt of wenst te ontvangen'. Zorgdiensten zijn diensten welke vallen onder geneeskundig onderzoek of behandeling (cure). [12]

Patiëntgegevens zijn alle gegevens die betrekking hebben op de patiënt, minst relevant voor de uitvoer van activiteiten in het ziekenhuis.

[3] Betrouwbaarheid bestaat uit de waarden tijdigheid, juistheid en volledigheid.

Registratie
Het vastleggen van patiëntgegevens in een zeker medium.

Uitwisseling
Het delen van geregistreerde patiëntgegevens tussen actoren.

Gebruik
Acties welke betrekking hebben op het toegang verkrijgen tot geregistreerde patiëntgegevens, deze te bewerken en/of te verwijderen.

1.2 Verantwoording

Maar is deze aandacht voor vertrouwelijkheid en betrouwbaarheid van patiëntgegevens in het ziekenhuis gegrond? Het is redelijk deze vraag volmondig met ja te beantwoorden.

Vertrouwelijkheid dient evident waardevolle doelen als het veiligstellen van een open communicatie van patiënt naar zorgverlener [13] en heeft dus een directe impact op de medische zorg die het ziekenhuis biedt aan patiënten. Patiënten kunnen significante economische, psychologische en sociale schade oplopen wanneer medische informatie wordt ontsloten [14]. Het ziekenhuis wordt dus geconfronteerd met een kritische patiënt, een kritisch publiek en media en een kritische toezichthouder. Ook kan verwacht worden dat de professional in de zorg kritisch kan staan tegenover (bepaalde) tekortkomingen waar het gaat om vertrouwelijkheid van patiëntgegevens, hij of zij is gebonden door een (afgeleide) geheimhoudingsplicht.

Het belang van een tijdig beschikbare, juiste en volledige set van patiëntgegevens, in het bijzonder in het operationele medische proces, is evident. Medische fouten kunnen verwacht worden wanneer actoren niet tijdig beschikken over de juiste en volledige patiëntgegevens. Mogelijke gevolgen hiervan kunnen zijn een letselclaim, imagoschade en (verscherpte) controle van de toezichthouder. Ook kunnen er financiële gevolgen verwacht worden wanneer de betrouwbaarheid van patiëntgegevens niet op orde is. Ook kan verwacht worden dat professionals in de zorg kritisch staan tegenover onbetrouwbare patiëntgegevens, dit verhoogd immers de kans dat hij of zij (medische) fouten maakt.

Een optimale omgang met patiëntgegevens is niet te bereiken door deze volledig af te sluiten voor gebruikers anders dan de patiënt, ze dienen te kunnen worden gedeeld om waarde te hebben. Stakeholders, anders dan de patiënt, kunnen valide redenen hebben voor toegang tot (een gedeelte) van de beschikbare patiëntgegevens. Een hoofdbehandelaar bijvoorbeeld die een patiënt medische zorg verschaft, een specialist die door de hoofdbehandelaar wordt geraadpleegd, verpleegkundigen en ondersteunend medewerkers. Ook kan zich een noodsituatie voordoen waarbij een, onder normale omstandigheden, ongeautoriseerde professional zich toegang wil verschaffen tot (een deel van) het dossier van de patiënt in nood. Echter een volledig open communicatie van patiëntgegevens voor iedereen die wel eens belang zou kunnen zou kunnen hebben bij toegang tot de gegevens beschermd de vertrouwelijkheid maar ook betrouwbaarheid van de gegevens onvoldoende.

Anderzijds hebben we ook te maken met de noodzakelijkheden en het gebruiksgemak van de professionals welke op een dagelijkse basis geconfronteerd worden met maatregelen om de vertrouwelijkheid en betrouwbaarheid van patiëntgegevens te waarborgen. In een pilot van het EPD, welke is uitgevoerd in het oosten van Nederland [16], is bijvoorbeeld gebleken dat de identificatiepassen (de zogenaamde UZI-passen) niet altijd werden verwijderd door de gebruikers wanneer dat eigenlijk wel moest. Een bekende uitspraak uit de informatie security wereld, 'de beveiliging is zo sterk als de zwakste schakel', zou ook hier wel eens relevant kunnen blijken.

Al deze factoren maken dat patiëntgegevens kwetsbaar kunnen zijn als professionals in de zorg, welke zich bezighouden met de informatisering van die ziekenhuisprocessen welke gebruik maken van patiëntgegevens, onvoldoende aandacht besteden aan vertrouwelijkheid en betrouwbaarheid van patiëntgegevens.

Kortom het is dus van belang om een oplossing te vinden voor het complexe dilemma *optimale toegang tot patiëntgegevens, met name door partijen anders als de patiënt, met een minimum aan risico voor de primaire gebruiker van deze gegevens, het ziekenhuis*.

1.3 Onderzoekstructuur

De centrale onderzoeksvraag zoals neergelegd in *paragraaf 1.1* kan worden beantwoordt middels het beantwoorden van de volgende deelvragen:

1. *Welke vereisten stellen het zorgproces en ondersteunende activiteiten in het ziekenhuis welke patiëntgegevens gebruiken aan de registratie, gebruik en uitwisseling van patiëntgegevens?*

   Om te kunnen bepalen wat de risico's zijn welke verbonden zijn aan het registeren, gebruiken en uitwisselen van patiëntgegevens in het ziekenhuis en welke beheersmaatregelen hierbij passen beginnen we onze analyse bij het begin, het domein waar deze patiëntgegevens worden geregistreerd, gebruikt en uitgewisseld, het ziekenhuis. In het antwoord op deze deelvraag beschrijven we het ziekenhuis in een aantal modellen, welke samen beschrijven wie of wat, welke patiëntgegevens wanneer registreert, bewerkt of uitwisselt en andere relevante concepten en relaties welke invloed hebben op de registratie, gebruiken en uitwisseling van patiëntgegevens in het ziekenhuis. De lezer moet na het lezen van het hoofdstuk inzicht hebben in het domein van ons probleem.

2. *Welke bepalingen uit wet- en regelgeving en normen hebben invloed de vertrouwelijkheid en betrouwbaarheid van patiëntgegevens bij de digitale registratie, gebruik en uitwisseling van patiëntgegevens in het ziekenhuis?*

   De registratie, gebruik en uitwisseling van patiëntgegevens wordt door verschillende wet- en regelgevingen en normen gereguleerd. In het antwoord op deze deelvraag brengen we de bepalingen uit de meest relevante wet- en regelgevingen en een relevante norm in beeld. Het antwoord is beschrijvend van aard. De lezer heeft na het lezen van het antwoord inzicht hebben in welke regulaties invloed hebben op de vertrouwelijkheid en betrouwbaarheid bij registratie, gebruik en uitwisseling van patiëntgegevens in het ziekenhuis.

3. *Welke risico's voor vertrouwelijkheid en betrouwbaarheid komen voort uit de digitale registratie, gebruik en uitwisseling van patiëntgegevens in het ziekenhuis, gegeven het antwoord op deelvraag één en twee?*

   Met het antwoord op deelvraag 1 en 2 hebben we een basis gelegd om bij deze derde deelvraag de risico's in kaart te brengen welke verbonden zijn aan de registratie, gebruik en uitwisseling van patiëntgegevens in het ziekenhuis waar het gaat om vertrouwelijkheid en betrouwbaarheid. Hierbij werken we in twee stappen, we beginnen bij een gedetailleerd overzicht van risico's, verbonden aan specifieke activiteiten in het ziekenhuis welke gebruik maken van patiëntgegevens. Deze specifieke risico's abstraheren we vervolgens naar een aantal modellen welke de kern van de risico's beschrijven. De risico's worden beschreven middels de kennis die we in het antwoord op deelvraag 1 en 2 vastleggen. De lezer moet na het lezen van het antwoord inzicht hebben in de belangrijkste problemen welke spelen in het domein als we patiëntgegevens digitaal registreren, gebruiken en uitwisselen.

4. *Hoe kunnen de in deelvraag drie vastgelegde risico's beheerst worden?*

   In het antwoord op deze vierde deelvraag leggen we de basis voor beheersmaatregelen welke de risico's beheersen welke we eerder in kaart hebben gebracht in het antwoord op de derde deelvraag. De beheersmaatregelen worden beschreven middels de kennis zoals deze is vastgelegd in het antwoord op de eerste en tweede deelvraag. We gebruiken primair modellen om de beheersmaatregelen te beschrijven, begeleid door een beschrijving of aangevuld met beschreven beheersmaatregelen.

1.4 Bereik

De vertrouwelijkheid en betrouwbaarheid van patiëntgegevens bij de digitale registratie, gebruik en uitwisseling in het ziekenhuis is een complex probleemgebied met vele invloedsfactoren. Het is dan ook niet mogelijk alles mee te nemen. We beperken ons door:

- We gaan uit van de correctheid van de domeinbeschrijving. De geformaliseerde kennis vormt een aanname voor het verdere onderzoek.
- Het beschreven domein komt overeen met de meeste ziekenhuizen, maar hoeft niet volledig overeen te stemmen met een specifiek ziekenhuis.
- We zullen enkel de meest invloedrijke wet- en regelgeving en de belangrijkste norm meenemen in dit onderzoek. We bespreken hierbij hoofdlijnen, het is niet mogelijk alle fijne nuances te vangen zoals een jurist dit zou kunnen.
- We richten ons in dit onderzoek op de risico's en beheersmaatregelen welke specifiek zijn voor of specifieke karakteristieken hebben voor de digitale registratie, gebruik en uitwisseling van patiëntgegevens in het ziekenhuis (dus bijvoorbeeld geen algemene risico's verbonden aan IT-infrastructuur).
- Het onderzoek kan niet garanderen dat alle risico's in kaart zijn gebracht. Door zorgvuldige analyse van het probleem kan echter wel aannemelijk worden gemaakt dat de meest relevante risico's (risicogroepen) in kaart zijn gebracht.
- Voor praktische toepassing van de voorgestelde beheersmaatregelen is verder onderzoek nodig, we brengen in dit onderzoek slechts de noodzakelijke basis voor deze maatregelen in kaart binnen de gekozen oplossingrichting.
- We maken, in beginsel, in ons onderzoek geen onderscheidt tussen specifieke typen gegevens. Het is relevant dat het patiëntgegevens zijn, niet dat ze betrekking hebben op de behandeling van een botbreuk.

1.5 Operationalisatie

In de eerste onderzoeksvraag is waar mogelijk gebruik gemaakt van literatuur, echter bronnen met relevante, actuele en betrouwbare informatie over het Nederlandse zorgsysteem bleken schaars. De belangrijkste onderdelen zijn dan ook geverifieerd door domeinexperts.

De tweede deelvraag is beantwoord met behulp van literatuur. Omdat bij de beantwoording van deze deelvraag invloedrijke wet- en regelgeving behandeld wordt bleken goed leesbare en betrouwbare bronnen voor handen te zijn. Ook de behandelde norm bleek goed toegankelijk.

Het antwoord op deelvraag drie en vier zijn met name tot stand gekomen door een kritische analyse welke voortbouwt op de kennis welke verkregen is in de beantwoording van deelvraag één en twee.

Samenhang hoofdstukken 2 t/m 5

Enkel op basis van een zorgvuldige analyse kan een valide beeld worden verkregen van de risico's verbonden aan digitale registratie, gebruik en uitwisseling van patiëntgegevens in het ziekenhuis en beheersmaatregelen welke passen bij deze risico's en het domein. Ieder van de *hoofdstukken 2* t/m *5* speelt een eigen rol in de totstandkoming van deze analyse. *Hoofdstuk 2* modelleert het probleemgebied, het domein, en legt hiermee de basis voor verdere analyse. *Hoofdstuk 3* voegt hier relevante wet- en regelgeving en een norm aan toe. Samen vormen zij de basis voor de analyse van risico's welke we vinden in *hoofdstuk 4*. Ten slotte wordt in *hoofdstuk 5* gekeken naar de beheersmaatregelen welke passen bij deze risico's en het domein.

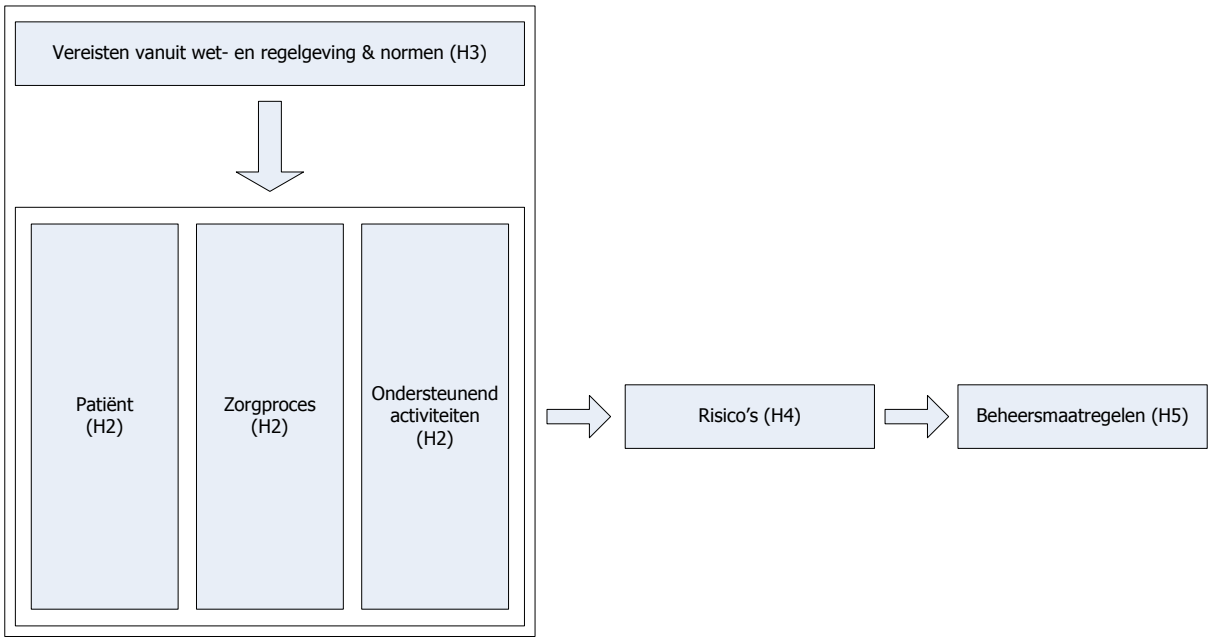


Diagram S.1 Samenhang tussen de *hoofdstukken 2* t/m *5*.

2 Het ziekenhuismodel

Om de risico's aan digitale registratie, gebruik en uitwisseling van patiëntgegevens in het ziekenhuis te kunnen bepalen en beheersen dienen we inzicht te hebben in de activiteiten, informatiestromen, actoren, competenties, autorisaties, concepten en relaties welke een rol spelen in het domein. Kortom we moeten kennis over het domein opbouwen. Dit is dan ook het doel van dit *derde hoofdstuk*.

Gegevens, ook in de medische zorg, verkrijgen vaak pas substantiële waarde wanneer ze gecommuniceerd (kunnen) worden tussen personen (en/of IT-systemen) en dienen vaak ook te kunnen worden bewerkt. In informatie-intensieve organisaties, zoals het ziekenhuis, leidt dit dan ook tot grote informatiestromen. Gegevens in de zorg zijn ook vaak gevoelig. Kleine aanwijzingen kunnen de vertrouwelijkheid van patiëntgegevens in gevaar brengen [30], wat de kritische patiënt en samenleving dan ook tegen de borst kan stuiten en in strijd kan zijn met wet- en regelgeving. Ook kan de effectiviteit, efficiëntie maar ook de veiligheid van medische zorg op het spel staan wanneer de informatievoorziening ontoereikend is. Wanneer bijvoorbeeld essentiële patiëntgegevens niet beschikbaar zijn in het geval van nood, kan dit medische fouten tot gevolg hebben wat weer kan leiden tot bijvoorbeeld imagoschade of letselclaims. Deze voorbeelden zijn typerend voor het belang van een goed inzicht in deze gegevensstromen en haar omgeving.

Dit *derde hoofdstuk* is als volgt opgebouwd: we bespreken allereerst enkele karakteristieken van de zorg relevant voor het probleemgebied, om vervolgens het zorgproces en ondersteunende activiteiten welke patiëntgegevens gebruiken in kaart te brengen. Vervolgens kijken we naar de competenties en autorisaties van de actoren welke betrokken zijn bij de gemodelleerde activiteiten. Ten slotte eindigen we met een aantal conceptuele modellen welke het probleemgebied modelleren.

2.1 Karakteristieken van de zorg

Om een goed inzicht te kunnen krijgen in wat nu een optimale beheersing van risico's in het probleemgebied betekent dient inzicht te worden verkregen in de karakteristieken van het ziekenhuis. Daarom sommen we in deze paragraaf karakteristieken van het ziekenhuis op welke invloed hebben op de digitale registratie, het gebruikt en uitwisseling van patiëntgegevens waar het gaat om vertrouwelijkheid en betrouwbaarheid:

- De zorgverlening vindt plaats in sterk gespecialiseerde, samenwerkende teams.

  Samenwerking tussen gespecialiseerde teams maakt het delen van informatie essentieel, dit heeft dan ook bijvoorbeeld impact op de verstrekking van autorisaties en de beschikbaarheid van kwalitatief hoogstaande, goede interpreteerbare patiëntgegevens.

- Zorgteams wisselen vaak van samenstelling.

  Dit heeft bijvoorbeeld gevolgen voor de wijze waarop autorisaties dienen te worden verstrekt en bewaakt. Dit moet op een flexibele maar krachtige wijze gebeuren zodat dergelijke beheersmaatregelen niet een belasting vormen voor het soepele verloop van het zorgproces maar wel voldoende de vertrouwelijkheid en betrouwbaarheid van patiëntgegevens garandeert.

- Er is een hoge werkdruk.

  Professionals in de zorg zullen hierdoor mogelijk arbeidsintensieve beheersmaatregelen (proberen te) verwerpen. Dit vraagt bovendien iets extra's van de bruikbaarheid, er is mogelijk beperkte ruimte voor training van deze professionals.

- Ziekenhuizen zijn complexe organisaties.

Dit maakt het lastig een toepassing te ontwerpen welke op een succesvolle wijze kan inspelen op de vereisten welke een dergelijke complexe omgeving stelt aan toepassingen om patiëntgegevens te registreren, gebruiken en uit te wisselen.

- De zorg is informatie-intensief.

  Er kunnen dus grote stromen van diverse soorten gevoelige en minder gevoelige patiëntgegevens worden verwacht welke allemaal in goede banen moeten lopen.

- De zorgaanbieder is meer selectief geworden waar het gaat om welke diensten het wil leveren en wie de organisatie wil behandelen.

  Dit betekent dat er tijdig voldoende bekend moet zijn over de patiënt.

- Patiënten zijn goed geïnformeerd, kritisch en willen soepel en eenvoudig het zorgproces doorlopen.

  Patiënten stellen hoge eisen aan kwaliteit van de geleverde zorg en de bescherming van hun privacy. Ze zullen kritisch staan tegenover tekortkomingen waar het gaat om vertrouwelijkheid en/of betrouwbaarheid.

- De zorg staat onder toezicht en onder controle van wet- en regelgeving.

  Dit dwingt af dat het ziekenhuis aan de vastgestelde eisen moet voldoen en laat dus weinig ruimte open voor tekortkomingen.

2.2 Het zorgproces

In *deze paragraaf* schetsen we het verloop van het gesimplificeerde en gegeneraliseerde operationele zorgproces van een ziekenhuis en de belangrijkste ondersteunende activiteiten welke patiëntgegevens registreren, gebruiken en/of uitwisselen of ondersteunende activiteiten waarbij de actor mogelijk toegang krijgt tot patiëntgegevens. Ons doel is inzicht te krijgen in die activiteiten die patiëntgegevens registeren, gebruiken en/of uitwisselen binnen het ziekenhuis.

Om *diagram 2.1* optimaal te kunnen gebruiken in onze analyse van risico's en beheersmaatregelen en de leesbaarheid van het diagram te verhogen maken we de volgende aannamen:

- De patiënt heeft niet eerder diensten afgenomen van het ziekenhuis en meldt zich fysiek bij de patiëntenbalie.
- De patiënt gaat akkoord met de wijze van diagnostiek, diagnose, behandelplan en behandeling.
- De diagnose van de patiënt is vast te stellen na enig onderzoek en vraagt om een behandeling.
- Alle activiteiten in het zorgproces worden succesvol uitgevoerd.

Om de leesbaarheid te verhogen hebben wij ervoor gekozen ons in *deze paragraaf* te beperken tot de hoofdactiviteiten van het zorgproces. In *bijlage B* kan een model worden gevonden welke het operationele zorgproces op een lager abstractieniveau beschrijft. In dit gedetailleerde diagram vindt u bovendien een indruk van de gegevensstromen welke de activiteiten in- en uitstromen en de actoren welke betrokken zijn bij de diverse activiteiten. De ondersteunende activiteiten zijn wel op het lagere abstractieniveau opgenomen in *deze paragraaf*.

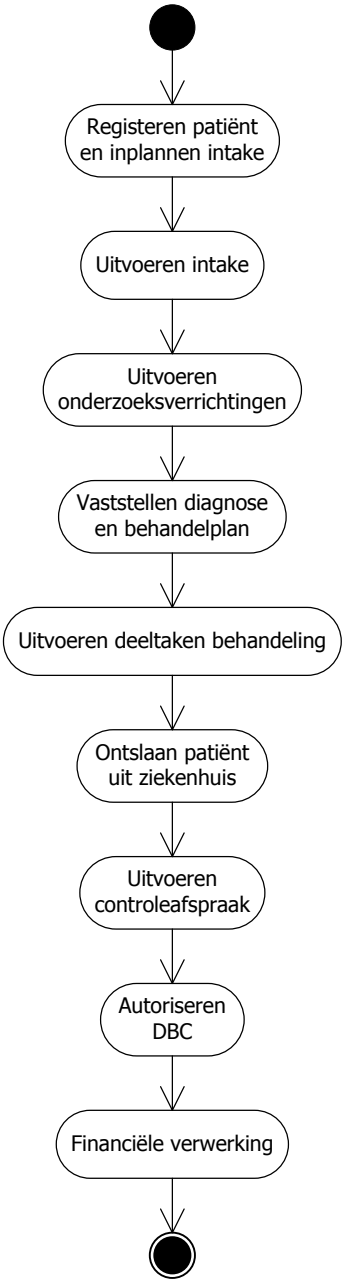


Diagram 2.1 (UML-activiteitendiagram) Het verloop, op hoofdactiviteiten, van het zorgproces. Bronnen [26][27][28][47].

DBC staat voor Diagnose Behandel Combinatie en dient de financiële administratie van ziekenhuizen en de geneeskundige geestelijke gezondheidszorg. Het DBC is een recente ontwikkeling binnen de zorg. Hoewel wij het begrip hier noemen gaan wij in dit onderzoek niet in op risico's welke specifiek verbonden zijn aan de vertrouwelijkheid en betrouwbaarheid van patiëntgegevens geregistreerd in het DBC en/of het gebruik en/of uitwisselen van patiëntgegevens middels het DBC. Lezers welke geïnteresseerd zijn in risico's en beheersmaatregelen verbonden aan het DBC verwijzen wij naar [26].

De belangrijkste ondersteunende activiteiten welke patiëntgegevens gebruiken of ondersteunende activiteiten waarbij de actor mogelijk toegang krijgt tot patiëntgegevens (gegroepeerd per actor):

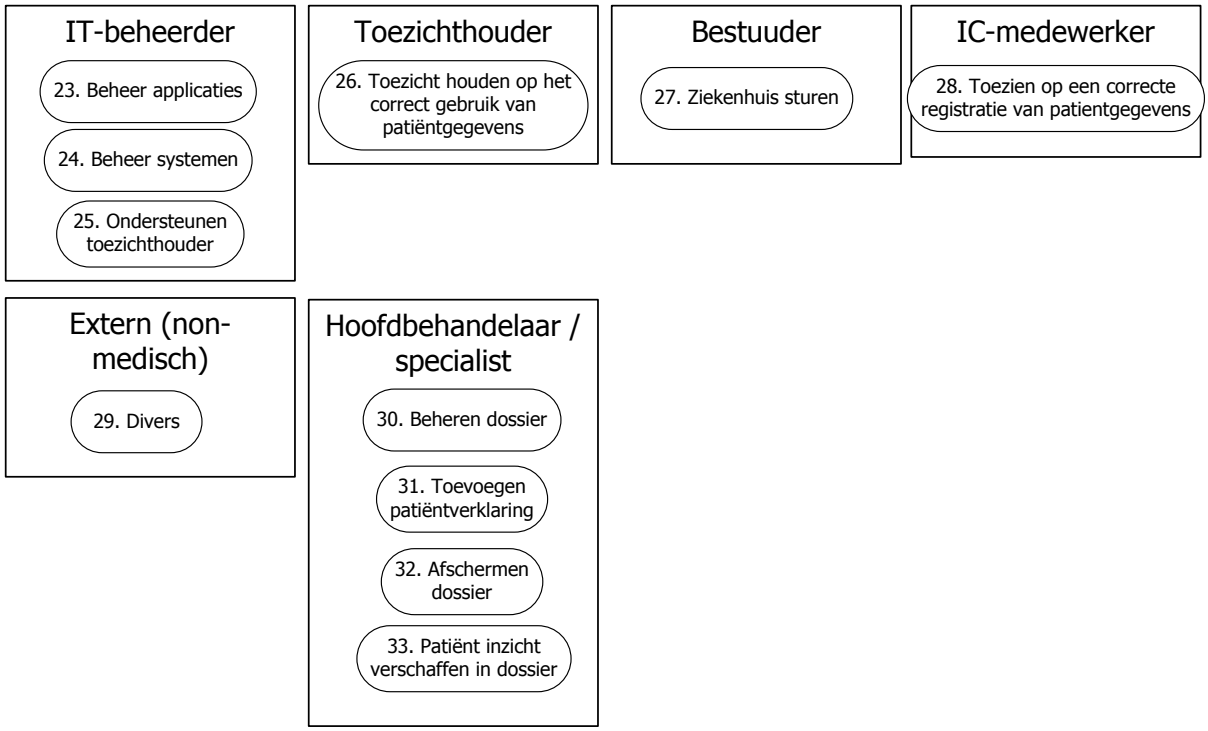


Diagram 2.3 ondersteunende activiteiten van het ziekenhuis welke gebruik maken van patiëntgegevens of ondersteunende activiteiten waarbij de actor mogelijk toegang krijgt tot patiëntgegevens.

De nummers bij de activiteiten in *diagram 2.3* worden in *bijlage C* gebruikt om te verwijzen naar *diagram 2.2* en *2.3*. Ze hebben in dit diagram nog geen betekenis.

2.3 Actoren & taken

2.3.1 Overzicht actoren

In *diagram B.1* en *diagram 2.3*, te vinden in respectievelijk *bijlage B* en *paragraaf 2.2*, hebben we de volgende actoren benoemd:

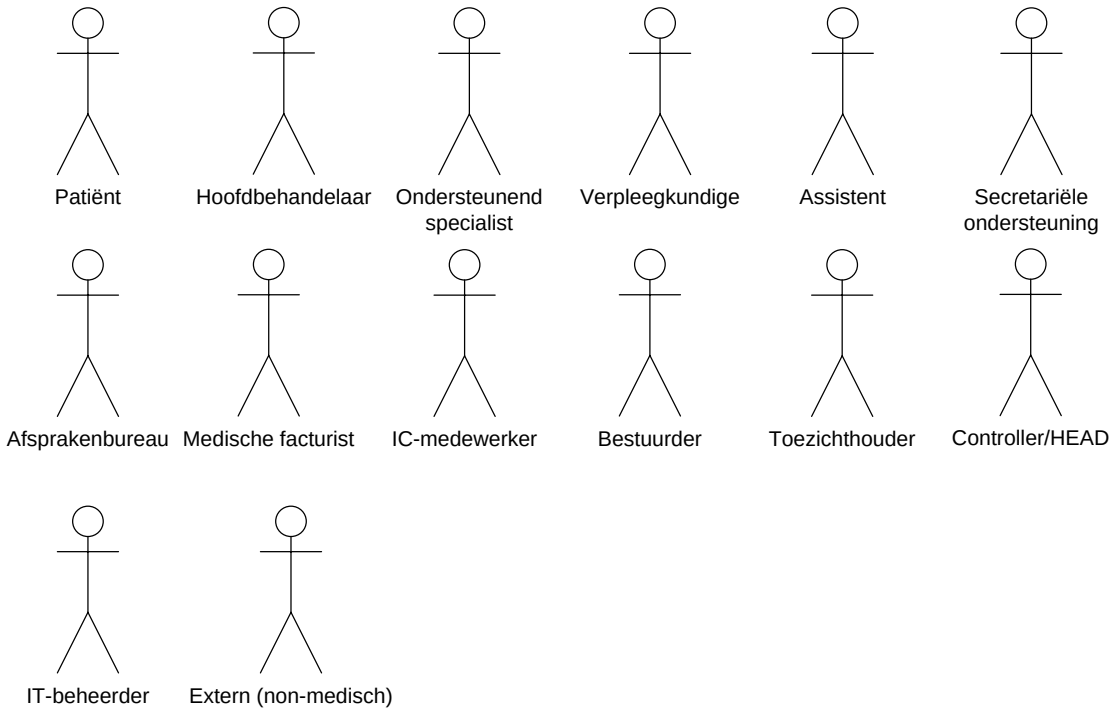


Diagram 2.4 Actoren welke patiëntgegevens gebruiken in het operationele zorgproces en ondersteunende activiteiten.

Wij gaan er vanuit dat uit de procesbeschrijving en de competentie- en autorisatiematrix, welke respectievelijk in *paragraaf 2.3.2* en *2.3.3* kunnen worden gevonden, voldoende inzicht biedt in de rol welke de diverse actoren spelen in het domein. Enkele zullen we echter introduceren:

- IC-medewerker
  De IC-medewerker ziet toe op de kwaliteit van registratie t.b.v. de facturatie van de verleende zorg aan de hand van externe normen, zoals de IC/AO Kaderregeling [29].

- Extern (non-medisch)
  Hiermee doelen we op iedereen welke mogelijk toegang zou kunnen krijgen tot patiëntgegevens maar niet actief is binnen het ziekenhuis en non-medisch is, een voorbeeld hiervan is een accountant.

2.3.2 Competentiematrix

Voor ieder van de actoren zoals benoemd in *paragraaf 2.3.1* hebben we in *tabel 2.1* vastgelegd wat hun competenties zijn aangaande de activiteiten in het operationele zorgproces zoals vastgelegd in *bijlage B*, *diagram B.1* en in de ondersteunende activiteiten in *diagram 2.3*.

Om de leesbaarheid van de tabel te bevorderen zijn de activiteiten zoals vastgelegd in *diagram B.1* gecategoriseerd op basis van de kern van de activiteiten.

De volgende symbolen worden gebruikt in *tabel 2.1*:
U: de actor voert deze activiteit uit of kan deze uitvoeren.
V: de actor is verantwoordelijk voor deze activiteit.
C: de actor controleert de uitvoer van deze activiteit.

Wanneer een symbool tussen haakjes is geplaatst betekend dit dat in sommige gevallen deze actor deze taak uitvoert maar dit doorgaans niet het geval is.

	Patiënt	Hoofdbehandelaar	Ondersteunend specialist	Verpleegkundige	Assistent	Sec. ondersteuning	Afsprakenbureau	Medisch facturist	IC-medewerker	Bestuurder	IT-beheerder	Toezichthouder	Controller / HEAD
Registratie patiënt													
Registratie persoonsgegevens		(U)/V	(U)	(U)	(U)	(U)	U		C				C
Controle & registratie van Wettelijk Identificatie Document (WID)		(U)/V	(U)	(U)	(U)	(U)	U		C				C
BSN opvraag & registratie		(U)/V	(U)	(U)	(U)	(U)	U		C				C
Intake													
Plannen intake		V					U						
Intake		U/V	U	U	U				C				
Dossier													
Verificatie dossier(s)*		U/V	(U)			(U)			C			(C)	
Ophalen dossier(s)*		U/V	U/V	U	U				C			(C)	
Registratie medische patiëntgegevens		U/V	U/V	U	U				C			(C)	
Beheren van het dossier*		U/V/C							C			(C)	
Diagnostiek													
Uitvoeren taak (t.b.v. diagnostiek)		U/V	U/V	U	U				C			(C)	
Diagnose stellen		U/V							C			(C)	
Voorbereiding													
Inzien agenda (van specialist)		V	V		U	U	U		C				
Plannen intake/behandeling/ controle afspraak		V	V		U	U	U						
Verkrijgen taak		V	U/V	U	U	U							
Behandeling													
Vaststellen behandeling		U/V	U						C			C	
Uitvoeren taak (t.b.v. behandeling)		U/V	U/V	U	U				C			C	
Aansturen van behandeling		U/V	U	U					C			C	
Afronden behandeling													

Ontslag uit ziekenhuis		U/V	U	U	U				C			C	
Controle afspraak		U/V	U						C			C	

Beheer IT													
Beheer systemen									C		U/V /C		
Beheer applicaties									C		U/V /C		
Ondersteunen toezichthouder									C		U/V /C		

Toezicht													
Toezien op een correct gebruik van patiëntgegevens									C			U/V	
Toezien op een correcte registratie van patiëntgegevens									U/V				

Tabel 2.1 Competentiematrix van de actoren uit *diagram 2.4*. Bron [26][27].

2.3.3 Autorisatiematrix

Voor de twee voor ons probleem belangrijkste 'administratieve producten' hebben we in *tabel 3.2* vastgelegd welke autorisaties de actoren, zoals weergegeven in *paragraaf 3.3.1*, heeft ten aanzien van deze 'producten'.

De volgende symbolen worden gebruikt in *tabel 2.2*:
L: De actor heeft autorisaties om het betreffende product te lezen.
S: De actor heeft autorisaties om het betreffende product te wijzigen.
V: De actor heeft autorisaties om het betreffende product te verwijderen.

	Patiënt	**Hoofdbehandelaar**	**Ondersteunend specialist**	**Verpleegkundige**	**Assistent**	**Sec. ondersteuning**	**Afsprakenbureau**	**Medisch facturist**	**IC-medewerker**	**Bestuurder**	**IT-beheerder**	**Toezichthouder****	**Controller / HEAD**
Registratie patiënt	L	L/S	L/S	L	L	L	L/S/V	L/S	L			L	L
Dossiers	L/S/V*	L/S/V	L/S	L/S	L/S				L			L	

* Hiermee lopen we vooruit op *hoofdstuk 3*, waar uit analyse van relevante wet- en regelgeving deze autorisaties naar voren komen als patiëntrechten. Schrijf- en verwijderrechten zijn voor de patiënt altijd indirect, via wet- en regelgeving en via de beheerverantwoordelijke voor het dossier.

** Deze toegang is tijdelijk en zal worden verstrekt op en voor het moment dat een controle plaatsvindt.

Tabel 2.2 Autorisatiematrix voor de drie belangrijkste 'administratieve producten' in het zorgproces en ondersteunende activiteiten. Bron [27].

2.4 Concepten

In deze *vierde paragraaf* kijken we naar vanuit een hoger abstractieniveau naar het probleemgebied zoals in de *voorgaande paragraven* beschreven en vullen waar modellen aan met concepten en relaties. Het doel is het gehele probleemgebied in beeld te krijgen. We benoemen hiervoor concepten en de relaties tussen deze concepten, minst relevant voor het probleemgebied van de registratie, gebruik en uitwisseling van patiëntgegevens in het ziekenhuis. De hier gepresenteerde modellen zijn mede gebaseerd op [28].

2.4.1 Kernconcepten

In onderstaand diagram, *diagram 3.5*, benoemen we de kernconcepten van het domein. In de hierop volgende paragraven richten we ons steeds op één (of enkele) van deze kernconcepten om deze op een lager abstractieniveau uit te diepen. Ieder diagram in deze paragraaf is voorzien van een korte toelichting.

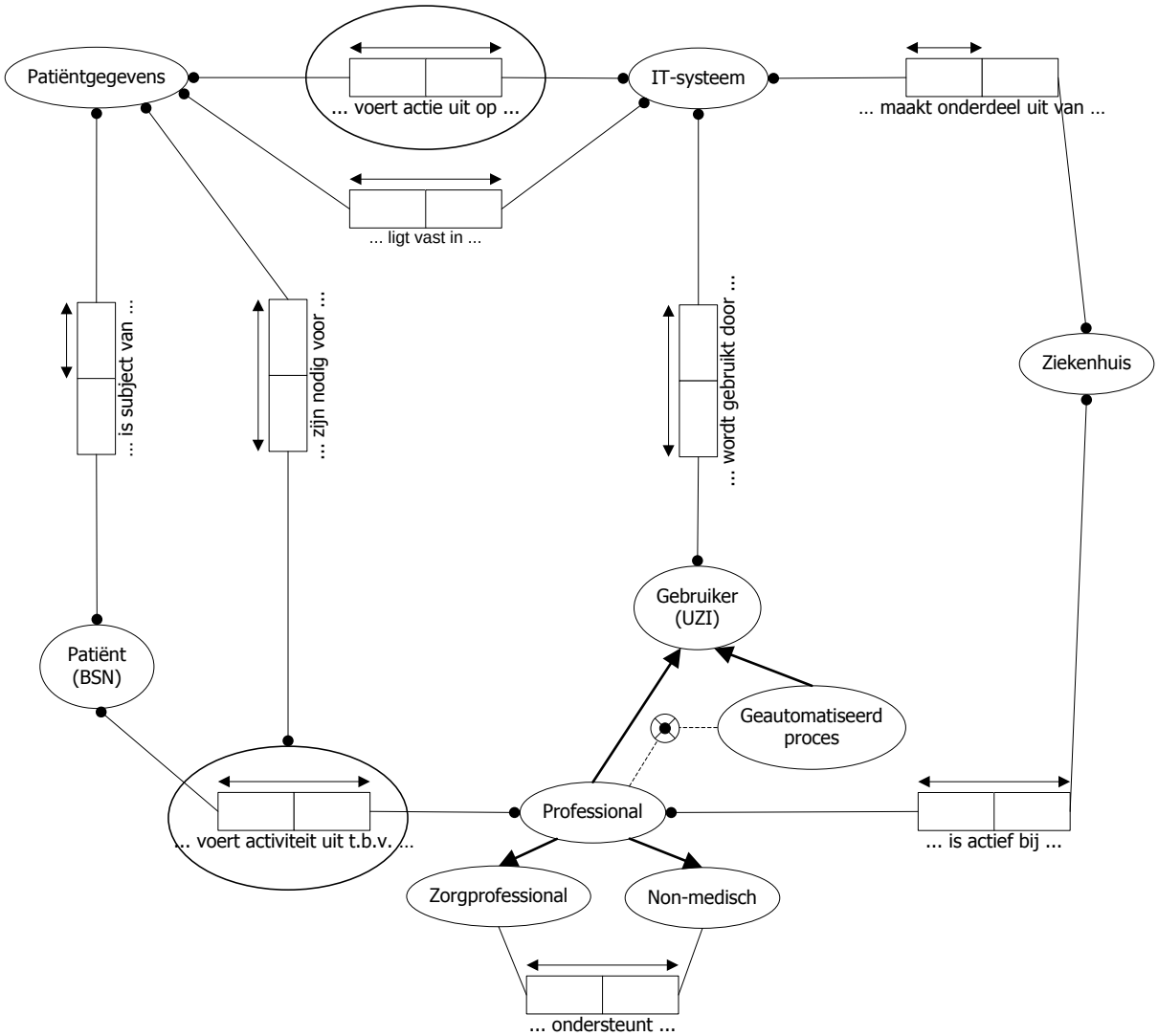


Diagram 2.5 (ORM-diagram) Concepten en relaties van het domein op een hoog abstractieniveau.

Een professional voert een activiteit uit ten behoeve van een patiënt. Hiervoor zijn bepaalde patiëntgegevens nodig waarvan de betreffende patiënt het subject is. We onderscheiden op dit abstractieniveau twee typen professionals: de zorgprofessional en de non-medische professional welke de zorgprofessional ondersteunt. De professional is actief bij een ziekenhuis. We hebben

bewust gekozen voor de woorden 'actief bij', het kan namelijk gaan om een professional welke werkzaam is bij een externe organisatie maar die via het ziekenhuis toegang heeft tot patiëntgegevens, denk bijvoorbeeld aan een toezichthouder. Een professional is een gebruiker en maakt gebruik van een IT-systeem, bijvoorbeeld om een deeldossier in te zien. Echter ook een geautomatiseerd proces kan een IT-systeem gebruiken. De gebruiker voert middels het systeem bepaalde acties uit op een verzameling patiëntgegevens welke gekoppeld zijn aan de patiënt.

2.4.2 Specificatie kernconcepten

3.4.2.1 Patiëntgegevens

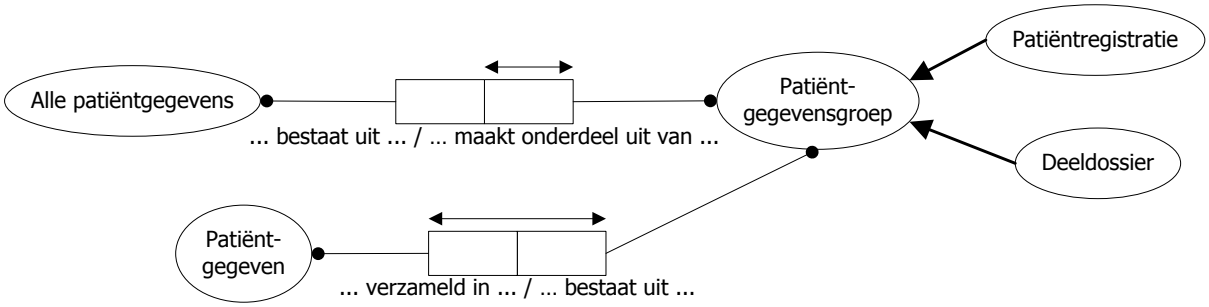


Diagram 2.6 (ORM-diagram) Detaillering kernconcept 'patiëntgegevens'.

Zoals gemodelleerd in *diagram 2.5* is de patiënt het subject van een verzameling patiëntgegevens. We onderscheiden voor dit onderzoek patiëntgegevens op verschillende abstractieniveaus. We onderkennen: alle patiëntgegevens, een zekere subset hiervan (patiëntgegevensgroep) en een individueel patiëntgegeven. Zo vormt een patiëntregistratie een logische subset van alle patiëntgegevens en kunnen we binnen deze subset individuele gegevens onderscheiden zoals de naam van de patiënt.

We onderscheiden ten minste twee typen patiëntgegevensgroepen: het deeldossier en de patiëntregistratie. Beiden vervullen een prominente rol binnen verschillende activiteiten zoals benoemd in *paragraaf 2.2*. Het model laat ruimte open voor andere typen patiëntgegevensgroepen.

2.4.2.2 Gebruiker

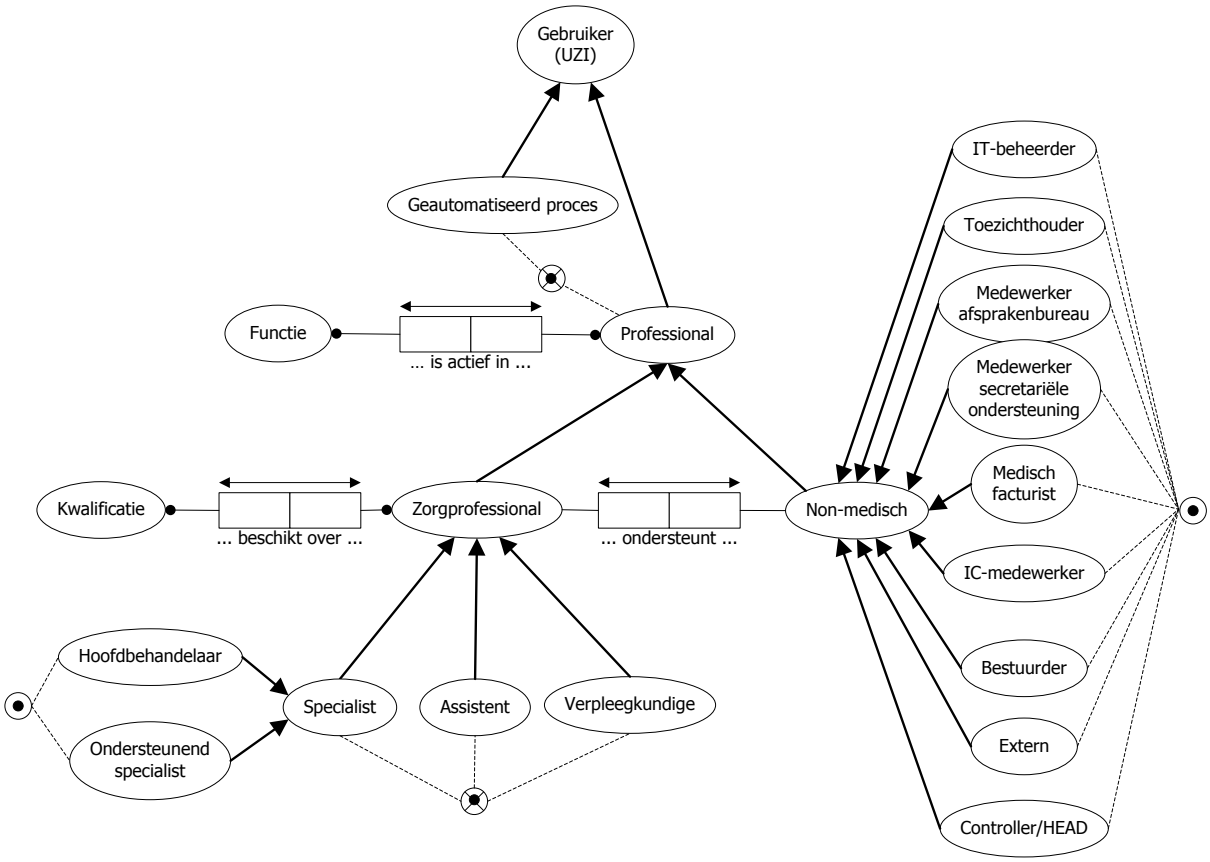


Diagram 2.7 (ORM-diagram) Detaillering kernconcept 'gebruiker'.

We onderscheiden twee typen gebruikers: geautomatiseerde proces en professional. Ze worden beiden uniek geïdentificeerd door een Unieke Zorgverlener Identificatie (UZI)[4]. Het concept professional onderscheiden we op haar beurt naar: zorgprofessional en non-medisch. We kunnen de zorgprofessionals alsmede de non-medisch opsplitsen naar alle actoren zoals eerder benoemd in *paragraaf 2.2*. Iedere professional is actief in één of meer functies en een zorgprofessional beschikt over één of meer kwalificaties. Binnen de behandeling van één patiënt kan een specialist de rol van hoofdbehandelaar vervullen of die van ondersteunend specialist. Een specialist kan tegelijkertijd, over meerdere behandeling heen, zowel de rol van hoofdbehandelaar als ondersteunend specialist vervullen.

2.4.2.3 Ziekenhuis

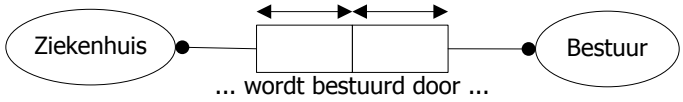


Diagram 2.8 (ORM-diagram) Detaillering kernconcept 'ziekenhuis'.

Het ziekenhuis is binnen ons probleemgebied een eenvoudig concept. Een ziekenhuis wordt bestuurd en omdat hierbij bepaalde patiëntgegevens worden gebruikt, denk bijvoorbeeld aan geaggregeerde patiëntgegevens om de patiëntlogistiek aan te sturen, is het relevant dit te modelleren.

[4] De Unieke Zorgverlener Identificatie (UZI) is een bestaande voorziening en wordt toegepast in het EPD.

2.4.2.4 Patiënt

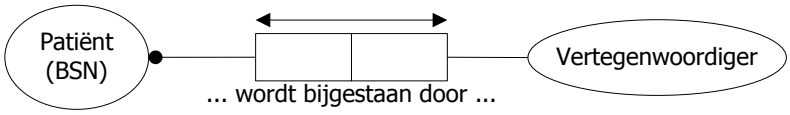


Diagram 2.9 (ORM-diagram) Detaillering kernconcept 'patiënt'.

Ook de patiënt is waar het gaat om dit onderzoek een eenvoudig concept. De patiënt wordt geïdentificeerd, dit nemen we tenminste aan voor dit onderzoek, door een identificerend Burger Service Nummer (BSN)[5]. De patiënt kan in zijn of haar behandeling worden bijgestaan door een vertegenwoordiger wanneer hij of zij niet (volledig) in staat is beslissingen te nemen over zijn of haar behandeling.

2.4.2.5 IT-systeem

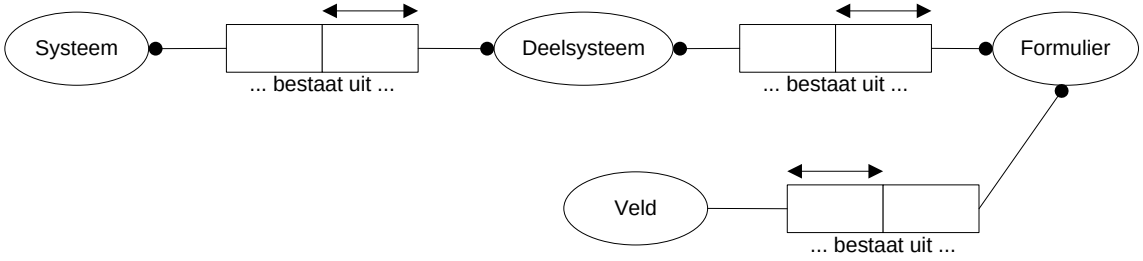


Diagram 2.10 (ORM-diagram) Detaillering kernconcept 'IT-systeem'.

Binnen het geheel aan IT binnen het ziekenhuis kunnen we één of meerdere deelsystemen onderkennen. Deze bestaan op haar beurt uit formulieren, welke weer bestaan uit velden.

2.4.2.6 Gegevensgebeurtenis

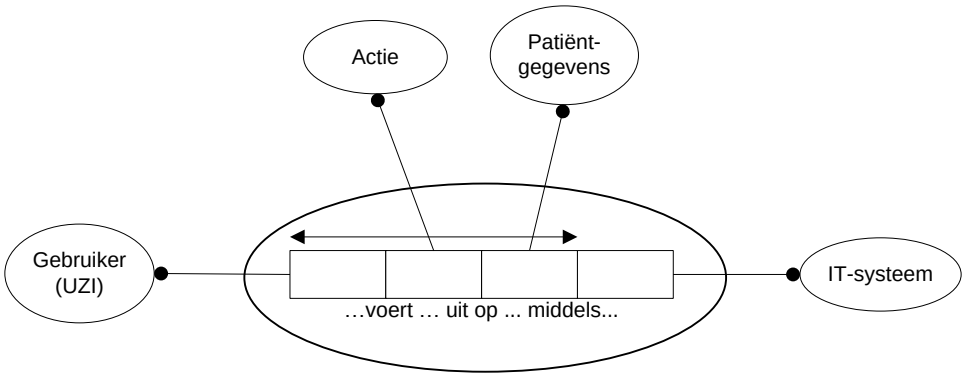


Diagram 2.11 (ORM-diagram) Detaillering kernconcept 'actie'.

Acties worden uitgevoerd op patiëntgegevens door een zekere gebruiker middels een zeker IT-systeem.

[5] Ook het Burger Service Nummer (BSN) is een bestaande voorziening en wordt ondermeer gebruikt in het EPD.

Let op dat de concepten gebruiker, patiëntgegevens en IT-systeem eerder geïntroduceerd zijn, zij zijn dan ook slechts opgenomen als referentie.

2.4.2.7 Activiteit

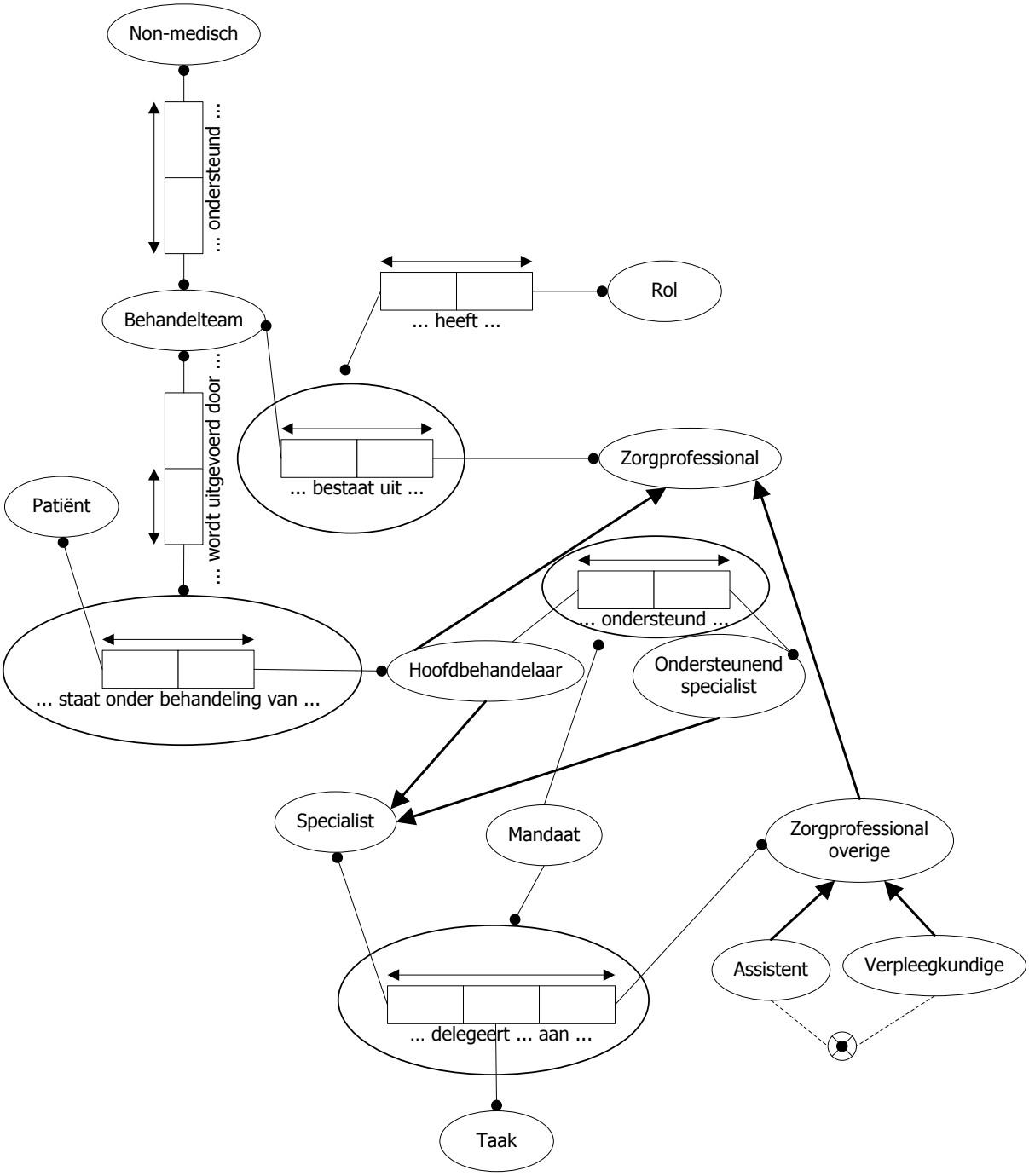


Diagram 2.12 (ORM-diagram) Detaillering kernconcept 'activiteit'.

Een patiënt staat onder behandeling van een hoofdbehandelaar. Deze wordt mogelijk ondersteund door een ondersteunend specialist. Deze beiden kunnen taken delegeren aan assistenten en verpleegkundigen. Samen vormen zij een behandelteam, waarin iedereen een zekere rol vervult. Dit behandelteam wordt ondersteund door non-medische actoren, welke direct of indirect bijdragen, daarom verwijzen we niet naar specifieke non-medische actoren.

3 Juridische en norm vereisten aan de registratie, gebruik en uitwisseling van patiëntgegevens

In *hoofdstuk 2* hebben we 'het ziekenhuis gemodelleerd', maar dit is op zichzelf onvoldoende als basis om de risico's aan digitale registratie, gebruik en uitwisseling van patiëntgegevens in het ziekenhuis en beheersmaatregelen ten aanzien van deze risico's te kunnen modelleren. Wet- en regelgeving maar ook normen reguleren het probleemgebied en hebben dus invloed op wat wenselijk is en wat niet en dus op risico's en beheersmaatregelen ten aanzien van het probleem. In dit *derde hoofdstuk* kijken we naar twee van de meest invloedrijke stukken wet- en regelgeving en de meest invloedrijke norm, in Nederland, op het gebied van informatiebeveiliging in de zorg.

Kijken we naar [12] dan zien we dat verschillende stukken wet- en regelgeving invloed hebben op het domein van patiëntgegevens bij zorgaanbieders. Echter niet alle stukken wet- en regelgeving welke genoemd worden zijn voor dit onderzoek relevant. Voor de meeste in deze bron genoemde wet- en regelgeving geldt ofwel dat deze ingaat op registers (bijvoorbeeld voor het BSN of zorgprofessionals), welke we als gegeven beschouwen; richten zich slechts op een klein deelgebied (bijvoorbeeld de Wet Elektronische Handtekening); of zijn te weinig specifiek voor ons probleemgebied (bijvoorbeeld de Kwaliteitswet Zorginstellingen). De 'wet EPD' is weliswaar interessant, maar nog in voorbereiding en heeft dus nog geen juridische status. Dit betekend dat we twee relevante stukken wet- en regelgevingen overhouden welke een brede invloed hebben op patiëntgegevens, ook in het ziekenhuis: de Wet bescherming Persoonsgegevens (Wbp) en de Wet op de geneeskundige behandelingsovereenkomst (Wgbo). Naast wet- en regelgeving zijn er normen welke van relevant zijn binnen ons probleemgebied. In dit onderzoek betrekken we de in Nederland meest relevante norm voor informatiebeveiliging in de zorg, de NEN 7510-norm.

3.1 Wet bescherming persoonsgegevens

Voor de behandeling van de Wet bescherming persoonsgegevens (Wbp) is bron [40] leidend. De Wbp is niet in alle gevallen waar persoonsgegevens worden geregistreerd relevant, er zijn uitzonderingen. Dus allereerst zullen we voor de volledigheid uiteenzetten waarom de Wbp van toepassing is op het probleemgebied:

- De gegevens welke in het kader van dit onderzoek relevant zijn, zijn 'persoonsgegevens' (in termen van het Wbp). Het zijn 'persoonsgegevens' want het bevat 'naar hun aard' feitelijke gegevens over een natuurlijk persoon en deze persoon is identificeerbaar. Anders gezegd de identiteit van het subject van de gegevens, in ons geval de patiënt dus, is zonder onevenredige inspanning vast te stellen. Ook gegevens over objecten kunnen worden aangemerkt als 'persoonsgegevens' wanneer zij iets zeggen over de persoonlijke levenssfeer van de patiënt waaraan ze gekoppeld zijn.
- Gegevens worden verwerkt door het ziekenhuis: men kan er macht over uitoefenen en er kunnen handelingen mee worden verricht. Hierdoor kan binnen de Wbp worden gesproken over het 'verwerken van gegevens'.
- In dit onderzoek richten wij ons op de systematische verwerking van patiëntgegevens, hier is de Wbp op van toepassing.
- De ziekenhuizen waarop wij ons in dit onderzoek richten, bevinden zich in Nederland.
- Het gebruik van patiëntgegevens is niet uitgezonderd van de Wbp.

Dit maakt dat het Wbp van toepassing is op de registratie, gebruik en uitwisseling van patiëntgegevens in het ziekenhuis. Om volledig te zijn zullen we ook vaststellen waarom het ziekenhuis patiëntgegevens mag gebruiken van de Wbp:

- Gegevensverwerking moet volgens de Wbp altijd plaatsvinden op basis van ten minste één grondslag. In het domein van het ziekenhuis zouden verschillende grondslagen van toepassing kunnen zijn (bijvoorbeeld verwerking op basis van ondubbelzinnige toestemming, noodzakelijk voor de uitvoering van een overeenkomst, uitvoering van een vitaal belang van de betrokkene),

- De Wbp geeft het ziekenhuis expliciete toestemming om, in beginsel, gegevens over de gezondheid van personen te verwerken. Ook andere zogenaamde 'speciale persoonsgegevens' (bijvoorbeeld over ras of geloof) mogen worden verwerkt door het ziekenhuis minst dit relevant is voor de behandeling.

Ook moeten we de rol van het ziekenhuis vaststellen, de Wbp onderkent namelijk 'verantwoordelijke' en 'verwerkers'. Ziekenhuizen zijn doorgaans de 'verantwoordelijke'. Dit wil zeggen dat dit de partij is 'die het doel en de middelen van werking vaststelt'. Dit kan zowel in de formeel-juridische zin zijn als in de sociale zin, oftewel wie volgens de geldende zienswijze door de maatschappij als verantwoordelijkheid wordt aangemerkt. In een ziekenhuis is de directie of Raad van Bestuur vaak eindverantwoordelijk, specialisten zijn medeverantwoordelijk voor de verwerking van patiëntgegevens.

Nu uiteengezet is dat de Wbp van toepassing is op het probleemgebied kunnen de belangrijkste vereisten worden vastgelegd welke de Wbp stelt aan de registratie, gebruik en uitwisseling van patiëntgegevens in een ziekenhuis:

- Patiëntgegevens dienen behoorlijk en op zorgvuldige wijze en in overeenstemming met de wet te worden geregistreerd.
- Patiëntgegevens van derden dienen rechtmatig verkregen te zijn, oftewel met kennis en (veronderstelde) toestemming van de patiënt.
- Patiëntgegevens mogen enkel voor een welbepaald en uitdrukkelijk doel worden verwerkt.
- Patiëntgegevens mogen niet zonder meer voor een doel anders dat het initiële doel worden gebruikt.
- Minst de patiëntgegevens direct herleidbaar zijn tot de patiënt, dient, in beginsel, in een dergelijk geval de toestemming van de patiënt te worden verkregen.
- Niet altijd hoeft men te beschikken over de expliciete toestemming van de patiënt voor secundair gebruik, echter de patiënt moet wel zijn geïnformeerd over dit gebruik en hij of zij moet geen bezwaar hebben gemaakt tegen het gebruik van zijn of haar patiëntgegevens voor dit doel.
- Secundair gebruik van geregistreerde patiëntgegevens mag niet onverenigbaar zijn met het initiële doel (o.a. bepaald door factoren als verwantschap, aard van de gegevens en gevolgen voor de betrokkenen).
- Er moet door het ziekenhuis / professional altijd worden gekeken of er geen minder ingrijpend alternatief is zodat hetzelfde doel bereikt kan worden met minder patiëntgegevens.
- De verwerking van patiëntgegevens mag niet bovenmatig zijn, maar dient wel toereikend en ter zake dienend te zijn:
    - Dit wil zeggen dat geregistreerde patiëntgegevens niet te gedetailleerd mogen zijn maar ook niet te weinig patiëntgegevens verzameld mogen worden, dit om te voorkomen dat een onvolledig beeld geschetst wordt.
    - De verzameling van patiëntgegevens moet het gestelde doel dienen.
    - De geregistreerde patiëntgegevens moeten juist en nauwkeurig zijn, binnen de grenzen van het redelijke. Bovendien moeten ze ook zo objectief mogelijk zijn.
- Een patiënt wiens patiëntgegevens verwerkt worden moet geïnformeerd worden over de identiteit van de verzamelaar en voor welke doeleinden de gegevens verzameld en verwerkt worden:
    - Het kan echter zijn dat dit gezien de aard van de patiëntgegevens, de wijze van verkrijgen, het gebruik en de gevoeligheid van de patiëntgegevens, deze punten onvoldoende zijn en dat er meer informatie dient te worden verstrekt aan de patiënt.
    - Het ziekenhuis moet weten dat de patiënt hiervan op de hoogte is, een vermoeden is niet voldoende. Men dient de informatie zo te verstrekken dat de patiënt deze informatie ook daadwerkelijk ontvangt.
    - Omdat er in de behandeling van patiënten doorgaans sprake is van een situatie waarbij de gegevens via de patiënt zelf verkregen worden moet deze, indien mogelijk, vooraf worden geïnformeerd.
    - Wanneer de patiëntgegevens niet direct via de betrokkene verkregen worden moet deze voorlichting plaatsvinden op het moment van registratie, of als het ziekenhuis de patiëntgegevens enkele vastlegt voor verspreiding aan derden, op het moment

van de eerste verstrekking. Het kan zijn dat het onredelijk is dit te verlangen, wel moet dan de herkomst van de gegevens worden vastgelegd.
    - In het geval van een groep patiënten mag men volstaan met een algemenere vorm van informatieverspreiding (bijvoorbeeld via een media, waarvan dan wel vaststaat dat het de gehele doelgroep bereikt).
- Iedereen die dit met redelijk tussenpozen verzoekt, moet door het ziekenhuis/zorgprofessional worden geïnformeerd of er patiëntgegevens zijn geregistreerd, gebruikt en/of uitgewisseld en zo ja welke:
    - Een dergelijk verzoek moet binnen een maand beantwoordt worden door een schriftelijke zending van de volgende gegevens:
        1. Een compleet overzicht van de geregistreerde patiëntgegevens.
        2. Omschrijving van doel of doeleinden, de categorie waarop de registratie, gebruik en/of uitwisseling betrekking heeft en de gebruikers of categorieën van gebruikers.
        3. Alle gegevens over de herkomst van de patiëntgegevens, voor zover beschikbaar.
        4. Desgevraagd informatie over de systematiek van de uitwisseling, waarbij overigens geen bedrijfsgeheimen hoeven te worden prijsgegeven.
    - Hierbij dient men wel zekerheid te hebben over de identiteit van de aanvrager, zodat het antwoord enkel het subject van eventuele patiëntgegevens bereikt.
    - Voor personen onder de 16 kan een verzoek enkel worden aangevraagd en het antwoord enkel gericht zijn aan de wettelijke vertegenwoordiger.
- Het ziekenhuis is op verzoek van de patiënt verplicht geregistreerde patiëntgegevens die feitelijk onjuist en/of onvolledig en/of niet ter zake dienend zijn voor het doel van verzameling en/of ze in strijd zijn met de Wbp of een andere wet te corrigeren:
    - Correctie betekend in deze verbetering, aanvulling, verwijdering, afscherming of op een andere wijze voorkomen dat patiëntgegevens worden gebruikt.
    - Binnen een maand moet aan de patiënt teruggekoppeld worden in hoeverre er kon worden voldaan aan het verzoek tot correctie.
- Een professional welke 'bijzondere persoonsgegevens' (bijvoorbeeld over de gezondheid van een persoon) registreert, gebruikt en/of uitwisselt wordt gebonden door een geheimhoudingsplicht.

Ten slotte enkele laatste opmerking over de Wbp:

- De Wbp wordt 'overruled' door meer specifieke wet- en regelgeving zoals bijvoorbeeld de Wgbo.

3.2 Wet op de geneeskundige behandelingsovereenkomst

Puntsgewijs vermelden we in *deze paragraaf* de belangrijkste bepalingen uit de Wgbo, voor zover het redelijk is om te verwachten dat deze invloed hebben op de registratie, gebruik en/of uitwisseling van patiëntgegevens in het ziekenhuis. De informatie is afkomst uit [41].

Deeldossierplicht

- De specialist heeft een plicht om een deeldossier bij te houden (art. 454.1).
- Deze plicht omvat in ieder geval de volgende patiëntgegevens: aantekeningen patiëntgegevens omtrent gezondheid, uitgevoerde verrichtingen en overige patiëntgegevens welke nodig zijn voor een goede zorgverlening (art. 454.1).
- Desgevraagd dient een patiëntverklaring hierin te worden opgenomen (art. 454.2).
- Het deeldossier dient tot tien jaar na vervaardiging, of langer indien dit professional wenselijk is, te worden bewaard (art. 454.3).
- Ook de patiënt kan de beheerverantwoordelijke voor het deeldossier verzoeken het dossier langer te bewaren.

- Op verzoek van de patiënt moeten de stukken drie maanden na vervaardiging worden vernietigd (art. 455.1), tenzij dit in strijd is met de wet of de 'aanmerkelijke belangen' van een derde (art. 455.2).
- De beheerverantwoordelijk specialist dient, tegen een redelijke vergoeding, desgevraagd de patiënt zo spoedig mogelijk inzage te verlenen in het dossier, tenzij dit de levenssfeer van een derde in gevaar brengt (art. 456).
- De patiënt heeft in beginsel geen recht op de originele deeldossiers, deze komen tot aan de opsteller of beheerderverantwoordelijke.
- De beheerverantwoordelijk specialist kan een dossier overdragen aan een opvolger, in dat geval kan de patiënt bezwaar maken tegen de overdracht.

Geheimhoudingsplicht

- De specialist heeft een geheimhoudingsplicht, tenzij verstrekking kan plaatsvinden met toestemming van de patiënt of de wet de specialist hiertoe verplicht (art. 457.1).
- Deze geheimhoudingsplicht geldt bovendien niet voor zorgprofessionals direct betrokken bij de behandelingsovereenkomst, voor zover deze patiëntgegevens nodig zijn voor de behandeling (art. 457.1).
- Deze geheimhoudingsplicht geldt boven ook niet voor vertegenwoordigers (begeleiders) van de patiënt, voor zover verstrekking van informatie past binnen de professionele grenzen van goed hulpverlenerschap (art. art. 457.3).

3.3 NEN 751X

De NEN 751X normen zijn een product van het Nederlands-normalisatie instituut (NEN). Ze zijn relevant voor iedere 'zorginstellingen en –organisaties werkzaam in de gezondheidszorg, ongeacht de aard en omvang van het bedrijfsproces' in Nederland [65]. Het beschrijft '… welke soorten maatregelen de leiding binnen organisaties moet treffen om via een gecontroleerd proces op adequate wijze met (medische) gegevens om te gaan.' [65].

De NEN 751X norm valt uiteen in drie delen. In NEN 7510 wordt de basis gelegd voor beheersmaatregelen welke relevant zijn voor ieder type zorgaanbieder. In NEN 7511 wordt NEN 7510 op een lager detailniveau uitgewerkt voor specifieke typen zorgaanbieders. In NEN 7512 richt zich op de communicatie van gegevens van zorgaanbieders. In dit onderzoek richten wij ons op NEN 7510.

De NEN 751X normen hebben echter een tweeledig karakter. De standaard is door de Minister van VWS voorgeschreven als 'verplicht' [17]. Hierdoor zou men dus kunnen stellen dat de standaard min of meer een juridische status heeft gekregen. Maar de NEN 751X normen verschillen in karakter van de andere vereisten welke we hebben benoemd in *dit hoofdstuk*, ze schrijven namelijk concrete beheersmaatregelen voor. We hebben er dan ook voor gekozen het direct te integreren met *hoofdstuk 5* waar we ingaan op beheersmaatregelen.

4 Risico's

De kern van dit onderzoek is het in kaart brengen van de risico's ten aanzien van vertrouwelijkheid en betrouwbaarheid van patiëntgegevens bij digitale registratie, gebruik en uitwisseling van deze patiëntgegevens in het ziekenhuis en het leggen van de basis voor maatregelen om deze risico's te beheersen. In dit *vierde hoofdstuk* leggen we de risico's vast. We doen dit in twee stappen, op basis van kennis uit *hoofdstuk 2* en *3*. We brengen allereerst uitgebreid de risico's per activiteit zoals benoemd in *diagram B.1* in kaart, om deze vervolgens te abstraheren tot enkele risicogroepen.

Dit *vierde hoofdstuk* is als volgt opgebouwd: we starten met het vastleggen van een kader om risico's te beschrijven, hierna brengen we de risicogroepen in beeld. De uitgebreide risicoanalyse per activiteit is ondergebracht in *Bijlage C*.

4.1 Kader

Voor alle risico's welke we identificeren in onze analyse geldt dat zij effect hebben op vertrouwelijkheid en/of betrouwbaarheid, oftewel, tijdigheid, juistheid en/of volledigheid. 'Effect hebben' betekent dat het redelijkerwijs te verwachten is dat er een inherent negatief gevolg uitgaat van het geschetste scenario, waarbij een 'negatief gevolg' betekent dat het ziekenhuis schade oploopt als gevolg van het zich voordoen van het scenario. Schade wordt in [11] gedefinieerd als 'nadeel dat voor iemand of voor een bepaald belang uit een gebeurtenis, handeling of handelwijze voortvloeit' of 'al wat de gaafheid van iets tenietdoet en (daardoor) de waarde ervan vermindert'. Onze aandacht gaat in dit onderzoek uit naar schade waar het ziekenhuis de negatieve gevolgen van ervaart. Om dit concreet te maken kijken wen naar schade aan patiëntregistratie en/of deeldossier.

Om dit begrip van risico hanteerbaar te maken gebruiken we het volgende model:

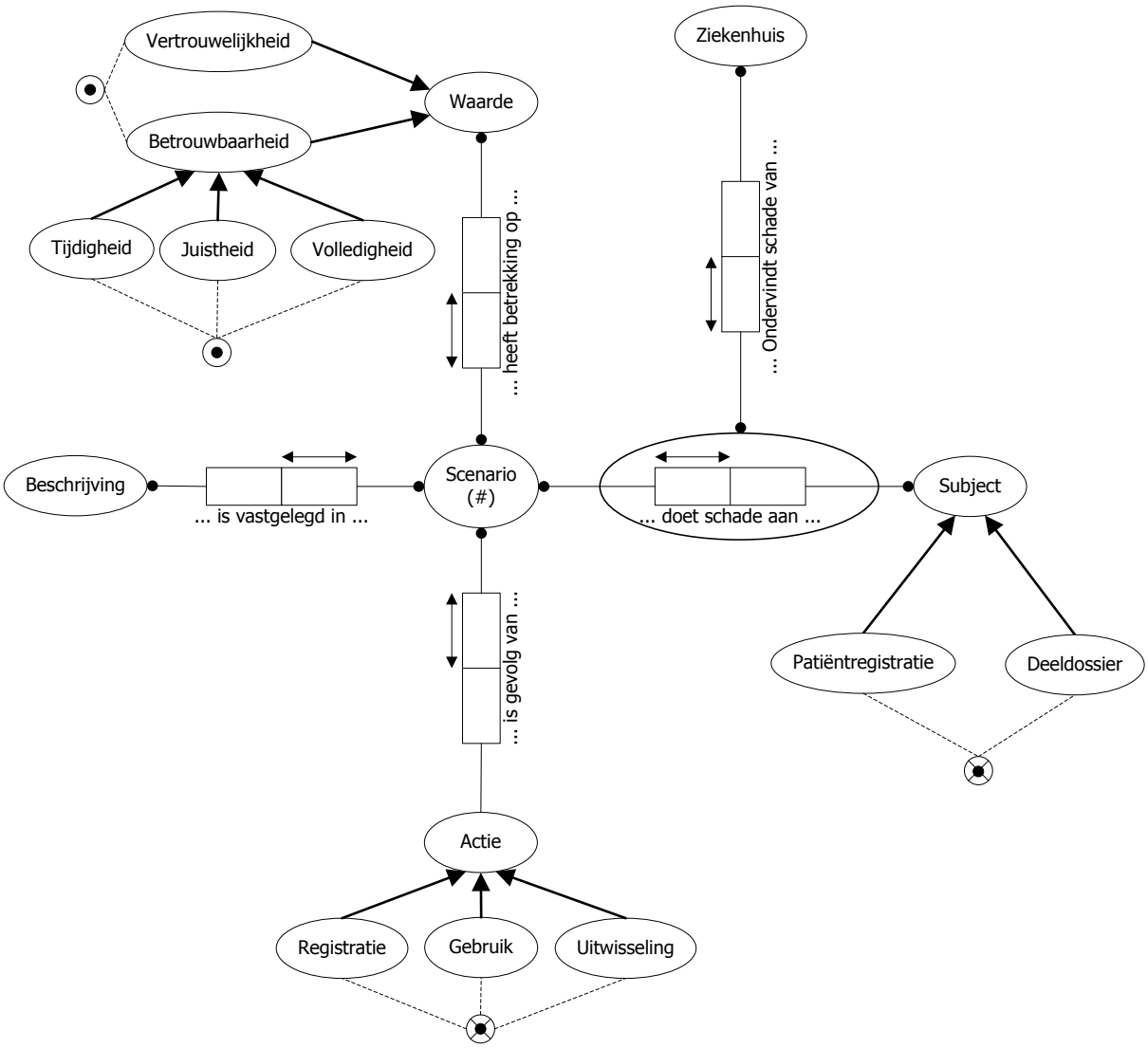


Diagram 4.1 (ORM-model) Modellering van het concept risico zoals toegepast in dit onderzoek.

4.2 Risicoscenario's

In deze *tweede paragraaf* beschrijven we de risicogroepen welke we kunnen abstraheren uit de uitgebreide risicoanalyse zoals opgenomen in *bijlage C*. Ieder risico wat hier is benoemd is op basis van de kern van het risico ondergebracht in een categorie. Deze categorieën vormen de risicogroepen.

Gegeven dat soortgelijke risico's zich in verschillende scenario's kunnen manifesteren modelleren we voor ieder risicogroep de gewenste domeinsituatie waar dit betrekking heeft op het risicogebied onder de aandacht. Het risico is dan ook iedere afwijking van deze situatie zoals beschreven in de uitgebreide risicoanalyse in de *bijlage C*.

4.2.1 'De gebruiker voert patiëntgegevens incorrect in, in de velden van het deelsysteem'

<u>Model</u>

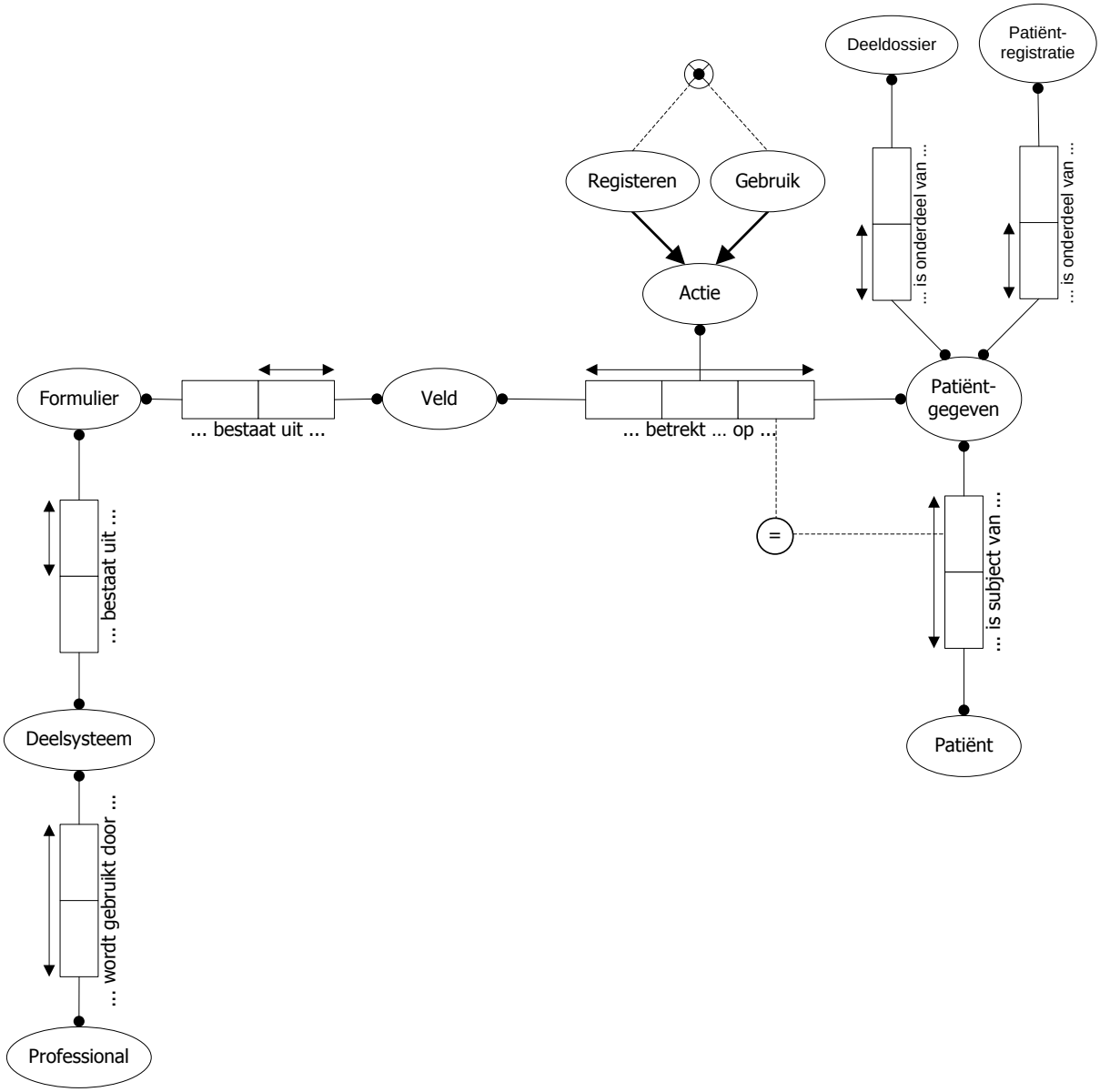


Diagram 4.1 (ORM-model) Risicogroep: 'De gebruiker voert patiëntgegevens incorrect in, in de velden van het deelsysteem'.

Kenmerken
Acties (direct): registratie, gebruik
Waarden (primair): juistheid
Subjecten: patiëntregistratie, deeldossier

4.2.2 'Benodigde patiëntgegevens zijn niet of onvolledig geregistreerd in deelsysteem'

Voor alle momenten waarop een patiëntgegeven geregistreerd dient te zijn in een deelsysteem dient te gelden:

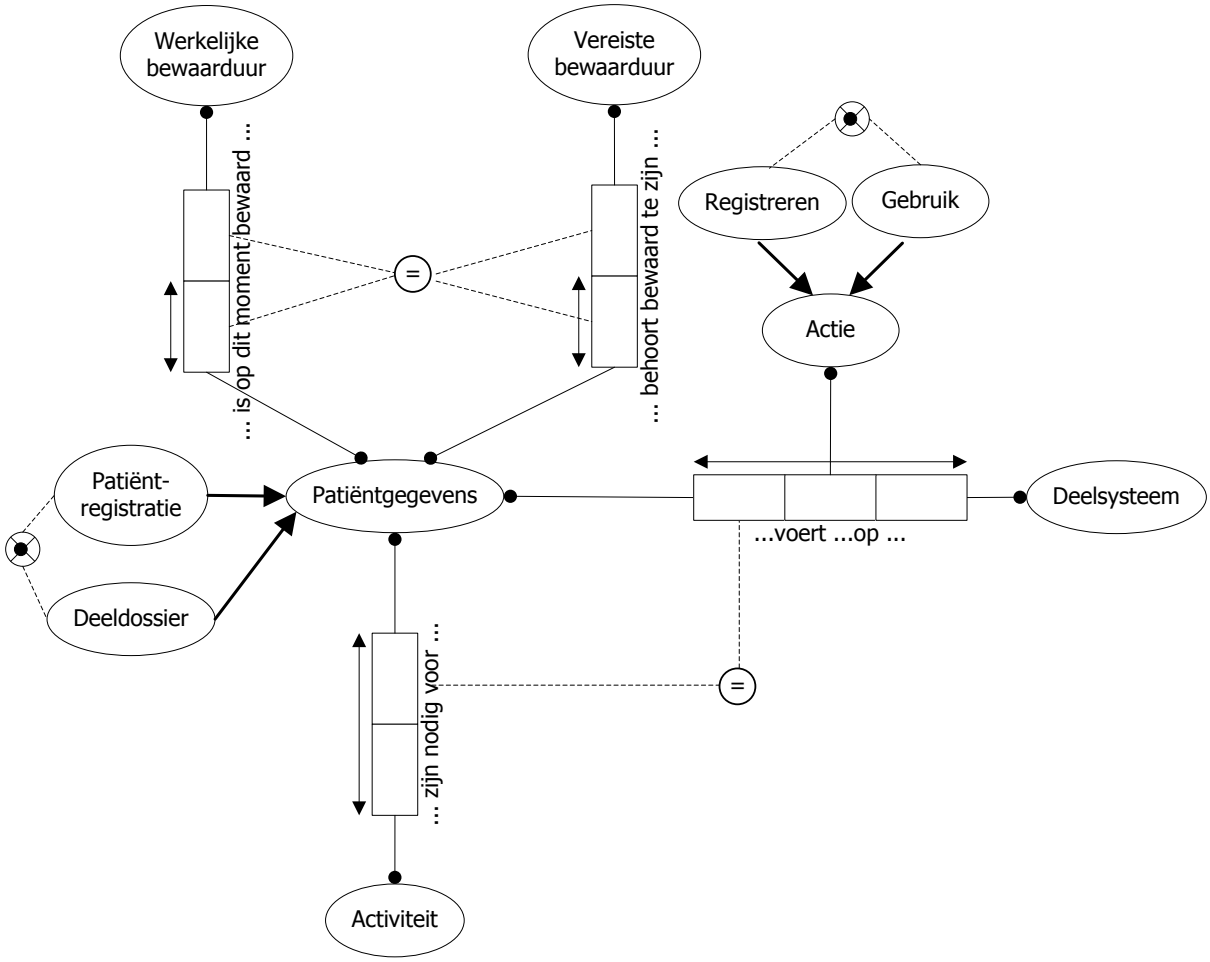


Diagram 4.2 (ORM-model) Risicogroep: 'Benodigde patiëntgegevens zijn niet of onvolledig geregistreerd in deelsysteem'.

Kenmerken

Acties (direct):	registratie, gebruik
Waarden (primair):	volledigheid
Subjecten:	patiëntregistratie, deeldossier

4.2.3 'Patiëntgegevens zijn niet (tijdig) beschikbaar voor niet-registrerende gebruikers'

Model

Voor alle momenten waarop een patiëntgegeven nodig is geldt:

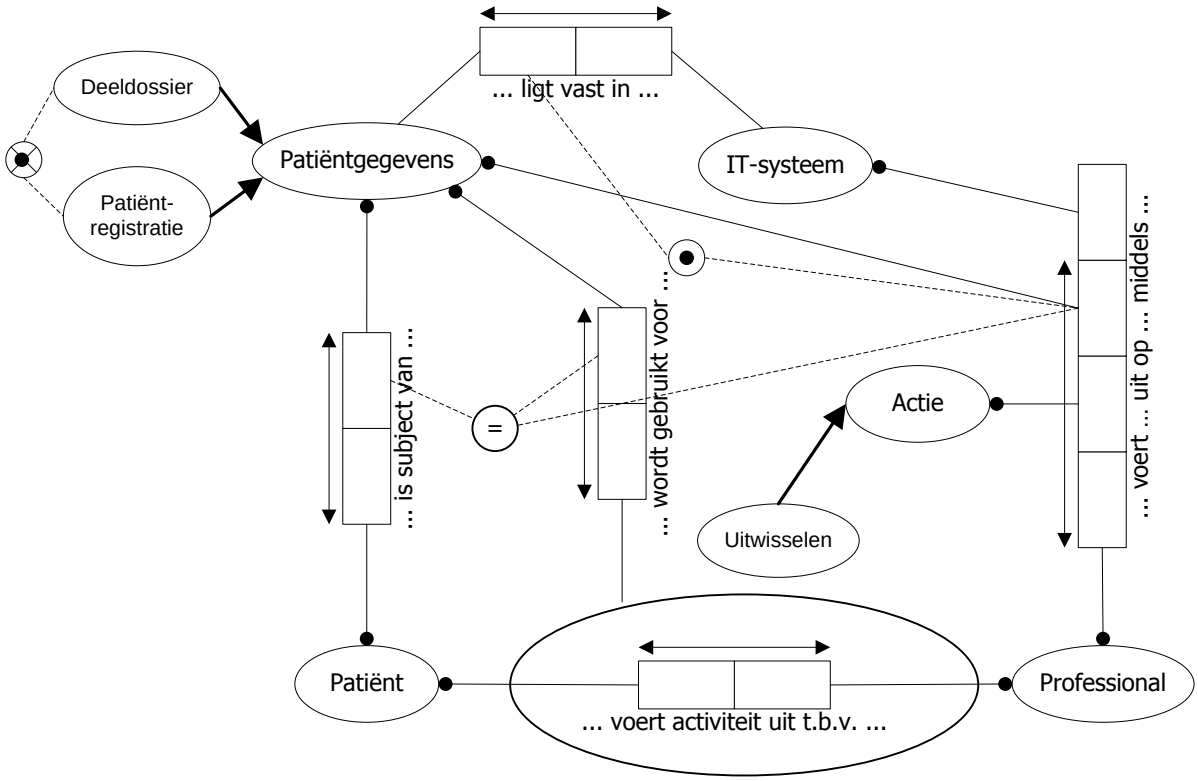


Diagram 4.3 (ORM-model) Risicogroep: 'Patiëntgegevens zijn niet (tijdig) beschikbaar voor andere professionals'.

Kenmerken

Acties (direct):	uitwisseling
Waarden (primair):	tijdigheid
Subjecten:	patiëntregistratie, deeldossier

4.2.4 'Gebruikers kunnen ongewenste acties uitvoeren op patiëntgegevens'

Model

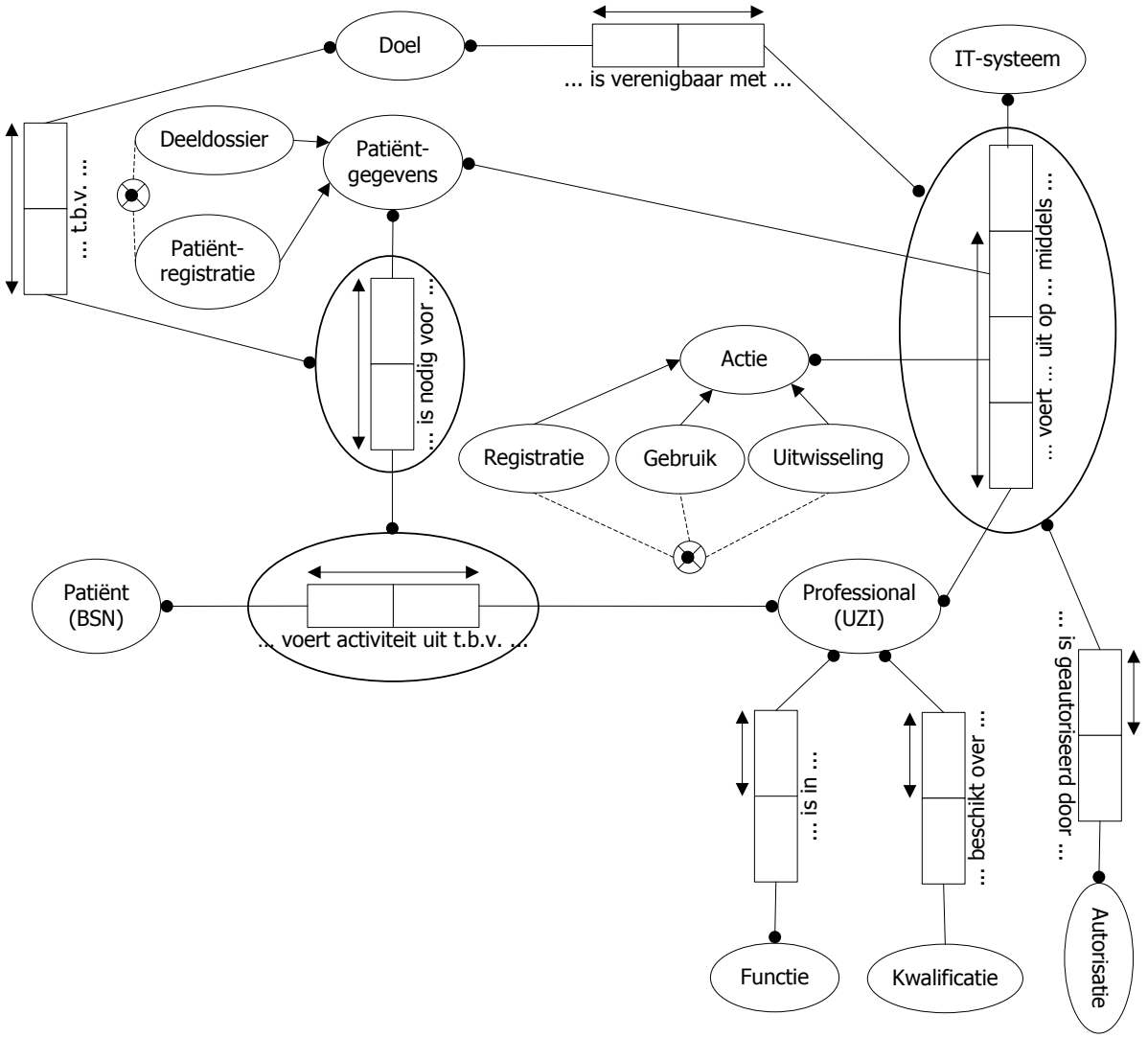


Diagram 4.4 (ORM-model) Risicogroep: 'Gebruikers kunnen ongewenste acties uitvoeren op patiëntgegevens'.

Kenmerken

Acties (direct):	registratie, gebruik, uitwisseling
Waarden (primair):	vertrouwelijkheid, juistheid
Subjecten:	patiëntregistratie, deeldossier

4.2.5 'Irrelevante patiëntgegevens zijn vastgelegd in deelsysteem'

Model

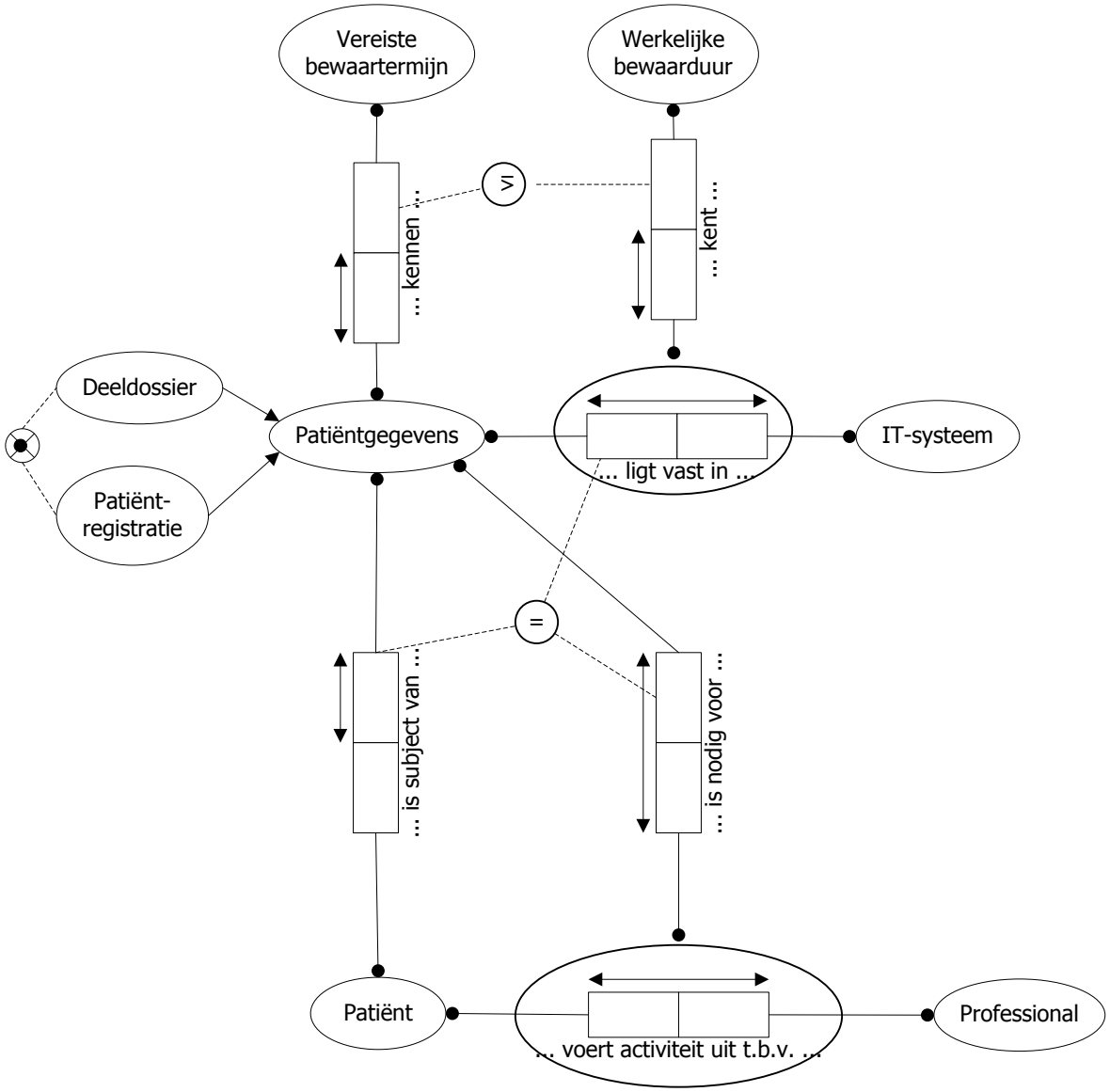


Diagram 4.5 (ORM-model) Risicogroep: 'Irrelevante patiëntgegevens zijn vastgelegd in deelsysteem'.

Kenmerken

Acties:	registratie, gebruik, uitwisseling
Waarden (primair):	volledigheid, juistheid
Subjecten:	patiëntregistratie, deeldossier

4.2.6 'Acties van gebruikers op patiëntgegevens zijn niet controleerbaar'

Model

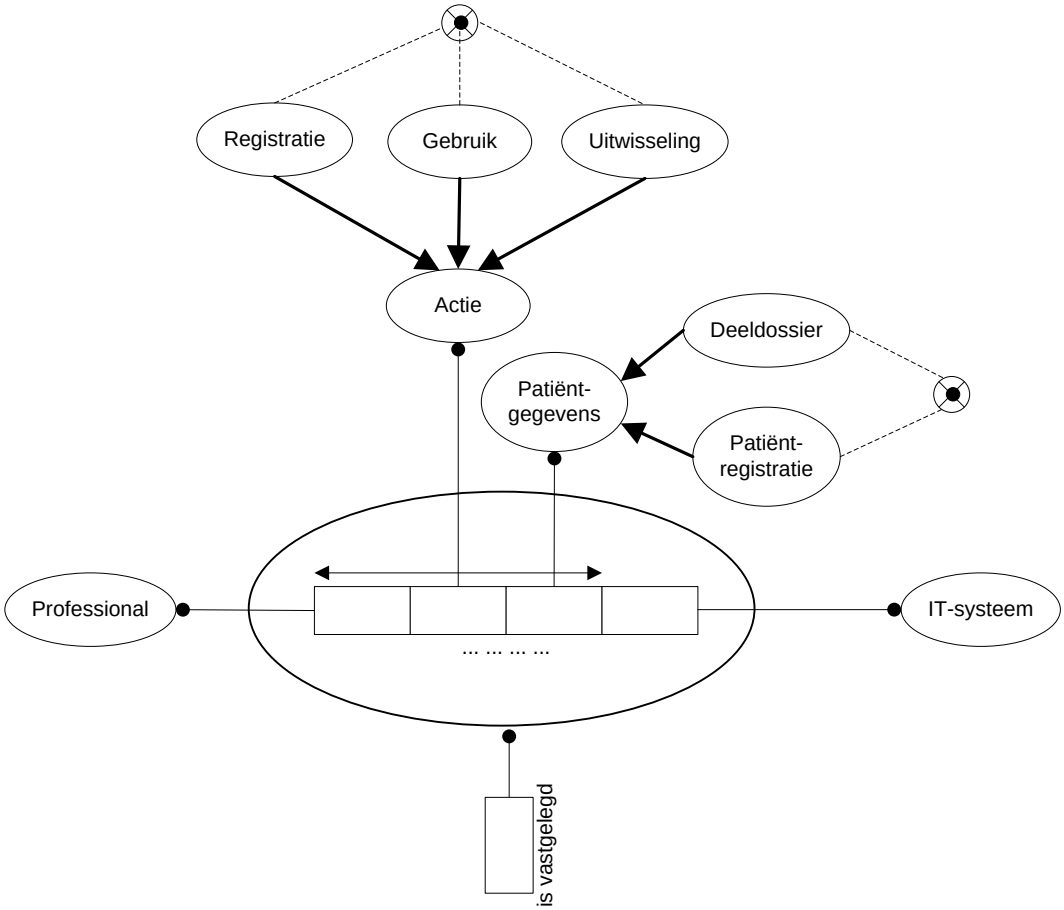


Diagram 4.6 (ORM-model) Risicogroep: 'Acties van gebruikers op patiëntgegevens zijn niet controleerbaar'.

Kenmerken

Acties:	registratie, gebruik, uitwisseling
Waarden (primair):	volledigheid, juistheid, vertrouwelijkheid, tijdigheid
Subjecten:	patiëntregistratie, deeldossier

4.2.7 'Patiëntgegevens zijn gekoppeld aan de verkeerde patiënt'

Model

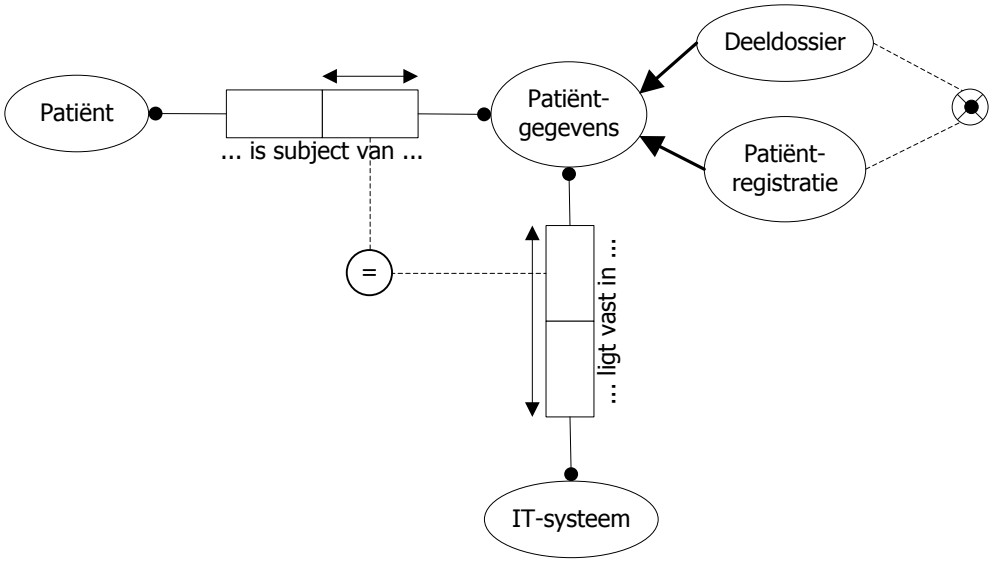


Diagram 4.7 (ORM-model) Risicogroep: 'Vastgelegde patiëntgegevens zijn gekoppeld aan de verkeerde patiënt'.

Kenmerken
Acties: registratie
Waarden (primair): juistheid
Subjecten: patiëntregistratie, deeldossier

4.2.8 'Patiëntgegevens zijn onvoldoende bruikbaar voor de niet-registrerend gebruiker'

Model

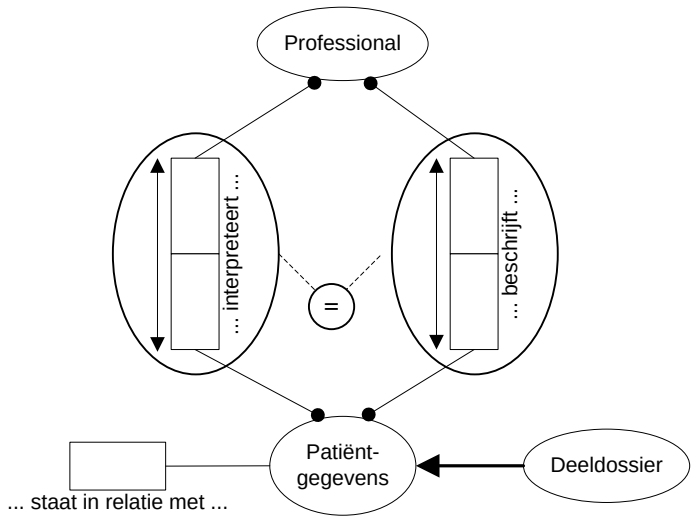


Diagram 4.8 (ORM-model) Risicogroep: 'Patiëntgegevens zijn onvoldoende bruikbaar voor de niet-registrerend gebruiker'.

Kenmerken
Acties: registratie
Waarden (primair): juistheid
Subjecten: deeldossier

4.2.9 'Actualiteit/bron van patiëntgegevens is onduidelijk voor de gebruiker'

Model

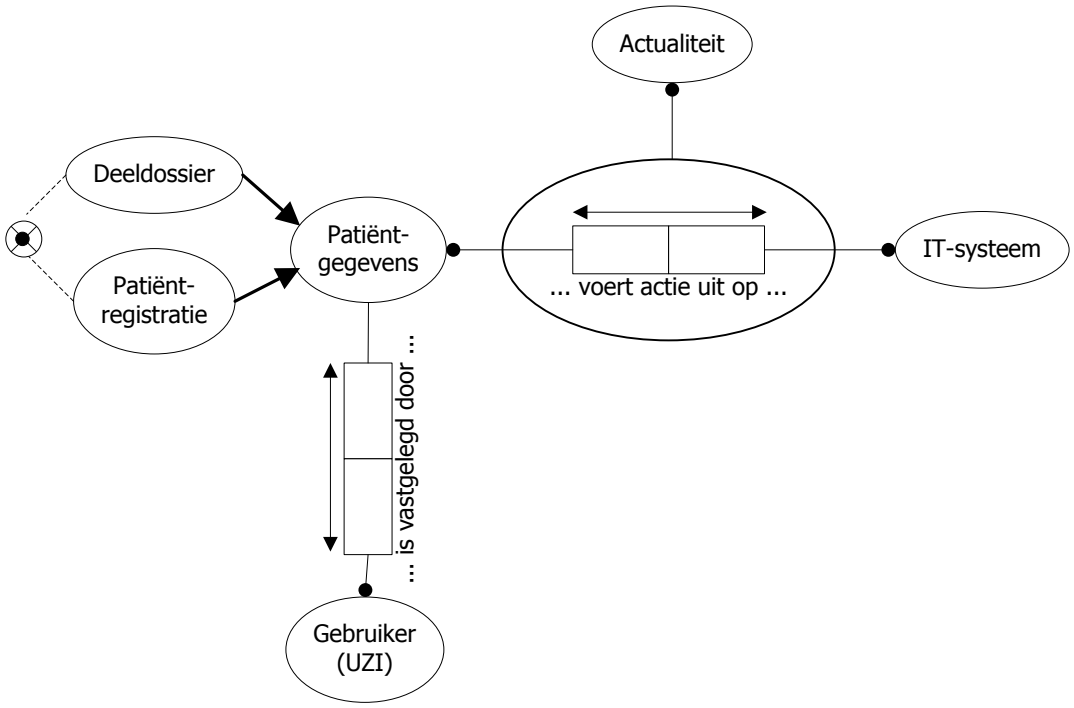


Diagram 4.9 (ORM-model) Risicogroep: 'Actualiteit/bron van patiëntgegevens is onduidelijk voor de gebruiker'.

Kenmerken

Acties:	gebruik, uitwisseling
Waarden (primair):	juistheid, volledigheid
Subjecten:	patiëntregistratie, deeldossier

4.2.10 'Deeldossiers zijn onvindbaar voor gebruiker'

Model

<<to do: invoegen bij afronding>>

Diagram 4.10 (ORM-model) Risicogroep: 'Deeldossiers zijn onvindbaar voor gebruiker'.

Kenmerken

Acties:	uitwisseling
Waarden (primair):	tijdigheid
Subjecten:	deeldossier

4.2.11 'Patiëntgegevens kunnen redundant worden geregistreerd / zijn vastgelegd in deelsysteem'

Model

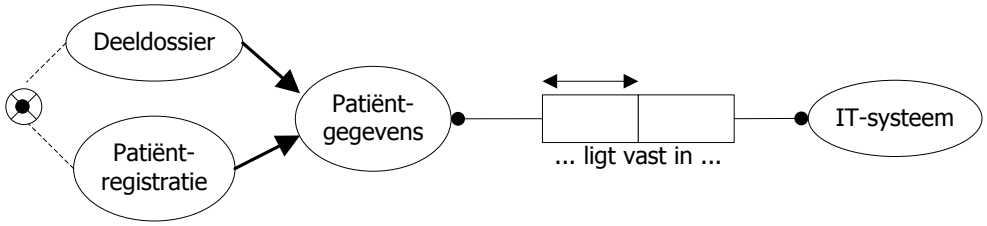


Diagram 4.11 (ORM-model) Risicogroep: 'Patiëntgegevens kunnen redundant worden geregistreerd / zijn vastgelegd in deelsysteem'.

Kenmerken
Acties: registratie, uitwisseling
Waarden (primair): juistheid, volledigheid
Subjecten: patiëntregistratie, deeldossier

4.2.12 'Patiëntgegevens zijn niet toegankelijk voor professional in geval van nood'

Model

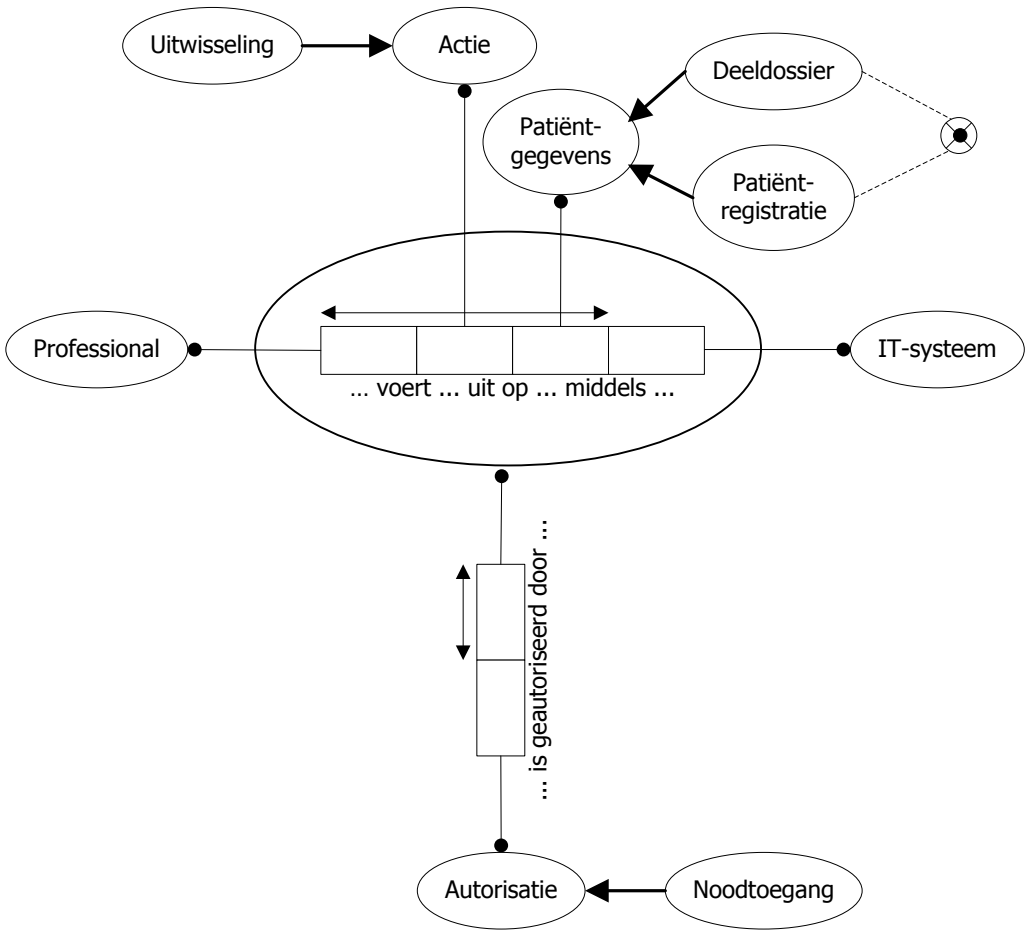
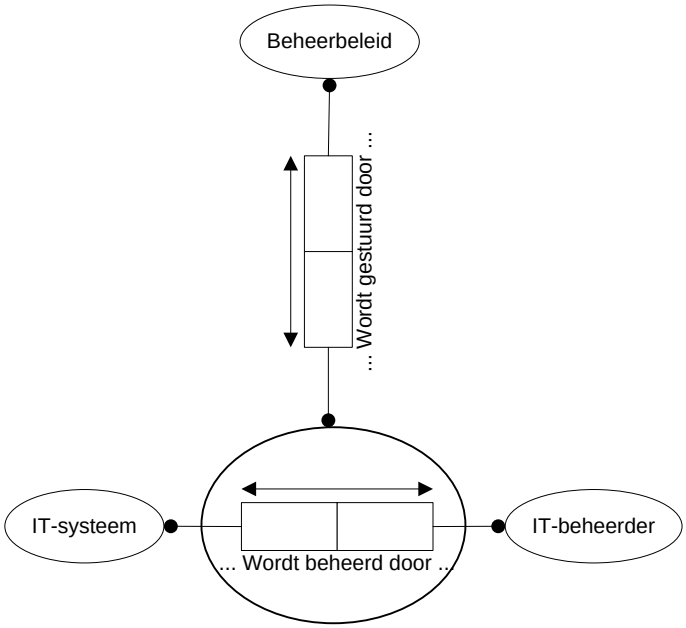


Diagram 4.12 (ORM-model) Risicogroep: 'Patiëntgegevens zijn niet toegankelijk voor professional in geval van nood'.

Kenmerken
Acties: uitwisseling
Waarden (primair): vertrouwelijkheid
Subjecten: patiëntregistratie, deeldossier

4.2.13 'Beheer van IT-systeem leidt tot problemen voor de vertrouwelijkheid en betrouwbaarheid van patiëntgegevens'

Model



Kenmerken

Acties:	n.v.t.
Waarden (primair):	vertrouwelijkheid, betrouwbaarheid
Subjecten:	patiëntregistratie, deeldossier

5 Beheersmaatregelen

In dit *vijfde hoofdstuk* leggen we de basis voor enkele maatregelen om de in *hoofdstuk 4* vastgelegde risicogroepen.

Om orde aan te brengen in de verschillende beheersmaatregelen worden ze gecategoriseerd naar de in *hoofdstuk 4* benoemde kernproblemen.

5.1 'De gebruiker voert patiëntgegevens incorrect in, in de velden van het deelsysteem' & 'Benodigde patiëntgegevens zijn niet of onvolledig geregistreerd in deelsysteem'

Professional voeren patiëntgegevens in en maken hierbij bewust of onbewust fouten. Soms verloopt de invoer via eenvoudige formulieren, soms gaat het om complexe deeldossiers waarbij het niet altijd wenselijk is (veel) structuur op te leggen aan de invoer van de zorgprofessional.

We kijken allereerst naar de meest eenvoudige categorie, de formulieren. Bijvoorbeeld wanneer de professional een patiënt registreert bij 'binnenkomst' in het ziekenhuis gebruikt hij of zij een formulier. De correctheid van de ingevoerde patiëntgegevens kan eenvoudig maar doeltreffend worden beheerst door een zorgvuldig opgebouwd formulier welke actief controles uitvoert op de invoer van de professional. Er moet daarvoor geïnventariseerd worden welke patiëntgegevens verplicht zijn en hoe het verwachte formaat (formaten) van deze patiëntgegevens eruit moet(en) zien. Tijdens de ontwikkeling van het deelsysteem dient de verworven kennis te worden meegenomen in de ontwikkeling van het formulier. Dit wordt geschetst in onderstaand formulier:

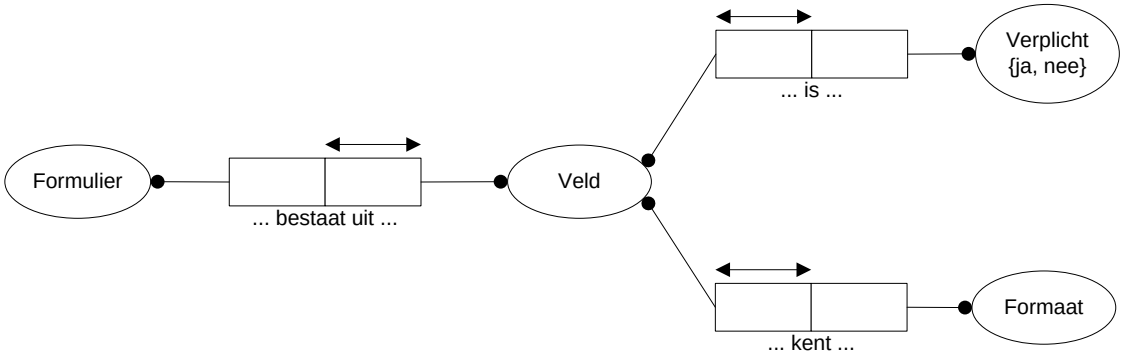


Diagram 5.1 (ORM-diagram) Beheersmaatregel voor eenvoudige invoerscenario: formulieren.

Resten ons de meer complexe invoerscenario's, deze treffen we met name aan als de zorgprofessional medische patiëntgegevens registreert in een deeldossier. Het is hierbij niet altijd wenselijk (veel) structuur op te leggen aan de zorgprofessional welke de patiëntgegevens vastlegt in het deeldossier. Om binnen deze flexibiliteit toch de invoer van patiëntgegevens te kunnen beheersen zou een regelgebaseerde aanpak kunnen worden gehanteerd. De regels leggen de randvoorwaarden vast waarbinnen de zorgprofessional zich kan gedragen. Dit garandeert de zorgprofessional flexibiliteit zonder wezenlijk toe te leggen op die voorwaarden welke belangrijk zijn voor de juistheid en volledigheid van de ingevoerde patiëntgegevens. Omdat een concrete toepassing hiervan meer onderzoek zou vereisen schetsen we hierbij in grove lijnen hoe een beheersmaatregel eruit zou kunnen zien:

De professional brengt zelf structuur aan door binnen de kaders van een vrij formaat enkele onderdelen te classificeren middels een label (dit zou kunnen worden afgedwongen door het deelsysteem). Om dit te bereiken zou het deelsysteem de zorgprofessional kunnen dwingen een bepaald scenario te selecteren, laten we zeggen een botbreuk. Aan een scenario zijn vooraf enkele

regels gekoppeld, bijvoorbeeld dat er tenminste één foto van het deeldossier gekoppeld is aan/deel uitmaakt van het deeldossier en dat tenminste de behandeling beschreven is. *Diagram 5.2* beschrijft deze oplossing:

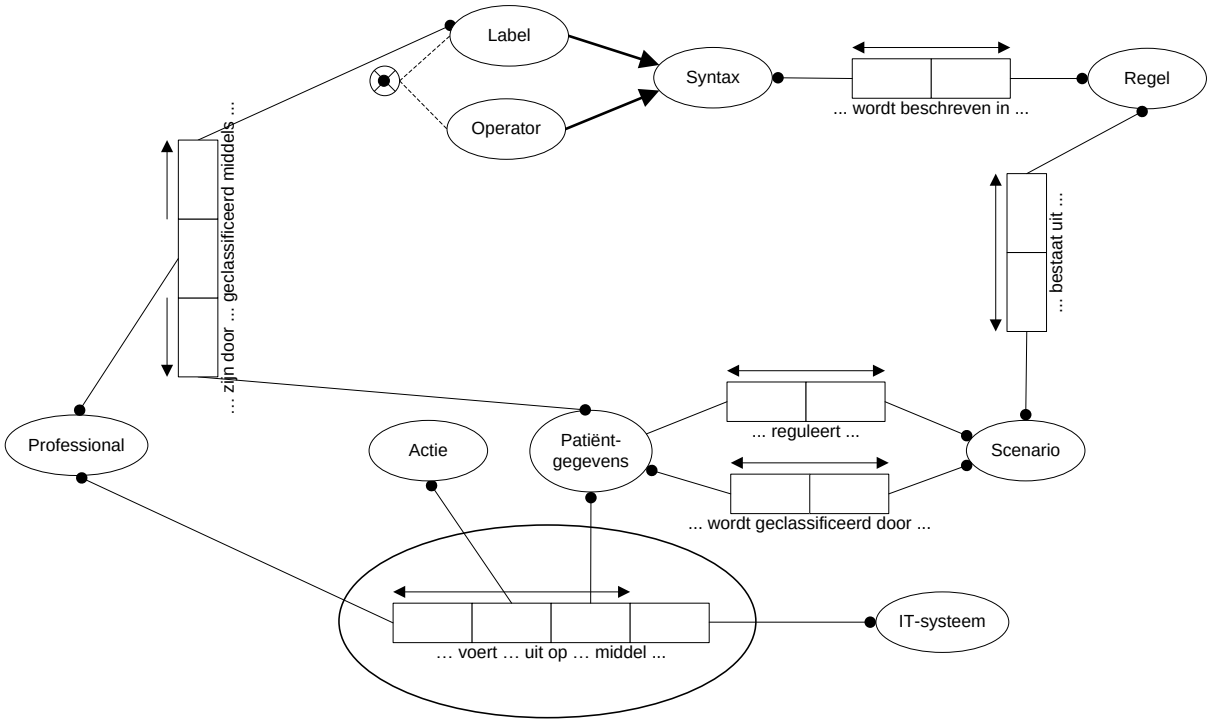


Diagram 5.2 (ORM-diagram) De toepassing van regels op vrij-formaat invoer in het deeldossier.

Doordat patiëntgegevens in het deeldossier met de toepassing van scenario en labels gecategoriseerd zijn zal het waarschijnlijk zelfs mogelijk zijn bepaalde meer geavanceerde controles los te laten op de invoer om dieper te kijken naar inhoudelijke aspecten, het deelsysteem kan nu immers 'snappen' wat er staat. Het is mogelijk deze oplossing te gebruiken in een simpele zowel als complexe toepassingen ervan. Bovendien zouden deze regels ook kunnen worden toegepast om de juistheid en volledigheid van de ingevoerde patiëntgegevens te controleren bij de verdere verwerking van de patiëntgegevens na invoer. Beheersing van de interne verwerking wordt vereist door NEN 7510.

Ook moet het mogelijk zijn patiëntgegevens waarvan wordt vermoedt dat deze onjuist of onvolledig zijn te markeren. Deze markeringen moeten ook inzichtelijk zijn voor die personen welke verantwoordelijk zijn voor deze patiëntgegevens of controles uitvoeren op de correctheid/volledigheid van deze patiëntgegevens.

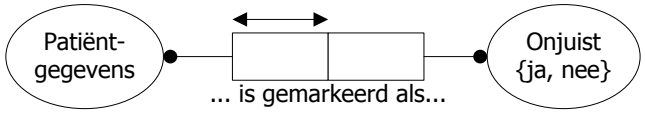


Diagram 5.3 (ORM-diagram) Markeren van vermoedelijk onjuiste of onvolledige patiëntgegevens.

Een opgevraagd BSN moet automatisch worden overgenomen om de kans op foute invoer te verkleinen.

Een patiëntverklaring moet direct kunnen worden toegevoegd door de patiënt, bijvoorbeeld middels een terminal welke de patiënt kan gebruiken om de eigen patiëntgegevens in te zien en patiëntverklaringen toe te voegen. Dit is de beste garantie dat een dergelijke verklaring aan het juiste deeldossier wordt gekoppeld.

Deeldossiers mogen enkel door de beheersverantwoordelijke specialist verwijderd worden. Wanneer dit binnen de wettelijke termijn gebeurd moet hiervoor een verklaring zijn van de patiënt waarvan een digitale kopie wordt opgeslagen door de beheersverantwoordelijke specialist. Om de privacy van de patiënt te beschermen mag deze kopie enkel toegankelijk zijn voor deze specialist en de patiënt. De wettelijke bewaarduur van patiëntgegevens kan worden vastgelegd bij registratie door het deelsysteem de patiëntgegevens direct onder te brengen in een categorie. Zo kan het deelsysteem erop toezien dat patiëntgegevens niet worden verwijderd binnen de gewenste bewaarduur. Als de patiënt wenst dat deeldossiers langer worden bewaard kan de beheerverantwoordelijke specialist de bewaarduur van de patiëntgegevens ophogen.

Het belang van handmatige beheersmaatregelen moet niet worden onderschat. Bijvoorbeeld de hoofdbehandelaar of IC-medewerker zou steekproefsgewijs kunnen controleren of patiëntgegevens zorgvuldig zijn vastgelegd. Indien dit niet het geval is kan de professional welke de patiëntgegevens heeft ingevoerd hierop worden aangesproken.

Ook zijn heldere en correcte procedures en training van belang en kunnen korte checklists handig zijn om de correctheid en volledigheid van ingevoerde patiëntgegevens te optimaliseren.

Ook NEN 7510 geeft een hint voor een goede beheersmaatregel, hoewel deze niet specifiek bedoeld is voor dit scenario. Het ziekenhuis zou een professional welke dicht op de betreffende activiteit zit kunnen aanstellen als verantwoordelijke. Deze kan vervolgens bepalen welke patiëntgegevens noodzakelijk zijn en wat te verwachten is waar het gaat om het formaat van de invoer. Voor iedereen dient duidelijk te zijn wie deze verantwoordelijke is voor de betreffende patiëntgegevens zodat deze persoon duidelijk aanspreekbaar is en terugkoppeling moet plaatsvinden via een gestructureerd proces zodat de taak structureel wordt uitgevoerd. Deze persoon zou binnen zijn of haar afdeling ook kunnen toezien op de juistheid van de patiëntgegevensregistratie.

In sommige scenario's kan het helpen de correctheid direct te verifiëren middels een Wettelijk Identificatie Document zoals bij de patiëntregistratie. Ook kan er een kopie van het identificatie document worden toegevoegd om later de correctheid van de patiëntregistratie te kunnen controleren. De correctheid van een afspraak kan worden beheerst door de afspraak af te stemmen met de patiënt, direct of per telefoon en/of brief.

Middels actieve geautomatiseerde controles kan het deelsysteem erop toezien dat de professional alle noodzakelijke patiëntgegevens vastlegt. Er is echter geen eenvoudige geautomatiseerde beheersmaatregel denkbaar welke het ziekenhuis met voldoende zekerheid kan garanderen dat ook die patiëntgegevens geregistreerd worden in het formulier welke in andere activiteiten nodig zijn en/of noodzakelijk zijn voor de uitvoer van de betreffende activiteit. Het ziekenhuis dient dan ook een proces in te richten om na te gaan hoe processen in elkaar steken en welke gegevensbehoeften hierbij spelen. Deze kennis moet vervolgens worden vertaald naar een formulier. Ook hierbij zou men een professional uit het deeldomein kunnen aanstellen, deze moet dan in kaart brengen welke informatiebehoeften er spelen in dat deeldomein. Een getrainde modelleur kan hierbij helpen.

5.2 'Patiëntgegevens zijn niet (tijdig) beschikbaar voor niet-registrerende gebruikers'

Principes uit workflow management en business rules bieden mogelijkheden om processen te sturen en hierdoor in het ziekenhuis een tijdige beschikbaarheid van patiëntgegevens te beheersen. Het is waarschijnlijk onwenselijk beide concepten volledig toe te passen in dit probleemgebied. Beiden vereisen dat vooraf bepaalde kennis aanwezig is over het (wenselijke verloop van een) proces en met name workflow management kan de flexibiliteit van het proces beperken. Toch zijn er interessante mogelijkheden om enkele ideeën uit beiden concepten toe te passen op het ziekenhuisdomein. Een voorbeeld ter illustratie van de mogelijkheden:

Hoofdbehandelaar x krijgt een nieuwe patiënt. Voor de diagnostiek moeten een tweetal onderzoeken worden uitgevoerd door twee ondersteunend specialisten. De hoofdbehandelaar kan zijn taken pas

hervatten als beiden taken van de ondersteunend specialisten zijn afgerond. De hoofdbehandelaar registreert dat er twee taken moeten worden uitgevoerd door specialist y en z, legt de verwachte uitvoer van patiëntgegevens vast middels bijvoorbeeld een identificatiecode (waarmee de ondersteunend specialisten de resultaten terugkoppelen) en geeft tenslotte aan het systeem door dat hij of zij gewaarschuwd moet worden wanneer beiden taken uitgevoerd zijn, oftewel wanneer de resulterende patiëntgegevens teruggekoppeld zijn.

Combineren we de workflow management-georiënteerde aanpak uit het voorbeeld met regels dan kunnen we een stap verder gaan. Zo zou de hoofdbehandelaar uit het voorbeeld kunnen eisen dat beiden taken af zijn binnen 14 dagen en dat de specialisten in ieder geval gegevens a en b opleveren (in combinatie met de oplossing gepresenteerd in *diagram 5.2*).

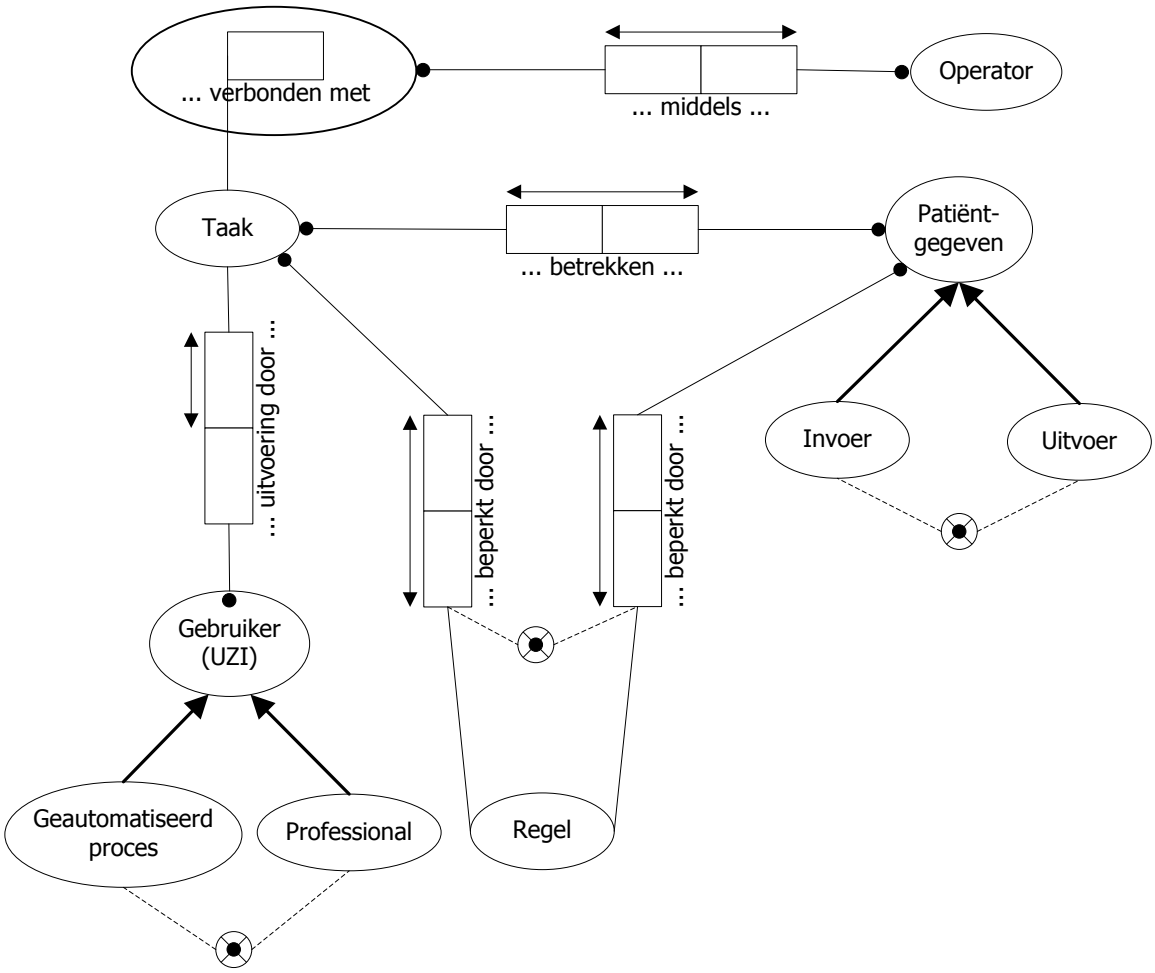


Diagram 5.4 (ORM-diagram) Een toepassing van workflow en business rules-georiënteerde technieken voor beheersing van tijdig beschikbare patiëntgegevens.

Bovendien zouden middels de 'workflow-aanpak' ook enkele noodzakelijkheden kunnen worden afgedwongen. Zo kan de zorgprofessional na registratie van medische patiëntgegevens in het deeldossier er op worden gewezen dat hij of zij het deeldossier dient aan te melden zodat deze kunnen worden uitgewisseld en kan de professional welke de patiënt registreert erop worden gewezen er zorg voor te dragen dat het BSN van de patiënt wordt opgevraagd.

Ook hier zou het NEN-7510 idee van een 'gegevensverantwoordelijk professional' kunnen worden toegepast. Deze gebruiker is actief in het domein en weet wanneer welke patiëntgegevens wanneer nodig zijn. Ook andere gebruikers binnen dit deeldomein kunnen deze gebruiker hier op aanspreken. Deze professional kan dan andere in het ziekenhuis aanspreken welke verantwoordelijk zijn voor procesinrichting en/of informatievoorziening.

Waar het lastig is de hiervoor gepresenteerde 'workflow-oplossing' bepaalde stappen af te laten dwingen kan een eenvoudige checklist en heldere, bij professionals bekende procedures en richtlijnen helpen om patiëntgegevens tijdig beschikbaar te krijgen.

5.3 'Gebruikers kunnen ongewenste acties uitvoeren op patiëntgegevens'

Naast de hieronder gepresenteerde beheersmaatregelen is het wenselijk te onderzoeken wat de mogelijkheden zijn om, waar mogelijk, de patiënt om toestemming te vragen dat een zekere gebruiker bepaalde acties op bepaalde patiëntgegevens mag uitvoeren. Hiermee krijgt het ziekenhuis grote zekerheid over de vraag of men handelt naar de wensen van de patiënt. Toch is dit geen eenvoudige opgave omdat een dergelijke beheersmaatregel al snel tegen zekere beperkingen oploopt. Zo is het onwaarschijnlijk dat de patiënt over voldoende achtergrondkennis beschikt om een grondige afweging te maken, kan goede voorlichting wel erg veel vragen van het ziekenhuis en is het onwaarschijnlijk dat men kan volstaan met een korte toelichting om de complexiteit van het probleem voldoende te doorgronden. En wat moet men doen als de wensen van de patiënt de behandeling sterk frustreert en zowel ziekenhuis als patiënt hier (ernstige) nadelen van ondervinden? Complexe vragen die niet binnen dit onderzoek kunnen worden beantwoord.

5.3.1 Mandateringen

De vastlegging van mandateringen mag niet leiden tot een grote toename van de werkdruk van de zorgprofessional, dit zou tot fouten kunnen leiden welke impact kunnen hebben op vertrouwelijkheid en/of betrouwbaarheid. We kiezen daarom voor een flexibele oplossing welke het werk minimaliseert:

- Een 'statisch' gedeelte.

  De relaties van een specialist met een team van ondersteunende (zorg)professionals binnen het ziekenhuis waar hij of zij een zeker beroep uitoefent zijn doorgaans relatief constant en kunnen dus onafhankelijk van een specifieke patiënt met een zekere klacht in kaart worden gebracht. De ondersteunend professional heeft in deze samenwerking een zekere rol. Op basis van deze rol zouden bepaalde mandateringen, oftewel een pakket aan regels zoals uitgewerkt in *paragraaf 5.4.2*, kunnen worden verstrekt welke passen bij de werkrelatie tussen de specialist en de te mandateren professional.

- Een 'dynamisch' gedeelte.

  De keuze voor een ondersteunend specialist, met de professionals welke hem of haar ondersteunen, is afhankelijk van de patiënt en klacht. Deze relatie kan dus niet onafhankelijk van de patiënt in kaart worden gebracht. De specialist dient aan te geven dat er bij de behandeling van de betreffende patiënt een relatie bestaat tussen hem of haar en de betreffende zorgprofessional, op basis hiervan kunnen dus bepaalde mandateringen, oftewel regels, worden vastgelegd.

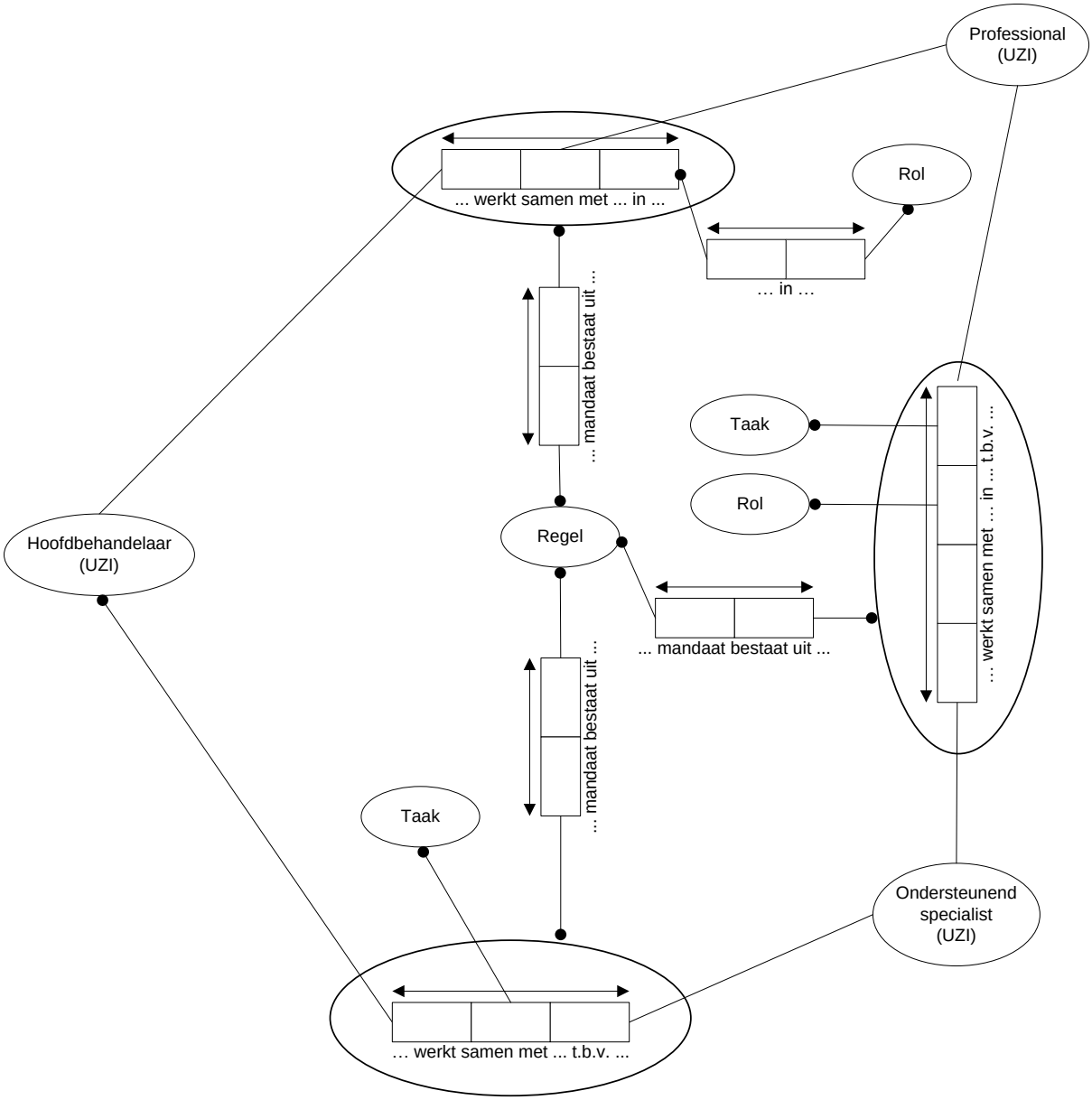


Diagram 5.5 (ORM-diagram) Conceptuele weergave van een maatregel om de verstrekking van mandateringen te beheersen.

Om de werklast voor de specialist te minimaliseren kan ervoor worden gekozen deze taak neer te leggen bij een beheerder welke deze (statische relaties) in kaart brengt. Een specialist moet dan natuurlijk nog wel instemmen met deze relaties, hij of zij blijft immers verantwoordelijk voor via deze weg verstrekte mandaten.

Ook zou het deelsysteem kunnen toezien op onverachte patronen middels deze beheersmaatregel. Zo is het onwaarschijnlijk dat een secretarieel medewerker welke enkel actief is op afdeling x mandateringen ontvangt van een specialist welke enkel actief is op afdeling y. Het deelsysteem kan hier de zorgprofessional welke het mandaat wenst te verstrekken op wijzen.

5.3.2 Reguleren van acties op patiëntgegevens

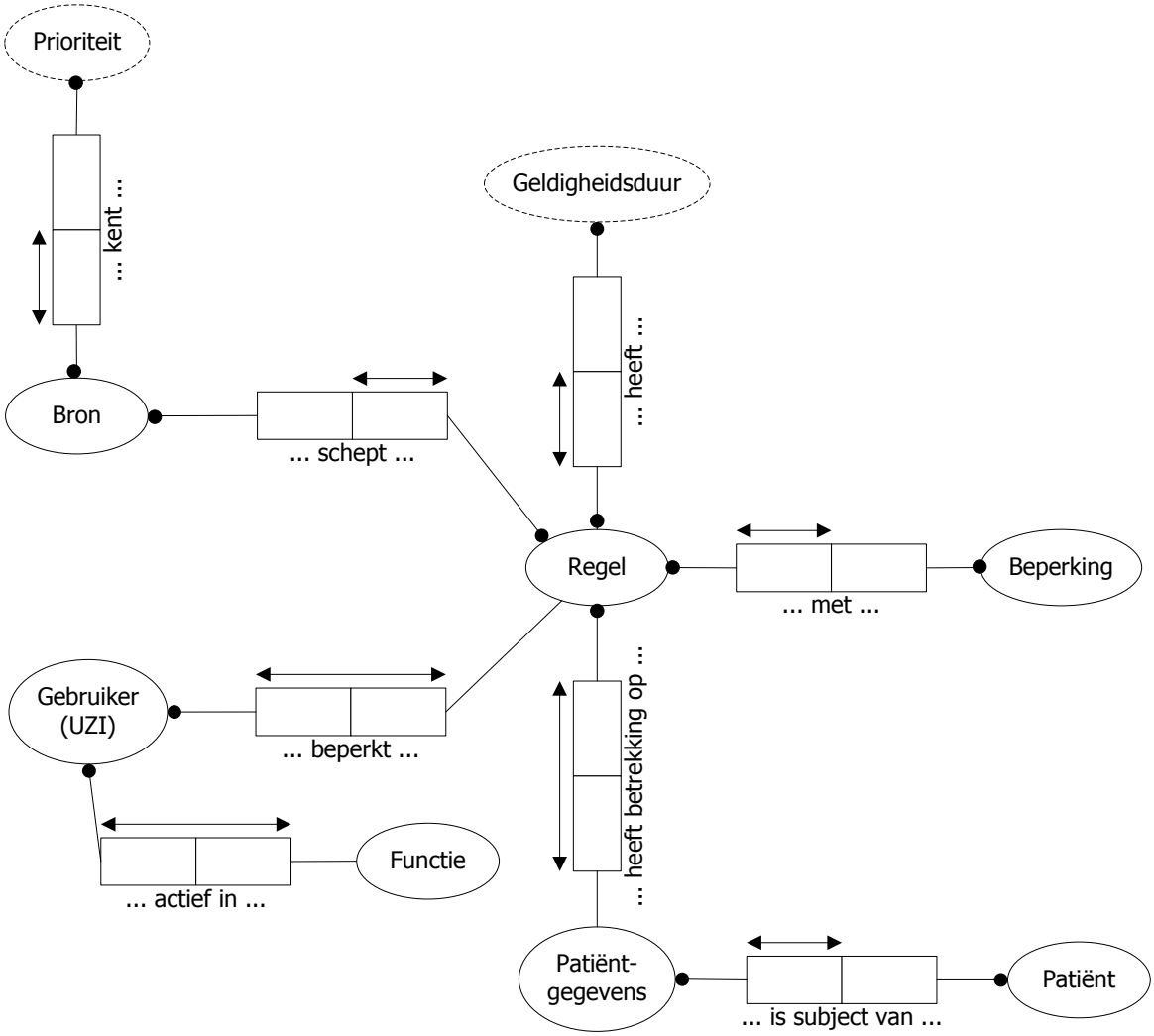


Diagram 5.6 (ORM-diagram) Regels om het gedrag van gebruikers van patiëntgegevens te beheersen.

Middels regels kunnen we het gedrag van gebruikers sturen. Ze kunnen op een flexibele wijze er voor zorgen dat het ziekenhuis voldoet aan wet- en regelgeving en interne en/of externe normen.

Een regel kan betrekking hebben op één of meerdere patiënten (dit kunnen ook alle patiënten zijn of alle patiënten die voldoen aan bepaalde eigenschappen). Bovendien kunnen ze betrekking hebben op één of meerdere gebruikers (ook hier geldt dat een regel betrekking kan hebben op alle gebruikers of alle gebruikers die voldoen aan bepaalde eigenschappen). Deze regels kunnen bovendien gelden voor iedere gebruiker welke een bepaalde functie uitoefent.

Een regel heeft altijd betrekking op een zekere verzameling van patiëntgegevens, de autorisaties hebben immers hierop betrekking.

Ook de bron van de regel moet vastliggen. Zo is het bijvoorbeeld duidelijk dat wet- en regelgeving altijd geldt. Echter soms kunnen regels tegenstrijdig zijn. Wanneer een regel van het ziekenhuis strijdig is met de regel welke voortkomt uit wet- en regelgeving moet deze voorrang krijgen op die van het ziekenhuis.

Een regel kan gekoppeld worden aan een geldigheidsduur, bijvoorbeeld wanneer we een bepaalde gebruiker slechts voor een bepaalde tijdsduur toegang willen verstrekken tot de patiëntgegevens van een zekere patiënt.

Ten slotte moet ook de beperking zelf beschreven worden. Het exacte formaat laten we hierbij in het midden, aanvullend onderzoek zou hier een antwoord op kunnen geven.

Merk overigens op dat deze beheersmaatregel niet kan functioneren wanneer een goede basis ontbreekt. Een goede basis betekend in deze dat het ziekenhuis inzicht moet hebben in welke functies welke acties moeten kunnen uitvoeren op welke gegevensgroepen. Dit betekend dat men moet beschikken over een competentie- en autorisatiematrix en inzicht moet hebben in de verschillende gegevensgroepen.

Middels deze beheersmaatregelen kunnen ook bezwaren van patiënten tegen bepaald secundair gebruik van bepaalde patiëntgegevens worden vastgelegd en afgedwongen.

Ook NEN 7510 veronderstelt dat gebruikers gereguleerd worden middels bepaalde 'regels en rechten'.

5.3.3 Beperking op het doel van het proces

Om de doelen waarvoor patiëntgegevens worden gebruikt te beheersen is het mogelijk patiëntgegevens te voorzien van een classificerende code. Het deelsysteem moet hiervoor bij registratie vastleggen om wat voor type patiëntgegevens het gaat. Per proces zou het ziekenhuis vervolgens kunnen vastleggen welke klassen van patiëntgegevens gebruikt mogen worden door het proces. Het is hierbij aan te raden gebruik te maken van gelaagde codes (bijvoorbeeld naam binnen de klasse persoonsgegevens) om het gebruik van de codes te vergemakkelijken. Dit maakt het heel inzichtelijk welke patiëntgegevens worden gebruikt voor welke doelen en vergemakkelijkt dus het toezicht. Bij geautomatiseerde activiteiten binnen het proces kan dit zelf geautomatiseerd worden afgedwongen.

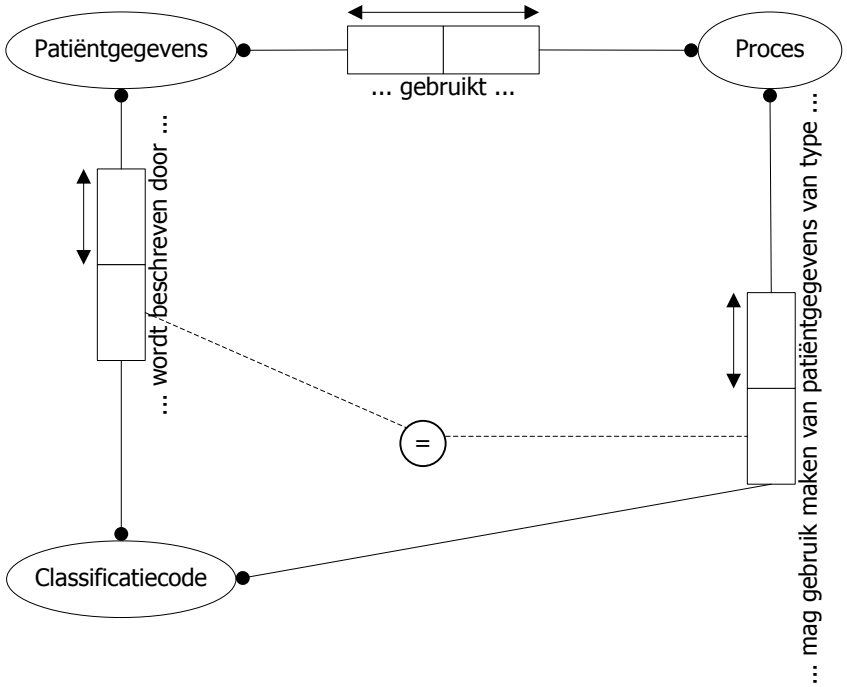


Diagram 5.7 (ORM-diagram) Middels classificatie van patiëntgegevens het gebruik van deze gegevens beheersen.

5.3.4 Lekken

Ten slotte bestaat er ook de mogelijkheid dat professionals welke toegang hebben tot patiëntgegevens deze lekken aan derden welke geen rol hebben binnen de behandeling of de patiëntgegevens mogen gebruiken voor een secundair doel.

NEN 7510 biedt enkele mogelijkheden om dit tegen te gaan welke we puntsgewijs zullen aanstippen:

- Beveiligingseisen opnemen in het functieprofiel.
- Informatiebeveiliging als onderwerp in het functioneringsgesprek.
- Screening van potentiële nieuwe medewerkers.
- Rechten en plichten ten aanzien van gegevensbescherming opnemen in het arbeidscontract.
- Zwijgplicht en geheimhoudingsplicht in het arbeidscontract.
- Professionals voorlichting over richtlijnen en stimuleren deze toe te passen.
- Proces bij vertrek van de medewerker (o.a. afsluitingsgesprek).
- Het vastleggen van sancties.

5.3.5 Overige

- Het kan belangrijk zijn patiëntgegevens zo te kunnen anonimiseren en/of aggregateren dat deze niet herleidbaar zijn tot individuele patiënten, dit maakt het altijd mogelijk de gegevens te gebruiken voor secundair gebruik.
- Voor beheerders van IT-systemen moeten speciale maatregelen worden genomen om te voorkomen dat zei acties (lezen, schrijven, verwijderen) kunnen uitvoeren op patiëntgegevens.

5.4 'Irrelevante patiëntgegevens zijn vastgelegd in deelsysteem'

Er is geen eenvoudig toepasbare geautomatiseerde beheersmaatregel denkbaar (uitgezonderd het scenario dat patiëntgegevens langer als wenselijk zijn vastgelegd in een IT-systeem) welke kan voorkomen dat patiëntgegevens welke niet noodzakelijk zijn voor de uitvoer van een activiteit, of patiëntgegevens waarvoor een alternatief voorhanden is welke ook geregistreerd kan worden, worden geregistreerd door een professional. Dit kan enkel worden voorkomen door training, heldere richtlijnen en steekproeven. Ook moet er een zeker bewustzijn worden gecreëerd onder de professionals welke de patiëntgegevens vastleggen dat patiëntgegevens niet zonder valide gebruiksdoel dienen te worden geregistreerd.

Om te voorkomen dat patiëntgegevens langer zijn vastgelegd in een IT-systeem als vereist door wet- en regelgeving of gevraagd door de patiënt, kan een beheersmaatregel worden toegepast welke eerder in *dit hoofdstuk* is gebruikt om te voorkomen dat deze gegevens 'voortijdig' verwijderd worden. Het classificeren van patiëntgegevens kan het voor het deelsysteem mogelijk maken de verantwoordelijke actoren te wijzen op patiëntgegevens welke langer als wenselijk worden vastgelegd. Vervolgens kan deze actor actie ondernemen om al dan niet de patiëntgegevens te verwijderen. De beheerverantwoordelijk specialist dient patiëntgegevens welke de patiënt wenst te verwijderen te verwijderen.

Ook moeten er beperkingen worden opgelegd aan de duur waaraan kopieën van patiëntgegevens kunnen worden bewaard als deze zijn uitgewisseld.

5.5 'Acties van gebruikers op patiëntgegevens zijn niet controleerbaar'

Het log is een van de belangrijkste reactieve middelen in het toezicht op het gebruik van patiëntgegevens. Het heeft tot doel te registreren wie wanneer wat heeft gedaan met patiëntgegevens. Het helpt hiermee zowel vertrouwelijkheid als betrouwbaarheid van patiëntgegevens te verhogen.

We leggen in het log de volgende zaken vast:

- Wie doet wat, wanneer met welke gegevens.

  Wil de controlerende professional/patiënt kunnen beoordelen of incorrect gehandeld is en wie of wat de bron is van een mogelijke fout dan dient er een verwijzing te zijn naar een zekere gebruiker. Om te bepalen welke patiëntgegevens mogelijk in gevaar zijn gekomen door fout handelen is ook een referentie naar patiëntgegevens, dus patiënt, noodzakelijk. Dit veronderstelt wel dat de actie gelukt is, maar het zou ook kunnen zijn dat de actie geweigerd is. Ook dit gegeven moet dus worden opgeslagen. Ook kunnen de gegevens mogelijk nodig zijn om te bepalen of er fout gehandeld is. Willen de registraties in het log van werkelijk nut zijn dan is het ook noodzakelijk informatie te hebben over wanneer de geregistreerde acties hebben plaatsgevonden, dit maakt het mogelijk patronen te herkennen en de falend professional te kunnen aanspreken op zijn of haar gedrag op een geloofwaardige wijze.

- Welke relatie bestaat er tussen degene die de actie wil uitvoeren en de patiënt wiens gegevens het betreft.

  De relatie tussen deze partijen geeft een belangrijke indicatie van wat geoorloofd is. Is er geen sprake van een behandelrelatie dan is het twijfelachtig als bijvoorbeeld een specialist patiëntgegevens heeft kunnen inzien, bewerken of verwijderen. Een referentie aan de gebruiker is dus noodzakelijk.

- Is er gehandeld in een noodsituatie.

  Een noodsituatie kan aanleiding vormen reguliere beheersmaatregelen niet toe te passen.

- Welke deelsystemen zijn gebruikt.

  Omdat bij het handelen van de gebruiker ook een deelsysteem ongewenst toegang kan hebben verkregen tot patiëntgegevens en dus mogelijk bijvoorbeeld ongewenst een kopie van een deeldossier bevat is het wenselijk een referentie op te nemen naar deelsysteem dat betrokken is geweest bij het uitvoeren van de actie op de patiëntgegevens.

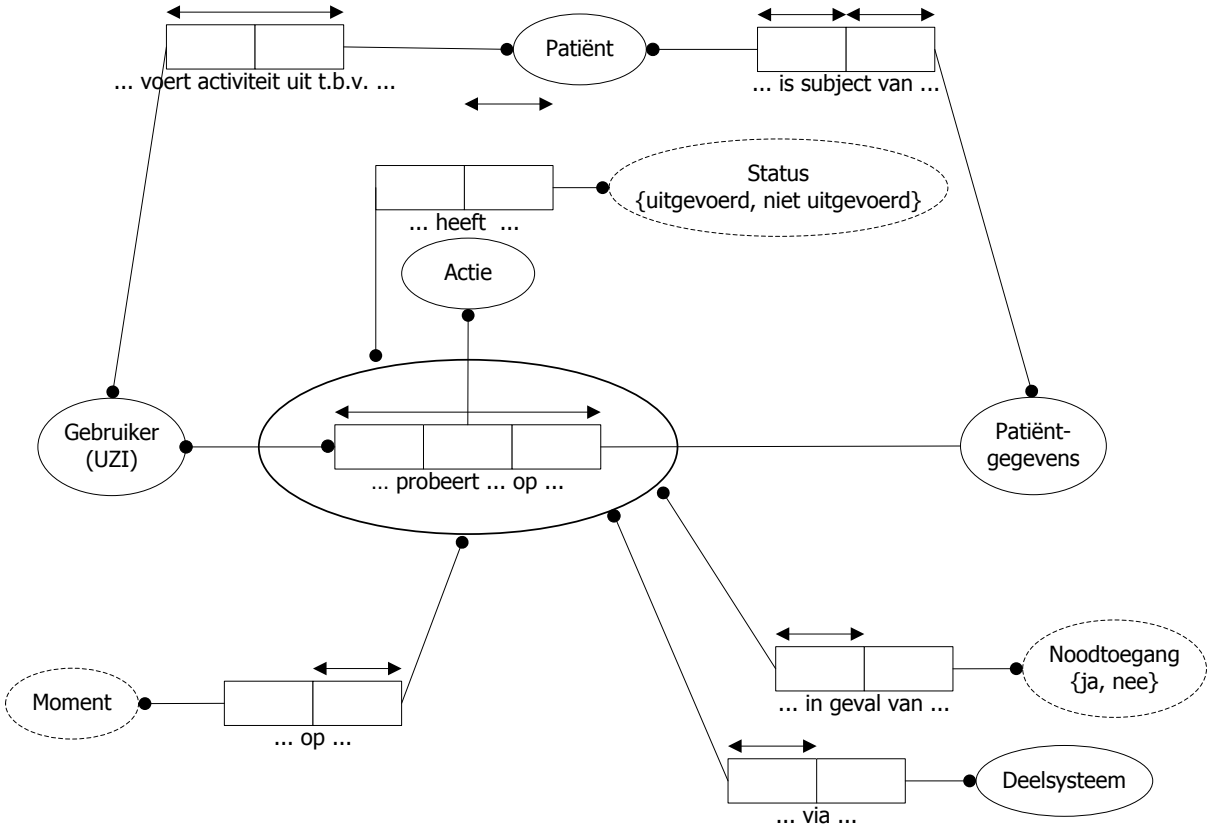


Diagram 5.7 (ORM-diagram) Conceptuele weergave van de log.

Ook NEN 7510 vereist loging van 'beveiligingsrelevante activiteiten' en het gebruik van systemen. Ook kan informatie uit het logboek worden gebruikt als bewijs bij incidenten en kan het gebruikt worden om lering te trekken uit incidenten.

Ook de patiënt moet toegang kunnen krijgen tot het log om hem of haar in te lichten over het werkelijk gebruik van zijn of haar patiëntgegevens. Ook dit zou kunnen gebeuren middels een terminal welke de patiënt tevens (onder andere) toegang biedt tot de eigen deeldossiers. Ook moeten er procedures zijn om informatieaanvragen van patiënten af te handelen, deze kunnen zowel betrekking hebben op algemene vragen over het gebruik van patiëntgegevens alsmede over het gebruik van de eigen patiëntgegevens. In de algemene procedurebeschrijving moeten tevens stappen zijn ingebouwd waarbij de patiënt inlichting ontvangt. Bij voorkeur moet geregistreerd worden of de patiënt reeds algemene voorlichting heeft ontvangen en indien dit aangevraagd is specifieke voorlichting over het gebruik van zijn of haar eigen patiëntgegevens.

Om patiënten correct en tijdig te kunnen informeren over de verwerking van patiëntgegevens is het noodzakelijk dat het ziekenhuis inzicht heeft in welke patiëntgegevens, op welke plaats, op welke manier worden verwerkt. Dit vereist goede (architectuur)ontwerpen, goede documentatie van het IT-systeem en een goed wijzigingsbeheer. Het aanstellen van een IT-architect lijkt dan ook aan te raden. Deze kan overzicht houden over de verwerking van patiëntgegevens.

5.6 'Patiëntgegevens zijn gekoppeld aan de verkeerde patiënt'

Er is al reeds een activiteit ingebouwd in het zorgproces (zoals eerder vastgelegd in *paragraaf 2.2*) om tijdens de intake na te gaan of de opgehaalde deeldossiers correct gekoppeld zijn aan de juiste patiënt. Dit hoeft echter niet voldoende te zijn, denk bijvoorbeeld aan het gebruik een deeldossiers in het geval dat de patiënt niet in de positie is na te gaan of de deeldossiers correct gekoppeld zijn. Er is hier een eenvoudige oplossing voor, namelijk de correcte koppeling na te gaan bij het ontslag van de patiënt uit het ziekenhuis.

5.7 'Patiëntgegevens zijn onvoldoende bruikbaar voor de niet-registrerende gebruiker'

Met name in het complexere domein van het deeldossier kunnen zich een aantal scenario's voordien waardoor patiëntgegevens in het deeldossier onvoldoende bruikbaar zijn voor een zorgprofessional wanneer deze gegevens worden uitgewisseld. Zo kunnen gehanteerde termen onduidelijk zijn voor een andere gebruiker van de patiëntgegevens maar kan ook de noodzakelijke context ontbreken om de patiëntgegevens goed te kunnen interpreteren. Het eerste probleem kan worden aangepakt door professional standaarden te laten hanteren waar het gaat om de wijze waarop patiëntgegevens door hen worden vastgelegd. Dit is echter vooral een discussie die in het medisch domein moet worden gevoerd en bovendien een complex probleem, waar men binnen het EPD dan ook sterk mee worstelt.

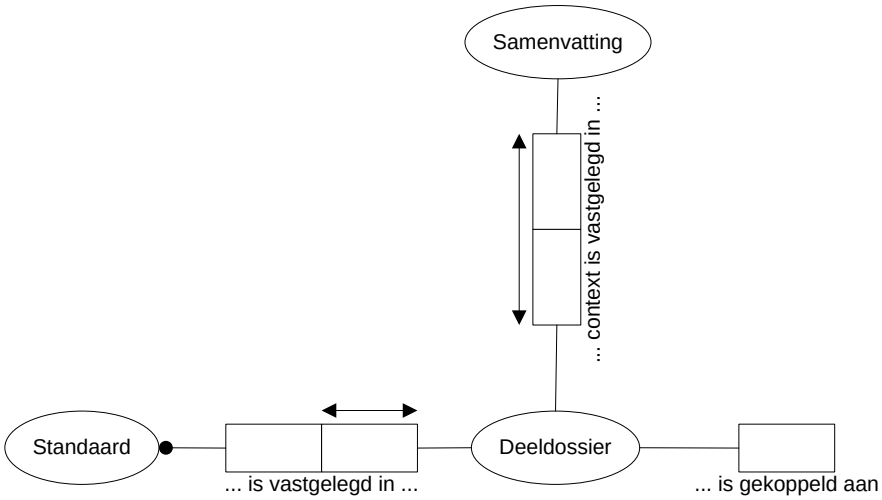


Diagram 5.8 (ORM-diagram) Het koppelen van deeldossier en het gebruik van een samenvatting om de context van patiëntgegevens te schetsen

Het gebrek aan context kan opgelost worden door de mogelijkheid te bieden deeldossier aan elkaar te koppelen zodat deze altijd samen worden uitgewisseld wanneer een zeker deeldossier wordt uitgewisseld met een andere zorgprofessional. Ook kunnen samenvattingen een oplossing bieden, wanneer de zorgprofessional een samenvatting van het deeldossier toevoegt aan het deeldossier kan hij of zij de geheimhouding optimaal bewaken door slechts de voor die zorgprofessional noodzakelijk patiëntgegevens op te nemen in de samenvatting. Bovendien zou men verschillende samenvattingen voor verschillen typen zorgprofessionals kunnen hanteren. Beiden oplossingen kunnen elkaar hierin aanvullen, zodat men optimaal kan voldoen aan wet- en regelgeving zoals de geheimhoudingsplicht welke voortkomt uit de Wgbo (en Wbp).

5.8 Status van document is onduidelijk

In deze categorie dienen twee subcategorieën te onderkennen.

- De bron is onduidelijk.
  Dit probleem kan eenvoudig worden ondervangen door alle toevoegingen te ondertekenen middels een digitale handtekening. Van iedere professional welke gegevens vastlegt is het redelijk om te eisen dat de identiteit met zekerheid vastgesteld kan worden. Door vervolgens iedere toevoeging te voorzien van een digitale handtekening kan altijd de bron van patiëntgegevens met zekerheid worden vastgesteld. Vervolgens moet deze identiteit ook worden teruggekoppeld aan de professional op wijze welke hanteerbaar is voor een mens.

- De actualiteit van de patiëntgegevens.
  Dit probleem speelt met name bij deeldossiers. Zoals we hebben kunnen zien in *hoofdstuk 2*

worden deeldossiers vaak al eerder opgehaald voordat ze gebruikt worden, Daarom moet voor ieder deeldossier duidelijk zijn of het om een kopie gaat of om een origineel. Zoals reeds eerder aangegeven moet een kopie van een deeldossier maar een beperkte tijd kunnen worden bewaard door een zorgprofessional.

5.9 'Deeldossiers zijn onvindbaar voor gebruiker'

5.10 'Patiëntgegevens kunnen redundant worden geregistreerd / zijn vastgelegd in deelsysteem'

Om te voorkomen dat patiëntregistraties redundant worden vastgelegd kan het deelsysteem het aanmaken van twee of meer registraties voor één patiënt beperken. Een eenvoudige mogelijkheid is het voor de gebruiker onmogelijk maken één BSN meer als één maal te registreren.

In het geval van een deeldossier zou het deelsysteem het gebruik van kopieën kunnen beperken zoals eerder besproken. Dit kan worden aangevuld door hashes te berekenen van deeldossiers en deze te vergelijken met bestaande deeldossiers. Ook moet het voor een gebruiker, in beginsel, niet mogelijk zijn een deeldossier te opnieuw registreren. Hierop zou uitzondering kunnen worden gemaakt wanneer het origineel onbedoeld verwijderd is.

5.11 'Patiëntgegevens zijn niet toegankelijk voor professional in geval van nood'

In het geval van een noodsituatie moet een zorgprofessional zich toegang kunnen verschaffen tot relevante patiëntgegevens, ook als dit de reguliere autorisaties doorbreekt. Een gebrek aan beheersing van deze noodzakelijke voorziening kan echter de vertrouwelijkheid van patiëntgegevens, en dus de compliance met de geheimhoudingsplicht, in gevaar brengen. Omdat het redelijk lijkt te verwachten dat een dergelijk scenario zich niet op structurele basis voor doet, immers zorgprofessionals op de spoedeisende hulp kunnen sowieso beschikken over ruimere autorisaties, lijkt het aanbevelingswaardig om ieder beroep op een noodsituatie te laten volgen door een audit om te bepalen of dit gebruik gerechtvaardigd kon worden voor de betreffende zorgprofessional in de betreffende setting.

Iedere beroep op de noodtoegang moet automatisch worden daartoe gemeld worden aan de IC-medewerker welke vervolgens nagaat of een beroep op de gebruikte patiëntgegevens te rechtvaardigen is gegeven de noodsituatie. Een belangrijk hulpmiddel hierbij is de log, maar ook het medisch dossier kan hierbij een belangrijke rol vervullen.

5.12 'Beheer van IT-systeem leidt tot problemen voor de vertrouwelijkheid en betrouwbaarheid van patiëntgegevens'

Het beheer van IT-systemen behoeft extra aandacht in het ziekenhuisdomein. Het gaat hier om kritische applicaties waarbij het niet acceptabel is dat deelsystemen incorrect functioneren of niet beschikbaar zijn. Dit kan immers een directe invloed hebben op vertrouwelijkheid en betrouwbaarheid, wat op haar beurt ernstige gevolgen kan hebben voor het ziekenhuis bijvoorbeeld ernstige imagoschade of verscherpt toezicht door medische fouten.

Er zijn vele prima methoden beschikbaar welke voorschrijven hoe een goed beheer van deelsystemen eruit moet zien. We zullen dit onderzoek dan ook niet aangrijpen om deze te herhalen. Wel willen we

aandacht vestigen op het probleem en het belang van goed en zorgvuldig beheer van het IT-systeem benadrukken.

Ook een belangrijk deel van de NEN 7510 norm spreekt zich uit over eisen ten aanzien van beheer. Omdat het ons inzien niet zinvol is alles te herhalen wat deze norm voorschrijft benoemen we hier in enkele kernwoorden enkele maatregelen welke voorgeschreven worden:

- De beschikbaarheid van bedieningsprocedures.
- Wijzigingsbeheer.
- Functiescheiding.
- Scheiden van ontwikkeling-, toets-, training-, productieomgeving.
- Het beschrijven van maatregelen in het contract bij uitbesteding.
- Capaciteitsbeheer.
- Beheer, behandeling en afvoer van media.
- Beveiling van systeemdocumentatie tegen ongeautoriseerd toegang.
- De aanwezigheid van een continuïteitsstrategie.
- Enz.

Conclusie

Vertrouwelijkheid en betrouwbaarheid van patiëntgegevens in het ziekenhuis vormen een uitdaging voor het ziekenhuis, er is een spanning tussen enerzijds het moeten delen van gegevens over de patiënt en anderzijds een geheimhoudingsplicht en ook de betrouwbaarheid (bestaat uit de waarden juistheid, volledigheid en tijdigheid) vormt een uitdaging met mogelijk ernstige gevolgen bij tekortkomingen. Met de komst van het nationale Elektronisch Patiënten Dossier (nationale EPD) is er een sterke aanleiding om het probleem nog eens onder de loep te nemen in het domein van het moderne ziekenhuis. Er is een evidente noodzaak om vertrouwelijkheid en betrouwbaarheid te garanderen, tekortkomingen kunnen leiden tot grote imagoschade, medische fouten, financiële gevolgen en verscherpt toezicht van de toezichthouder. Er is dus een duidelijke noodzaak voor beheersmaatregelen welke ruimte open laten voor de noodzakelijkheden van het domein en de kans en/of impact van incidenten verlagen. Dit is echter geen triviale uitdaging, het ziekenhuis is een complexe omgeving waarin verschillende activiteiten en actoren (mogelijk) toegang hebben en nodig hebben tot patiëntgegevens. Bovendien stelt wet- en regelgeving (in het bijzonder Wet bescherming persoonsgegevens (Wbp) en Wet op de geneeskundige behandelingsovereenkomst (Wgbo) en de 'bindende norm' NEN 7510 (Nederlandse norm voor informatiebeveiliging in de zorg) eisen aan het probleemgebied.

In dit onderzoek hebben we het domein, het ziekenhuis, waar patiëntgegevens worden geregistreerd, gebruikt en uitgewisseld in kaart gebracht en gekeken welke bepalingen uit wet- en regelgeving en normen relevant zijn voor dit probleemgebied en er een belangrijke invloed hebben. Op basis van deze kennis hebben we vervolgens een aantal risicogroepen in beeld gebracht:

1. 'Benodigde patiëntgegevens zijn niet of onvolledig geregistreerd in deelsysteem'.

   Patiëntgegevens welke een zeker doel dienen binnen activiteiten van het ziekenhuis ontbreken, bijvoorbeeld omdat ze verwijderd zijn binnen de wettelijke bewaartermijn of formulieren onvolledig zijn en de gebruiker niet vragen om alle noodzakelijke informatie. Onvolledige patiëntgegevens kunnen resulteren in fouten en het ziekenhuis / de zorgprofessional kan daardoor in gebreken zijn waar het gaat om verplichten opgelegd door de Wbp. Ook NEN 7510 vereist beheersmaatregelen t.b.v. een volledige invoer van patiëntgegevens (waar het gaat om het invoeren van gevraagde informatie).

2. 'Patiëntgegevens zijn niet (tijdig) beschikbaar voor niet-registrerende gebruikers'.

   Patiëntgegevens welke beschikbaar zouden moeten zijn, bijvoorbeeld omdat een gebruiker ze vereist voor de uitvoer van een activiteit, zijn niet beschikbaar. Dit kan bijvoorbeeld gebeuren wanneer patiëntgegevens niet tijdig worden geregistreerd door de professional in de zorg. Dit kan tot gevolgen hebben dat er fouten worden gemaakt bij de behandeling van de patiënt, bijvoorbeeld omdat relevante informatie ontbrak bij de uitvoer van medische handelingen.

3. 'Gebruikers kunnen ongewenste acties uitvoeren op patiëntgegevens'.

   Gebruikers kunnen acties uitvoeren op patiëntgegevens waartoe zij op basis van identiteit/functie/rol in de behandeling van de betreffende patiënt niet toe geautoriseerd zijn. Ook kan het zo zijn dat patiëntgegevens worden gebruikt voor doelen waar zij eigenlijk niet voor gebruikt dienen te worden. Dit kan gevolgen hebben voor de juistheid en volledigheid van de patiëntgegevens. Ook kan het zijn dat het ziekenhuis / de zorgprofessional de door de Wgbo en Wbp opgelegde geheimhoudingsplicht schendt. Ook NEN 7510 stelt bepaalde vereisten aan toegangscontrole.

4. 'Irrelevante patiëntgegevens zijn vastgelegd in deelsysteem'.

Patiëntgegevens welke geen valide doel dienen binnen de activiteiten van het ziekenhuis worden wel vastgelegd door gebruikers. Het ziekenhuis / de zorgprofessional kan hierdoor in gebreken zijn waar het gaat om verplichten opgelegd door de Wbp.

5. 'Acties van gebruikers op patiëntgegevens zijn niet controleerbaar'.

   Dit maakt het voor controlerende partijen lastig toe te zien op een correcte omgang met patiëntgegevens. Dit kan op haar beurt gevolgen hebben voor zowel vertrouwelijkheid als betrouwbaarheid.

6. 'Patiëntgegevens zijn gekoppeld aan de verkeerde patiënt'.

   Dit kan bijvoorbeeld tot gevolg hebben tot in principe ongeautoriseerde gebruikers toegang krijgen tot de medische dossiers of de professionals in de zorg bij een volgende behandeling het dossier niet onder ogen krijgen. Kortom fouten kunnen worden verwacht.

7. 'Patiëntgegevens zijn onvoldoende bruikbaar voor de niet-registrerend gebruiker'.

   Patiëntgegevens zijn niet interpreteerbaar voor de gebruiker of context noodzakelijk voor een juiste interpretatie ontbreekt. Zorgprofessionals worden hierdoor onvolledig geïnformeerd of maken fouten.

8. 'Actualiteit/bron van patiëntgegevens is onduidelijk voor de gebruiker'.

   De betreffende patiëntgegevens kunnen niet 'op waarde worden ingeschat'. Mogelijk ziet de zorgprofessional patiënttoevoegingen aan voor patiëntgegevens afkomstig van de specialist of gebruikt de professional een verouderde kopie van een dossier. Dit kan resulteren in medische fouten.

9. 'Patiëntgegevens zijn onvoldoende bruikbaar voor de niet-registrerend gebruiker'

   Wanneer patiëntgegevens worden beschreven in een formaat welke niet bruikbaar is voor een gebruikers welke de gegevens verkrijgt van een andere gebruiker kan het zijn dat hij, zij of het de patiëntgegevens niet juist kan interpreteren of misschien zelfs verkeerd begrijpt. Ook kan het zijn dat noodzakelijke context ontbreekt. Ook dat kan leiden tot fouten.

10. 'Deeldossiers zijn onvindbaar voor gebruiker'.

    De gebruiker kan hierdoor niet tijdig beschikken over benodigde patiëntgegevens of ziet patiëntgegevens over het hoofd, dit kan fouten in activiteiten tot gevolg hebben.

11. 'Patiëntgegevens kunnen redundant worden geregistreerd / zijn vastgelegd in deelsysteem'.

    Er kan hierdoor onduidelijkheid bestaan over de juistheid van patiëntgegevens of de gebruiker krijgt een onvolledig overzicht van de beschikbare patiëntgegevens, met bijvoorbeeld medische fouten tot gevolg of fouten bij de financiële verwerking van de behandeling.

12. 'Patiëntgegevens zijn niet toegankelijk voor professional in geval van nood'.

    In geval van nood kunnen reguliere autorisaties niet worden doorbroken. Dit kan medische gevolgen hebben voor de patiënt en hiermee ook negatief uitpakken voor het ziekenhuis, bijvoorbeeld omdat het imagoschade lijdt als gevolg van negatieve media aandacht.

13. 'Beheer van IT-systeem leidt tot problemen voor de vertrouwelijkheid en betrouwbaarheid van patiëntgegevens'

Ook het beheer van het IT-systeem vraagt wat extra's in het ziekenhuisdomein. Onzorgvuldig beheer kan leiden tot problemen ten aanzien van vertrouwelijkheid en betrouwbaarheid van patiëntgegevens.

Incidenten kunnen in alle bovenstaande situaties leiden tot verminderde effectiviteit/efficiëntie van de behandeling, medische fouten en/of non-compliance met wet- en regelgeving. Kortom gevolgen die het ziekenhuis dient te vermijden. Bovendien hebben we gezien dat er bij alle en veelvoorkomende activiteit zoals vastgelegd in *diagram C.1* risico's verbonden welke mogelijk de vertrouwelijkheid en betrouwbaarheid van patiëntgegevens bedreigen. Kortom de impact en frequentie van de geconstateerde risico's in doorgaans hoog.

In dit onderzoek hebben we ook de basis gelegd om deze risico's te beheersen. Kijken we naar de door ons voorgestelde oplossingen dan zien we dat er soms eenvoudige maar doeltreffende maatregelen kunnen worden genomen. Soms is bijvoorbeeld een kleine inspanning nodig van de professional om risico's af te dekken. Soms zijn er ook meer complexere maatregelen nodig. In alle gevallen is aanvullend onderzoek vereist. Zoals eerder vermeld is het een complex domein welke vele uitdagende vereisten kent. Toch bieden de voorgestelde oplossingsrichting een goede richting om te komen tot doeltreffende beheersmaatregelen.

Aanbeveling

Met dit onderzoek in handen heeft het ziekenhuis een goed uitgangspunt om risico's ten aanzien van de vertrouwelijkheid en betrouwbaarheid bij digitale registratie, gebruik en uitwisseling van patiëntgegevens binnen het ziekenhuis in kaart te brengen en te werken aan maatregelen om deze risico's te beheersen. Echter de risico's zijn in dit onderzoek in kaart gebracht voor een 'gemiddeld' en 'gegeneraliseerd' ziekenhuis. De resultaten van het onderzoek kunnen dan ook zeker niet één of één worden toegepast op een specifiek ziekenhuis.

Het in kaart brengen van risico's in dit probleemgebied is een arbeidsintensief proces. Het ontwerpen en implementeren van passende beheersmaatregelen is zo mogelijk nog arbeidsintensiever en een moeizamer proces waar het vaak invloed heeft op alle medewerkers in het ziekenhuis. Toch is het zeer noodzakelijk dat het ziekenhuis inzicht krijgt in haar risico's binnen dit probleemgebied, de zorg is en wordt namelijk geconfronteerd met vele veranderingen waaronder: het Burger Service Nummer (BSN), NEN 751X (Nederlandse norm voor informatiebeveiliging in de zorg), Diagnose Behandel Combinatie (DBC) en het nationale Elektronisch Patiënten Dossier (nationale EPD). Allen veranderingen welke een grote impact hebben op het functioneren van het ziekenhuis en raakvlakken hebben met het onderzochte probleemgebied.

Bij het in kaart brengen van risico's kan het ziekenhuis dezelfde stappen maken zoals toegepast in dit onderzoek. Sommige onderdelen behoeven hierbij meer aandacht als anderen:

1. Domeinbeschrijving
   Het ziekenhuis dient in kaart te brengen wat het eigen ziekenhuis nu karakteriseert waar dit invloed kan hebben op het probleemgebied. Het ziekenhuis dient het de modellering van het operationele zorgproces en ondersteunende activiteiten welke (mogelijk) toegang hebben tot patiëntgegevens aan te passen aan de specifieke situatie in het eigen ziekenhuis. De competentie- en autorisatiematrix dient zonder meer ook te worden aangepast waar dit sterk afhankelijk is van het specifieke ziekenhuis, maar dit hulpmiddel geeft het ziekenhuis dan ook meteen een goed inzicht in het functioneren van het eigen autorisatiebeleid en is dan ook zeker waardevol. Wij gaan er vanuit dat de conceptuele weergave van het domeingebied ongewijzigd kan worden toegepast door het specifieke ziekenhuis.

2. Wet- en regelgeving en norm
   De in kaart gebrachte wet- en regelgeving (Wet bescherming persoonsgegevens en Wet op de geneeskundige behandelovereenkomst) en norm (NEN 7510) zijn organisatieonafhankelijk en kunnen direct worden toegepast in de analyse van het specifieke ziekenhuis.

3. Risicoanalyse
   De risicoanalyse moet in ieder geval worden afgestemd op het specifieke operationele zorgproces en ondersteunende activiteiten welke patiëntgegevens gebruiken. Hierbij kan verwacht worden dat de in dit onderzoek in kaart gebrachte risico's vaak een prima basis bieden om de ziekenhuisspecifieke risico's in kaart te brengen. Het is redelijk om te verwachten dat de beschreven 'kernrisico's' voor alle ziekenhuizen (grotendeels) identiek zijn.

4. Beheersmaatregelen
   De beschreven beheersmaatregelen behoeven verder onderzoek om te worden toegepast in ziekenhuizen. Toch vormen de beschreven beheersmaatregelen een prima uitgangspunt voor deze onderzoeken omdat zij de minimum vereisten binnen een zekere, in onze ogen geschikte, oplossingrichting in kaart brengen.

Bijlage A. Architectuur van het EPD

Deze bijlage biedt de lezer inzicht in de architectuur van het EPD. Omdat het EPD een project is wat nog sterk in ontwikkeling is, is die documentatie gebruikt welke voorhanden was bij aanvang van het project (februari 2009).

De feiten zoals gepresenteerd in dit hoofdstuk zijn gebaseerd op informatie afkomstig uit [12], ook de quotes welke opgenomen zijn in het hoofdstuk zijn afkomstig uit deze bron. Waar informatie afkomstig is uit een andere bron zal dit expliciet vermeldt worden.

Ook de naamgeving zoals gehanteerd in dit hoofdstuk is afkomstig van de gerefereerde literatuur.

A.1 Doelstellingen

Een bondige beschrijving van de belangrijkste doelstelling gekoppeld aan de invoering van het EPD [6][12]:

Strategisch

- Kwalitatief hoogstaande (effectieve) zorg.
  De zorgsector staat onder druk om effectieve zorg te leveren, dit wil zeggen zorg met een hoog niveau van herstel.

- Efficiënte zorg.
  De zorgsector staat onder druk om deze zorg te leveren tegen minimale kosten.

- Veilige zorg.
  Het publiek heeft weinig tolerantie voor fouten in de medische zorg.

Operationele doelstellingen

- De juiste patiëntgegevens, op het juiste moment op de juiste plek.

- Patiëntgegevens moeten eenvoudig kunnen worden uitgewisseld.

- Een goede relatie tussen arts en patiënt.

A.2 Introductie structuur EPD

Diagram A.1 toont als introductie op het EPD op hoog niveau en sterk vereenvoudigd de belangrijkste onderdelen en stakeholders van het EPD. In de hierop volgende paragraven zullen meer details worden aangebracht. Om de leesbaarheid van het diagram te optimaliseren zijn niet alle relaties ingetekend. De weggelaten relaties zullen echter wel aan bod komen in de toelichting welke volgt op het diagram.

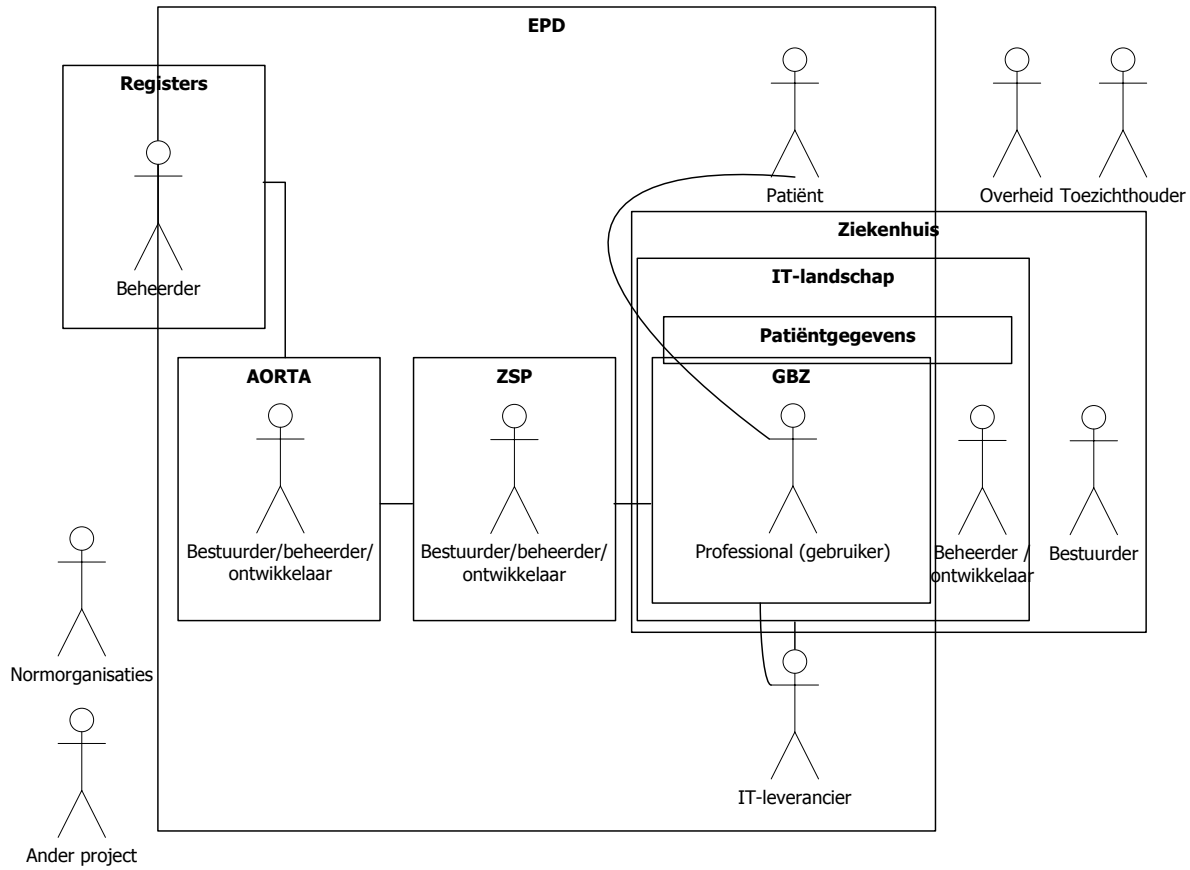


Diagram A.1 Hoog niveau overzicht van de belangrijkste systemen en actoren van het EPD.

Ter introductie een korte inleiding op de benoemde systemen, actoren en relaties:

De patiënt staat centraal in het probleem. Het zijn, zijn of haar medische gegevens (en andere persoonsgegevens) welke worden uitgewisseld tussen hem of haar en de zorgaanbieder, tussen zorgaanbieders onderling of met derden.

Het ziekenhuis levert zorgdiensten aan de patiënt en werkt hiervoor mogelijk samen met andere zorgaanbieders en met (o.a.) de overheid.

Het ziekenhuis maakt gebruik van een zeker IT-landschap; dit wil zeggen alle IT-systemen en bijbehorende organisatorische voorzieningen (procedures, projecten, etc.).

Binnen dit IT-landschap vinden we een deelsysteem (bestaande uit één of meer IT-systemen) welke patiëntgegevens uitwisselt via het EPD. Dit deelsysteem is het zogenaamde Goed Beheerd Zorgsysteem (GBZ).

Het zijn de professionals (gebruikers) welke via het GBZ patiëntgegevens uitwisselen.

Het IT-systemen in het IT-landschap wordt geleverd door één of meerdere IT-leverancier(s).

Patiëntgegevens worden, in principe, gedeeld met andere zorgaanbieders middels een geheel aan centrale voorzieningen, de AORTA. Deze wordt bestuurd, beheerd en ontwikkeld.

Omdat de zorgaanbieder fysiek gescheiden is van de AORTA is er een derde partij welke de twee verbindt, in staat stelt te communiceren. Dit is de zogenaamde Zorg Service Provider (ZSP). Ook voor de ZSP geldt dat er naast een voorziening ook een organisatie is welke het beheerd, ontwikkeld en bestuurd.

De registers zijn nodig om patiënten en professionals (gebruikers) correct te kunnen identificeren. Deze registers dienen uiteraard te worden beheerd. Let op dat de registers weliswaar gebruikt worden door het EPD, maar niet exclusief het EPD dienen.

De overheid heeft een sturende rol in het EPD. Het heeft onder meer een regierol en stelt wetten en regels welke de elektronische uitwisseling van patiëntgegevens reguleren.

De toezichthouder ziet toe op een correct gebruik van patiëntgegevens.

Ook normorganisaties en andere projecten hebben een invloed op de architectuur van het EPD.

A.3 Elektronisch Patiënten Dossier vs. lokaal

Binnen ons onderzoek kunnen we een tweetal domein onderkennen; het lokale domein bij het ziekenhuis (hetgeen in de directe invloedssfeer van het ziekenhuis) en een domein met nationale centrale voorzieningen welke gedeeld wordt door alle zorgaanbieders binnen de grenzen van het Nederlandse zorgsysteem.

Zoals eerder vermeldt is er een nationaal, en mogelijk op termijn internationaal, domein waarbinnen patiëntgegevens worden uitgewisseld tussen zorgaanbieders via centrale voorzieningen, de AORTA. Deze voorzieningen zijn niet gebonden aan een specifiek ziekenhuis.

Het andere domein heeft, met name, plaats binnen de organisatiegrenzen van het ziekenhuis. In dit domein worden ook patiëntgegevens uitgewisseld, maar met name binnen de grenzen van het ziekenhuis en met behulp van een eigen IT-landschap. Er wordt voor uitwisseling geen gebruik gemaakt van de centrale voorzieningen, AORTA. Ook in dit tweede domein kunnen patiëntgegevens worden uitgewisseld tussen verschillende ziekenhuizen, hierbij wordt dan echter geen gebruik gemaakt van AORTA, maar van regionale voorzieningen, bijvoorbeeld een gedeeld GBZ.

A.4 Deelsystemen

Nu we in *paragraaf A.2* op hoog niveau de belangrijkste systemen en actoren in kaart hebben gebracht brengen we in deze paragraaf een overzicht van de deelsystemen welke betrokken zijn bij de uitwisseling van patiëntgegevens via het EPD.

Na het diagram welke een overzicht biedt van alle deelsystemen volgt een korte introductie op ieder van deze deelsystemen.

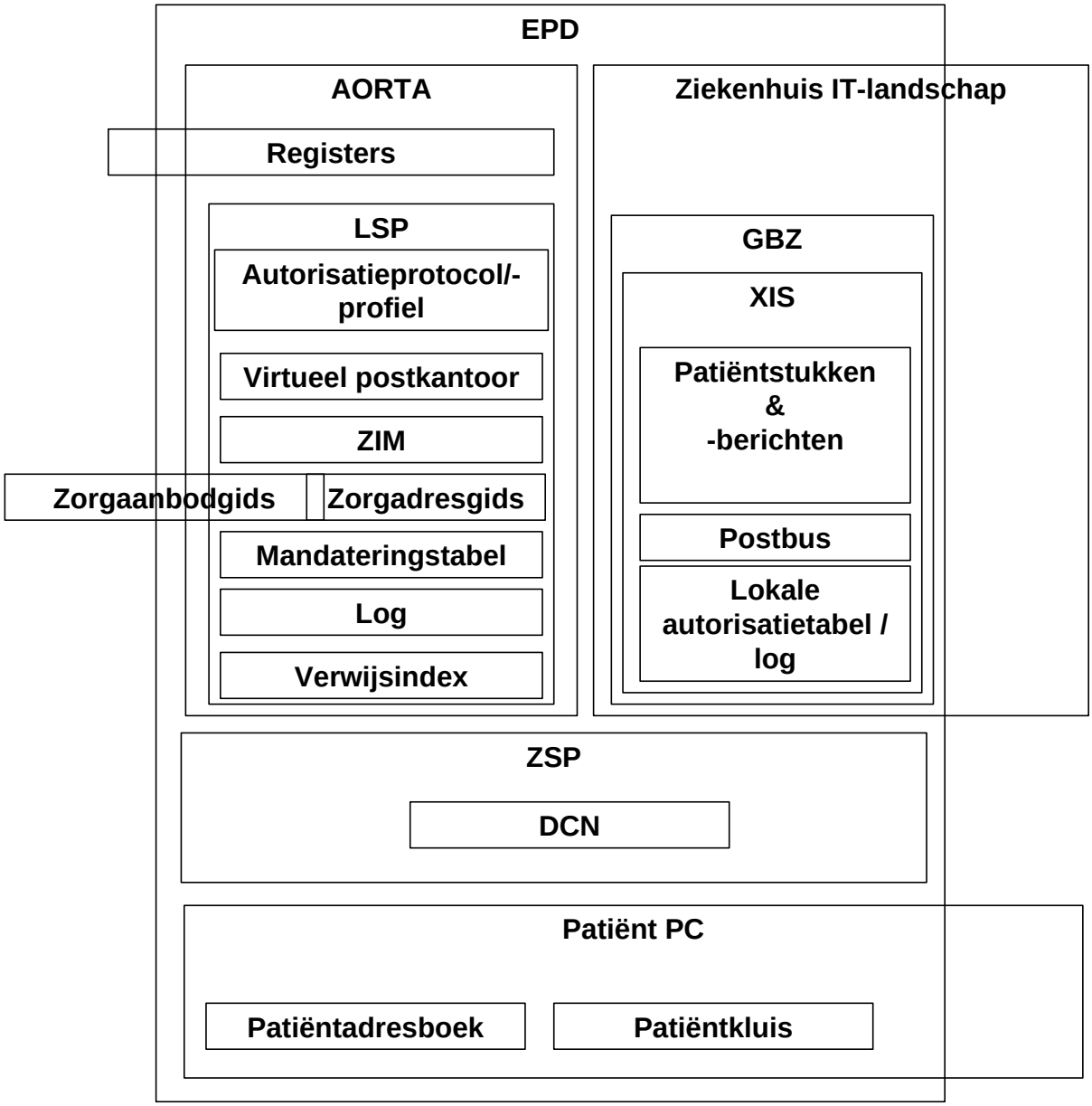


Diagram A.2 Deelsystemen van het EPD.

A.4.1 Ziekenhuis IT-landschap

Zoals gezegd bestaat het Ziekenhuis IT-landschap uit lokale systemen welke patiëntgegevens registreren en systemen welke deze gegevens uitwisselen via het EPD en systemen geen patiëntgegevens uitwisselen via het EPD, maar mogelijk wel patiëntgegevens uitwisselen tussen systemen binnen de organisatorische grenzen van het ziekenhuis of met andere ziekenhuizen middels regionale voorzieningen.

Het deel welke wel patiëntgegevens uitwisselt via het EPD wordt aangeduid als het Goed Beheerd Zorgsysteem (GBZ). Het GBZ bestaat op haar beurt uit één of meer zorginformatiesystemen (XIS'en), een verzamelnaam voor verschillende typen zorginformatiesystemen.

Het zijn deze XIS'en welke de patiëntstukken (medische gegevens) en patiëntberichten (communicatieberichten tussen ziekenhuizen en patiënten (toekomst) en zorgaanbieders) bevatten.

Om deze patiëntberichten te kunnen uitwisselen via het EPD is er een postbus, voor individuen maar ook voor groepen.

Om de vertrouwelijkheid van patiëntgegevens ook lokaal (bijvoorbeeld na uitwisseling) te kunnen bewaken is er een lokale log en autorisatietabel.

A.4.2 AORTA

Het AORTA wordt gevormd door een verzameling samenhangende centrale voorzieningen welke de spil vormen in de uitwisseling van patiëntgegevens via het EPD. We bespreken hieronder ieder van deze voorzieningen:

Tot de AORTA kunnen we gedeeltelijk de verschillende registers rekenen welke het voor het EPD mogelijk maken gebruikers van het EPD en patiënten te identificeren. Deze registers dienen echter ook andere voorzieningen.

Binnen de AORTA vinden we het Landelijk Schakelpunt (LSP). Zoals de naam al suggereert vindt de uitwisseling van patiëntgegevens plaats middels deze voorziening. Het LSP kan worden opgedeeld in een aantal deelsystemen (zie *diagram A.2*). Ook deze zullen we toelichten in *deze paragraaf*.

Het LSP bevat een autorisatieprotocol welke regelt welke rol toegang heeft tot wat binnen het EPD. Het komt tot stand door overleg van belangenverenigingen van patiënten/cliënten en beroepsverenigingen van de zorgaanbieders.

Het autorisatieprofiel staat onder controle van de patiënt zelf en kan gebruikt worden om het autorisatieprofiel in te beperken, door bijvoorbeeld geen toestemming te verlenen voor de elektronische uitwisseling van zijn of haar patiëntgegevens via het EPD of bepaalde ziekenhuizen/gebruikers uit te sluiten van toegang tot bepaalde gegevens.

Het virtueel postkantoor maakt het mogelijk patiëntberichten, zoals in *paragraaf A.4.1* benoemt, uit te wisselen via het EPD.

Het Zorg Informatie Makelaar (ZIM) is het deelsysteem welke de daadwerkelijke uitwisseling verzorgt. Het regelt onder meer de identificatie- en autorisatie van gebruikers (in samenwerking met andere deelsystemen).

De zorgadresgids bevat de adressen van de postbussen van zorgaanbieders, afdelingen en gebruikers zodat een verzendende zorgaanbieder de adresgegevens kan opvragen van de partij welke de berichten dient te ontvangen. In de toekomst zal deze gids ook door de patiënt kunnen worden gebruikt wanneer deze zelf berichten kan verzenden via het EPD. Dit is voorlopig echter nog niet mogelijk.

Het patiëntadresboek biedt vergelijkbare functionaliteit (indien er een noodzaak voor bestaat bij voldoende deelnemende patiënten) voor het adressen van patiënten wanneer zij in de toekomst een eigen postbus krijgen.

De zorgaanbodgidsen bevatten informatie over de dienstverlening van de zorgaanbieder. In de toekomst worden dergelijke gidsen mogelijk gecombineerd met het zorgadresboek.

De mandateringstabel vormt een centrale administratie waarin is vastgelegd wie gemandateerd is door een zogeheten verantwoordelijk zorgverlener om bepaalde handelingen uit te mogen voeren in zijn of haar naam. Deze kan zo een medebehandelaar zijn of een medewerker mandateren.

Het log registreert op een logisch centrale plaats acties welke verlopen via het EPD. Lokale acties worden geregistreerd in het eerder genoemde lokale log.

De verwijsindex is de centrale administratie van alle patiëntgegevens welke zijn aangemeld zijn voor landelijke uitwisseling.

A.4.3 Zorg Service Provider

Deze partij verzorgt, zoals eerder vermeld, de koppeling van het GBZ van de zorgaanbieder (of het samenwerkingsverband) aan het LSP.

De communicatie verloopt middels een Data Communicatie Netwerk (DCN). De ZSP kan bovendien ook aanvullende diensten verlenen aan het ziekenhuis, dit is echter afhankelijk van het individuele geval.

A.4.4 Patiënt

De patiënt zal in de toekomst beschikken over eigen voorzieningen om actief deel te kunnen nemen in de uitwisseling van patiëntgegevens middels het EPD. In de loop van het project zal de patiënt beschikken over een patiëntadresboek (vergelijkbaar in functie met het eerder besproken zorgadresboek) en een patiëntkluis waarmee hij of zij medische gegevens kan uitwisselen met de zorgaanbieder.

Bijlage B. Gespecificeerd zorgproces

Diagram B.1 Uitgebreide specificatie van het zorgproces en ondersteunende activiteiten voor zover deze relevant zijn voor het probleemgebied.

Bijlage C. Risicoanalyse

In deze bijlage brengen we per activiteit zoals vastgelegd in *diagram B.1* risico's welke verbonden zijn aan de vertrouwelijkheid en betrouwbaarheid van patiëntgegevens in het ziekenhuis in kaart.

Activiteit	**Num.**	**Risico**	**Kwaliteitsaspect**	**Categorie**
Registratie persoonsgegevens	1.1	Persoonsgegevens worden incorrect geregistreerd door de registrerend professional, hierdoor worden mogelijk door actoren foute persoonsgegevens gebruikt bij de uitvoer van vervolgactiviteiten.	J	incorrecte patiëntgegevens

	1.2	De registerend professional registreert niet alle door het deelsysteem gevraagde persoonsgegevens voor de patiëntregistratie, hierdoor kunnen actoren in vervolgactiviteiten niet beschikken over voldoende patiëntgegevens.	Vo	onvolledige patiëntgegevens
	1.3	De registrerend professional registreert de patiëntregistratie niet tijdig, mogelijk kunnen zorgprofessionals hierdoor deeldossiers niet tijdig koppelen aan een identiteit en/of het ziekenhuis start een behandeling op een bijvoorbeeld onverzekerde patiënt.	T	patiëntgegevens niet tijdig beschikbaar
	1.4	De registrerend professional kan niet tijdig beschikken over noodzakelijke persoonsgegevens en kan hierdoor de patiëntregistratie niet tijdig afronden, hierdoor kan de identiteit van de patiënt niet tijdig worden bepaald en vervolg activiteiten niet (correct) worden uitgevoerd.	T	patiëntgegevens niet tijdig beschikbaar

	1.5	Er kunnen acties worden uitgevoerd op de patiëntregistratie door gebruikers welke hier op basis van hun identiteit/functie geen autorisatie toe hebben, de correctheid van de patiëntgegevens staat hiermee op het spel.	J	ongewenste acties patiëntgegevens
	1.6	Persoonsgegevens welke geen valide doel dienen binnen het domein worden door het ziekenhuis/professional geregistreerd of er is een minder ingrijpend alternatief voor registratie van de betreffende persoonsgegevens voorhanden, mogelijk is het ziekenhuis hierdoor in strijd met de Wbp.	Ve	registratie irrelevante patiëntgegevens
	1.7	Persoonsgegevens welke een valide doel dienen binnen het domein worden niet geregistreerd in de patiëntregistratie, gebruikers in vervolgactiviteiten kunnen hierdoor niet beschikken over noodzakelijke patiëntgegevens en mogelijk is het ziekenhuis in strijd met de Wbp.	Vo	onvolledige patiëntgegevens
	1.8	Het is voor toezichthouders, IC-medewerkers en controller/HEAD niet mogelijk te achterhalen wie, welke acties zijn uitgevoerd op de patiëntregistratie, er is daardoor mogelijk onvoldoende toezicht mogelijk op correcte gedrag van gebruikers waar het gaat om de registratie, gebruik en/of uitwisseling van patiëntregistraties.	Ve/Vo/J/T	acties zijn niet controleerbaar

	1.9	Persoonsgegevens worden door gebruikers gebruikt voor een doel, anders als het initiële doel van verzameling en onverenigbaar met het initiële doel, mogelijk overtreed het ziekenhuis/professional hiermee de Wbp.	Ve	ongewenste acties patiëntgegevens
	1.10	De patiënt wordt onvoldoende/niet-tijdig geïnformeerd over de identiteit van de verzamelaar en/of het doel van de registratie en, indien daartoe aanleiding is, andere relevante informatie over de patiëntregistratie, het ziekenhuis zou hierdoor is strijd kunnen zijn met de Wbp.	Ve	acties zijn niet controleerbaar
	1.11	De patiënt kan op aanvraag niet door het ziekenhuis correct en/of tijdig worden geïnformeerd over de (mogelijke) verwerking van zijn of haar persoonsgegevens in de patiëntregistratie (conform Wbp), het ziekenhuis is hierdoor mogelijk in overtreding met de Wbp.	Ve	acties zijn niet controleerbaar
	1.12	Een patiëntregistratie wordt niet gecorrigeerd wanneer noodzakelijk, actoren gebruiken hierdoor in vervolgactiviteiten mogelijk onjuiste en/of onvolledige gegevens en men handelt mogelijk in strijd met de Wbp.	J	incorrecte patiëntgegevens
	1.13	Persoonsgegevens zijn niet toegankelijk voor de gebruiker in geval van nood, dit kan mogelijk medische fouten tot gevolg hebben.	Ve	noodtoegang patiëntgegevens
	1.14	De gebruiker kan de patientregistratie niet tijdig vinden, vervolgactiviteiten kunnen hierdoor niet tijdig worden gestart.	T	patiëntgegevens zijn onvindbaar

	1.15	Patientregistratie kan redundant worden geregistreerd door de professional, dit kan de correctheid van de patientregistratie in gevaar brengen.	J	redundantie patiëntgegevens
	1.16	Patiëntregistraties kunnen door de medewerkers van het afsprakenbureau verwijderd worden binnen de gewenste tijdsduur van registratie, andere patiëntgegevens zijn hierdoor niet begeleid door een patiëntregistratie.	J	onvolledige patiëntgegevens
BSN opvraag & registratie*	2.1	De opvraag van het BSN door de uitvoerend professional levert een incorrect BSN op, hierdoor zullen actoren waarschijnlijk het verkeerde BSN worden gebruikt bij vervolgactiviteiten waardoor bijvoorbeeld deeldossiers worden gekoppeld aan het verkeerde BSN.	J	incorrecte patiëntgegevens
	2.2	Het door de uitvoerend professional opgevraagde BSN wordt fout overgenomen in de patiëntregistratie. (De gevolgen zijn identiek aan 2.1)	J	incorrecte patiëntgegevens
	2.3	Het is voor de uitvoerend professional niet mogelijk het BSN tijdig op te vragen omdat men over onvoldoende persoonsgegevens beschikt, dit kan beperkingen opleveren voor gebruikers bij vervolgactiviteiten.	T	patiëntgegevens niet tijdig beschikbaar
	2.4	Persoonsgegevens worden door gebruikers gebruikt voor een doel, anders als het initiële doel van verzameling en onverenigbaar met het initiële doel, mogelijk overtreed het ziekenhuis/professional hiermee de Wbp.	Ve	ongewenste acties patiëntgegevens

	2.5	De patiënt wordt door het ziekenhuis onvoldoende/niet-tijdig geïnformeerd over de identiteit van de verzamelaar en/of het doel van de registratie en, indien daartoe aanleiding is, andere relevante informatie over de patiëntregistratie, het ziekenhuis zou hierdoor is strijd kunnen zijn met de Wbp.	Ve	acties zijn niet controleerbaar
	2.6	De patiënt kan op aanvraag door het ziekenhuis niet correct en/of tijdig worden geïnformeerd over de (mogelijke) verwerking van zijn of haar persoonsgegevens in de patiëntregistratie (conform Wbp), het ziekenhuis is hierdoor mogelijk in overtreding met de Wbp.	Ve	acties zijn niet controleerbaar
	2.7	Persoonsgegevens zijn niet toegankelijk voor de gebruiker in geval van nood, dit kan mogelijk medische fouten tot gevolg hebben.	Ve	noodtoegang patiëntgegevens
Plannen intake (3) / inzien agenda (4)*	3.1	De professional welke de afspraak registreert voert de afspraak verkeerd in of geconstateerde fouten worden niet gecorrigeerd, de intake wordt hierdoor mogelijk niet tijdig uitgevoerd.	J	incorrecte patiëntgegevens
	3.2	Een niet daartoe geautoriseerde gebruiker kan acties uitvoeren op registraties van afspraken in de agenda, hierdoor loopt de correctheid van de agenda gevaar.	J	ongewenste acties patiëntgegevens
	3.3	Patiëntgegevens worden door gebruikers gebruikt voor doelen anders dan het initiële doel van verzameling voor een doel niet verenigbaar met het initiële doel van verzameling, het ziekenhuis/professional handelt hiermee mogelijk in strijd met de Wbp.	Ve	ongewenste acties patiëntgegevens

	3.4	Het is voor de toezichthouder, IC-medewerker en controller/HEAD onvoldoende mogelijk te achterhalen welke acties door gebruikers zijn uitgevoerd op de agenda, het is hierdoor onvoldoende mogelijk toezicht te houden op de correct gedrag t.a.v. deze patiëntgegevens.	J/T/Vo	acties zijn niet controleerbaar
	3.5	De patiënt wordt door het ziekenhuis onvoldoende/niet-tijdig geïnformeerd over de identiteit van de verzamelaar en/of het doel van de registratie en indien van toepassing andere relevante informatie, het ziekenhuis is hiermee mogelijk in overtreding met de Wbp.	Ve	acties zijn niet controleerbaar
	3.6	De patiënt kan op aanvraag door het ziekenhuis niet correct en/of tijdig worden geïnformeerd over de (mogelijke) verwerking van zijn of haar persoonsgegevens in de patiëntregistratie (conform Wbp), het ziekenhuis is hierdoor mogelijk in overtreding met de Wbp.	Ve	acties zijn niet controleerbaar
	3.7	Een afspraak wordt niet tijdig vastgelegd in de agenda door de registrerend professional, de agenda is hierdoor incorrect en onbetrouwbaar voor gebruikers in vervolgactiviteiten.	T	patiëntgegevens niet tijdig beschikbaar

Dossier(s) ophalen	5.1	Een deeldossiers is toegankelijk voor gebruikers welke op basis van identiteit/functie en betrokkenheid bij de actuele behandeling van de patient welke subject is van het deeldossier geen autorisatie hiervoor hebben, het ziekenhuis / de professional schendt zeer waarschijnlijk hiermee de geheimhoudingsplicht opgelegd door de Wgbo en Wbp.	Ve	ongewenste acties patiëntgegevens
	5.2	Een afgeschermd deeldossier is toegankelijk voor een ander dan de beheerverantwoordelijk specialist, het ziekenhuis / de professional handelt hiermee in strijd met de wet en tegen de wens van de patiënt.	Ve	ongewenste acties patiëntgegevens
	5.3	Een verwijderd deeldossier is toegankelijk voor een gebruiker, het ziekenhuis / de zorgprofessional handelt hiermee in strijd met de wet en tegen de wens van de patiënt.	Ve	ongewenste acties patiëntgegevens

	5.4	Een deeldossier verkregen van derden wordt gebruikt zonder (veronderstelde) toestemming van de patiënt, het ziekenhuis / de zorgprofessional handelt hierdoor in strijd met het Wbp.	Ve	ongewenste acties patiëntgegevens
	5.5	De beheersverantwoordelijke voor een zeker deeldossier en controlerende partijen hebben onvoldoende inzicht in welke gebruikers welke toegang hebben tot het deeldossier, de vertrouwelijkheid van het deeldossier kan hierdoor onvoldoende worden gecontroleerd.	Ve	acties zijn niet controleerbaar
	5.6	De zorgprofessional welke toegang heeft tot een deeldossier lekt informatie uit het deeldossier aan derden niet betrokken bij de behandeling, de zorgprofessional schendt hiermee de geheimhoudingsplicht opgelegd door de Wgbo.	Ve	ongewenste acties patiëntgegevens
	5.7	Een relevante deeldossier is niet (tijdig) beschikbaar (mogelijk ongemerkt), de zorgprofessional handelt hierdoor op basis van incomplete informatie, kan bepaalde activiteiten niet starten of voert activiteiten redundant uit.	T	patiëntgegevens niet tijdig beschikbaar
	5.8	Een deeldossier is voor een zorgprofessional niet toegankelijk in geval van nood, de zorgprofessional beschikt hierdoor niet tijdig over relevante medische informatie.	T	noodtoegang patiëntgegevens

	5.9	Een relevante deeldossier is niet of moeilijk vindbaar voor de gebruiker, relevante medische informatie wordt hierdoor gemist met mogelijk medische fouten tot gevolg.	T	patiëntgegevens zijn onvindbaar
	5.10	De actualiteit van een deeldossier is met onvoldoende zekerheid te bepalen door de gebruiker, de zorgprofessional handelt hierdoor mogelijk op basis van verouderde, onjuiste patiëntgegevens met mogelijk medische fouten tot gevolg.	J	status patiëntgegevens
	5.11	De bron van een deeldossier is onduidelijk voor de gebruiker, hierdoor kan de waarde van de patiëntgegevens in het deeldossier niet op waarde worden geschat.	J	status patiëntgegevens
	5.12	De authenticiteit van patiëntgegevens in een deeldossier is onvoldoende bepaalbaar door de gebruiker, de correctheid van de patiëntgegevens kan hierdoor met onvoldoende zekerheid worden vastgesteld.	J	incorrecte patiëntgegevens
	5.13	Een deeldossier wordt door de beheerverantwoordelijk specialist korter/langer bewaard als gewenst door de patiënt en vereist door wet- en regelgeving, het ziekenhuis handelt hierdoor mogelijk in strijd met de Wgbo.	Ve	onvolledige patiëntgegevens respectievelijk registratie irrelevante patiëntgegevens

	5.14	De gebruiker heeft geen toegang tot de meest recente relevante patiëntgegevens in een deeldossier, mogelijk handelt het ziekenhuis / de professional hierdoor op basis van onjuiste patiëntgegevens.	T	toegang actuele/historische patiëntgegevens
	5.15	De gebruiker heeft geen toegang tot eerdere versies van een deeldossier, mogelijk kunnen hierdoor fouten in het deeldossier ontstaan.	T	toegang actuele/historische patiëntgegevens
	5.17	Het ziekenhuis / Een beheerverantwoordelijk specialist verliest één of meer deeldossiers, ze zijn hierdoor niet meer beschikbaar voor gebruikers in vervolgactiviteiten en waarschijnlijk is het ziekenhuis / de beheerverantwoordelijk specialist non-compliant met de Wgbo en mogelijk Wbp.	T	onvolledige patiëntgegevens
	5.18	Het deeldossier wordt onvolledig vastgelegd door de zorgprofessional, bij toekomstig gebruik van het betreffende deeldossier of vervolgactiviteiten gebruikers van het deeldossier hierdoor fouten maken.	Vo	onvolledige patiëntgegevens
Verificatie dossier(s)	6.1	Het gebruik van een niet aan de patiënt gebonden deeldossier wordt niet opgemerkt, hierdoor worden mogelijk een verkeerd deeldossier gebruikt bij diagnostiek en behandeling.	J	verkeerde koppeling patiëntgegevens
Intake	7.1	Een deeldossier bevat niet alle noodzakelijke patiëntgegevens, voor de uitvoering van de intake door de hoofdbehandelaar, relevante informatie over de gezondheid van de patiënt wordt hierdoor mogelijk gemist door de hoofdbehandelaar met mogelijk medische fouten tot gevolg.	Vo	onvolledige patiëntgegevens

	7.2	Een deeldossier bevat incorrecte patiëntgegevens, mogelijk leidt dit tot medische fouten.	J	incorrecte patiëntgegevens
	7.3	De hoofdbehandelaar kan het deeldossier onvoldoende gebruiken omdat patiëntgegevens noodzakelijk voor het bepalen van de context van patiëntgegevens in het deeldossier ontbreekt, dit kan leiden tot medische fouten.	J	onbruikbare patiëntgegevens
	7.4	Een hoofdbehandelaar kan het deeldossier onvoldoende gebruiken omdat hij of zij de daarin opgenomen patiëntgegevens niet kan interpreteren, hij of zij kan hierdoor niet beschikken over de noodzakelijke patiëntgegevens of maakt fouten bij de interpretatie.	J	onbruikbare patiëntgegevens
Verkrijgen taak	8	Geen relevante risico's.		
Dossier(s) ophalen	9	Zie activiteit 5.		
Uitvoeren taak	10	Identiek aan risico's beschreven bij activiteit 7.		
Registratie medische patiëntgegevens	11.1	Medische gegevens worden onvolledig vastgelegd in een deeldossiers door de zorgprofessional, gebruikers van deze deeldossiers worden hierdoor onvolledig geïnformeerd over de uitkomsten van taken ten behoeve van diagnostiek of behandeling en het medische verleden van de patiënt. Bovendien kan het ziekenhuis / de zorgprofessional in overtreding zijn met het Wbp en Wgbo.	Vo	onvolledige patiëntgegevens
	11.2	Medische gegevens worden door de zorgprofessional incorrect vastgelegd in het betreffende deeldossiers, gebruikers van deze deeldossiers worden hierdoor onvolledig geïnformeerd over de uitkomsten van taken ten behoeve van diagnostiek of behandeling en het	J	incorrecte patiëntgegevens

		medische verleden van de patiënt.		
	11.3	Medisch gegevens worden niet tijdig vastgelegd in een deeldossier door de zorgprofessional, (potentiële) gebruikers van het deeldossier kunnen hierdoor niet tijdig beschikken over relevante patiëntgegevens nodig voor diagnose of behandeling.	T	patiëntgegevens niet tijdig beschikbaar
	11.4	Deeldossiers worden niet (tijdig) gedeeld door de zorgprofessional, andere gebruikers kunnen hierdoor niet tijdig beschikken over de patiëntgegevens in het dossier.	T	patiëntgegevens niet tijdig beschikbaar
	11.5	Gebruikers anders dan bij de diagnostiek/behandeling betrokken zorgprofessionals, kunnen gegevens registreren. Dit verhoogt de kans dat gegevens foutief worden geregistreerd.	J	ongewenste acties patiëntgegevens
	11.6	Medische patiëntgegevens worden door de zorgprofessional geregistreerd in het deeldossier zonder dat hier valide aanleiding toe is, mogelijk handelt het ziekenhuis / de zorgprofessional hierdoor in strijd met de Wbp.	Ve	registratie irrelevante patiëntgegevens

	11.7	Medische gegevens worden door de zorgprofessional meermaals vastgelegd in verschillende deeldossiers, dit verhoogt het risico dat fouten niet gecorrigeerd worden en maakt het lastiger toe te zien op een correcte geheimhouding van de patiëntgegevens. Ook is het lastiger te overzien of de vastlegging compleet is.	Ve/J/Vo	redundantie patiëntgegevens
	11.8	Medische gegevens vastgelegd in een deeldossier worden niet gewijzigd wanneer geconstateerd is dat deze incorrect zijn, de juistheid van de gegevens is hierdoor onvoldoende en dit kan medische fouten tot gevolg hebben.	J	incorrecte patiëntgegevens
	11.9	Medische gegevens kunnen door gebruikers gewijzigd worden na initiële vastleggen in een deeldossier, dit maakt het voor de toezichthouder en IC-medewerker lastig toe te zien op correct gedrag omtrent de registratie van medisch gegevens en maakt het lastig correctheid en volledigheid te garanderen.	J(/Vo)	incorrecte patiëntgegevens, onvolledige patiëntgegevens
	11.10	Medische gegevens uit deeldossiers worden door een gebruiker gebruikt voor doelen anders dan het initiële doel van verzameling en dit doel is onverenigbaar met het initiële doel.	Ve	ongewenste acties patiëntgegevens
	11.11	Noodzakelijke meta-gegevens worden niet vastgelegd bij het deeldossier, dit kan er bijvoorbeeld voor zorgen dat een deeldossier niet vindbaar is voor de gebruiker.	Vo	onvolledige patiëntgegevens

	11.12	Een deeldossier wordt door de registrerend zorgprofessional gekoppeld aan de verkeerde patiënt, het dossier is als gevolg hiervan bijvoorbeeld niet tijdig vindbaar en/of toegankelijk voor ongeautoriseerde gebruikers.	J/T/Ve	verkeerde koppeling patiëntgegevens
	11.14	Patiëntverklaringen zijn onvoldoende te onderscheiden van toevoegingen van zorgprofessionals, hierdoor kunnen de patiëntgegevens welke opgenomen zijn in het deeldossier mogelijk niet op de juiste waarde worden geschat.	J	status patiëntgegevens
	11.15	De identiteit van een registrerend zorgprofessional wordt niet vastgelegd, de waarde van de patiëntgegevens in het deeldossier zijn hierdoor onvoldoende te bepalen.	J	status patiëntgegevens
	11.16	De patiënt kan op aanvraag door het ziekenhuis niet correct en/of tijdig worden geïnformeerd over de verwerking van zijn of haar medische gegevens in het deeldossier conform Wbp, het ziekenhuis is hierdoor mogelijk in overtreding met de Wbp.	Ve	acties zijn niet controleerbaar
	11.17	Een deeldossier kan door de beheerverantwoordelijk specialist verwijderd worden binnen de tijdsgrenzen van wet- en regelgeving of tegen de wens van de patiënt in, dit deeldossier is hierdoor niet meer beschikbaar voor andere gebruikers.	Vo	onvolledige patiëntgegevens
	11.18	De patiënt krijgt tegen de wens van de zorgprofessional inzage in aantekeningen, de vertrouwelijkheid van deze aantekeningen wordt hiermee geschonden.	Ve	ongewenste acties patiëntgegevens

Diagnose	12	Identiek aan risico's activiteit 7.		
Vaststellen behandeling	13	Geen relevante risico's.		
Planning behandeling	14	Zie risico's activiteit 3/4.		
Verkrijgen taak	15	Geen relevante risico's.		
Opvragen dossier(s)	16	Zie risico's activiteit 5.		
Uitvoeren taak	17	Identiek aan risico's beschreven bij activiteit 7.		
Registratie medische patiëntgegevens	18	Zie risico's activiteit 11.		
Ontslag patiënt uit ziekenhuis	19	Geen relevante risico's.		
Plannen controle afspraak	20	Zie risico's activiteit 3/4.		
Controle afspraak	21	Zie risico's activiteit 7.		
Registratie medische patiëntgegevens	22	Zie risico's activiteit 11.		
Beheer applicaties (23) / beheer systemen (24)**	23.1	De IT-beheerder heeft toegang tot patiëntgegevens, dit schendt mogelijk de geheimhoudingsplicht zoals opgelegd door de Wgbo.	Ve	ongewenste acties patiëntgegevens
	23.2	Er vinden ongeautoriseerde wijzigingen plaats in de applicatie, dit maakt het gedrag van applicaties onvoorspelbaar.	J	beheer leidt tot fouten

	23.3	Wijzigingen veroorzaken problemen voor de beschikbaarheid van patiëntgegevens, dit kan	T	beheer leidt tot fouten
	23.4	De applicatie kan niet meegroeien met ontwikkelingen in vereisten vanuit actoren en/of wet- en regelgeving.	Ve/J/Vo/T	beheer leidt tot fouten
Ondersteunen toezichthouder (specifieke risico's)	25	Beheerder krijgt inzicht in tot de patiënt herleidbare gegevens, mogelijk is dit een schending van de geheimhoudingsplicht opgelegd aan ziekenhuis / professional.	Ve	ongewenste acties patiëntgegevens
Toezicht houden op het correct gebruik van patiëntgegevens	26.1	De toezichthouder kan niet bepalen welke acties uitgevoerd zijn op patiëntgegevens, controle wordt hiermee praktisch onmogelijk.	Ve/J/Vo/T	controle patiëntgegevens niet mogelijk
	26.2	De toezichthouder kan niet bepalen welke gebruiker een zekere actie heeft uitgevoerd, de toezichthouder kan hierdoor geen individuele gebruikers aanspreken.	Ve/J/Vo/T	controle patiëntgegevens niet mogelijk
	26.3	Een gebruiker kan het uitvoeren van een actie op patiëntgegevens ontkennen, een gebruiker kan niet worden gestraft.	Ve/J/Vo/T	controle patiëntgegevens niet mogelijk
	26.4	De toezichthouder kan een actie van een gebruiker niet herleiden tot een specifiek moment, het wordt onmogelijk te bepalen of het om een oud incident gaat of een recent incident.	Ve/J/Vo/T	controle patiëntgegevens niet mogelijk
	26.5	De toezichthouder heeft onvoldoende inzicht in de situatie waarin een incident heeft plaatsgevonden.	Ve/J/Vo/T	controle patiëntgegevens niet mogelijk

	26.6	De toezichthouder kan niet bepalen wie een autorisatie heeft uitgegeven, dit verlaagt voor professionals de drempel om op een correcte wijze autorisaties uit te geven.	Ve/J/Vo/T	controle patiëntgegevens niet mogelijk
	26.7	Gebruiker/verantwoordelijke van/voor patiëntgegevens kan niet aantonen dat zijn of haar handelen correct is.	Ve/J/Vo/T	controle patiëntgegevens niet mogelijk
Ziekenhuis sturen	27.1	(afhankelijk van specifiek doel) Patiëntgegevens zijn herleidbaar tot individuele patiënten, mogelijk beperkt dit het secundaire gebruik van de gegevens.	Ve	ongewenste acties patiëntgegevens
Toezien op een correcte registratie van patiëntgegevens***	28.1	Geen relevante risico's anders anders als eerder benoemd in verschillende activiteiten.		
Divers	29.1	Externe actor heeft toegang tot deeldossiers en andere gevoelige patiëntgegevens.		
Beheren dossiers	30	Relevante risico's zijn al benoemd bij activiteit 11.		
Toevoegen patiëntverklaring	31	Relevante risico's zijn al eerder benoemd in activiteit 11.		
Afschermen dossiers	32	Relevante risico's zijn al eerder benoemd in activiteit 11.		
Patiënt toegang verschaffen tot de eigen medische patiëntgegevens	33.1	Patiënt heeft onvoldoende toegang tot de eigen medische gegevens.	T	patiëntgegevens niet tijdig beschikbaar

Bijlage D. Patiëntgegevens over de grens

Opmerking vooraf: deze bijlage maakt geen onderdeel uit van het onderzoek en heeft een eigen literatuurlijst.

Nederlandse patiënten betrekken hun zorg niet alleen (meer) binnen de nationale grenzen en dus de grenzen van ons zorgsysteem. Vooral de Nederlandse buurlanden zijn interessante uitwijkingsmogelijkheden voor patiënten welke in Nederland bijvoorbeeld op een wachtlijst zijn geplaatst. Ook in de Europese Unie heeft men dit opgepikt. Er is momenteel dan ook discussie over het bieden van zorg over de grens [1]. Ook verzekeraars bieden de verzekerde de mogelijkheid om de behandeling in het buitenland te ondergaan.

We kunnen dus stromen van medische patiëntgegevens verwachten tussen Nederlandse en buitenlandse ziekenhuizen. Met de aanwezigheid van Internet lijkt er een reële mogelijkheid om patiëntgegevens ook digitaal uit te wisselen. Dit biedt kansen, zo kan in binnen- en buitenland de kwaliteit van zorg (o.a. effectiviteit, efficiëntie en patiëntveiligheid) worden verhoogd door de aanwezigheid van alle relevante medische informatie. Het brengt echter ook een aantal uitdagingen/risico's met zich mee waarvoor aandacht in dit hoofdstuk.

Hoewel het buiten het bereik van dit onderzoek gaat om uitgebreid in te gaan op de risico's van registratie, gebruik en uitwisseling van patiëntgegevens van patiëntgegevens van Nederlanders in buitenlandse ziekenhuizen en het delen van patiëntgegevens met buitenlandse ziekenhuizen, kunnen we op basis van ons onderzoek wel een aantal aandachtspunten aanstippen. Deze aandachtspunten hebben vaak impact op registratie, gebruik en uitwisseling tussen Nederlandse ziekenhuizen, maar ook specifieke kenmerken wanneer we het probleemgebied uitbreiden:

- Identificatie van patiënten.

  Wanneer de patiënt een behandeling ondergaat bij een buitenlands ziekenhuis moet deze uniek kunnen worden geïdentificeerd, voor onder de financiële afwikkeling maar ook om het dossier te kunnen koppelen aan de juiste identiteit. In Nederland gebruiken wij hiervoor het BSN, echter dit beperkt zich tot het Nederlandse zorgsysteem. Waarschijnlijk dient er dan ook te worden gekozen voor een van de volgende twee oplossingen:

  - Er komt een gezamenlijk identificatiemiddel, met bijbehorende voorzieningen om de identificatie op te vragen.
  - Er wordt gekozen voor een oplossing waarbij nationale identificaties kunnen worden vertaald naar identificaties binnen een andere nationaal systeem.

  Beiden mogelijkheden brengen veel uitdagingen met zich mee, ook waar het gaat om vertrouwelijkheid en betrouwbaarheid.

- Centrale of decentrale voorzieningen.

  Het uitwisseling van patiëntgegevens over landgrenzen brengt met zich mee dat er een oplossing moet worden gezocht om de (medische) patiëntgegevens ook in handen te krijgen. Grofweg liggen er twee mogelijkheden voor de hand: centrale voorzieningen voor alle lidstaten of decentrale voorzieningen met toegang tot elkaars voorzieningen. Indien gekozen wordt voor deze laatste oplossing dient ook te worden beslist of we bij zoeken naar beschikbare dossiers alle register willen doorzoeken, of alleen op aangeven van de gebruiker. Ook kan het onwenselijk blijken alle voorzieningen decentraal te houden. Zo zien we dat ook in het Nederlandse EPD, wat getypeerd zou kunnen worden als decentraal, bepaalde voorzieningen centraal geplaatst zijn. Kiezen we echter voor een centrale registratie van medische patiëntgegevens dan kan dit bij het publiek extra weerstand oproepen omdat het te verwachten valt dat dit extra gevoelig valt bij het publiek. Ook leidt dit misschien tot gevoelige

discussies over beheer en eigendom van de voorzieningen en rechten en plichten ten aanzien van de patiëntgegevens.

- Identificatie en autorisatie van gebruikers van patiëntgegevens.

  Hoe identificeren we buitenlandse gebruikers van patiëntgegevens? Evengoed als voor de patiëntidentificatie geldt dat binnen het Nederlandse EPD de gebruikers geïdentificeerd worden via nationale voorzieningen, in dit geval doormiddel van het UZI-nummer. Voor de authenticatie gebruiken we UZI-middelen zoals de UZI-pas, wederom nationale voorzieningen. Een gebruiker buiten het nationale zorgsysteem kan zich momenteel dan ook niet identificeren en authenticeren binnen het nationale EPD. Dus hoe gaan we dit probleem oplossen wanneer gebruikers uit iedere lidstaat zich moeten kunnen identificeren en authenticeren? Ook daarbij liggen grofweg twee oplossingen voor de hand: centrale voorzieningen waar de gebruikers zich kan 'aanmelden' of het 'vertalen' tussen zorgsystemen. Beiden oplossingen vereisen dat er afspraken worden gemaakt. Ook bij de tweede oplossing is het van groot belang dat er afspraken komen over eisen ten aanzien van de uitgifte van identificatienummer en autorisatiemiddelen. Wanneer dit proces ruimte risico laat voor ontoelaatbare risico's dan heeft dit mogelijk een nadelige impact op de nationale systemen van andere lidstaten. Overigens worden kwalificaties van zorgprofessionals ook in andere lidstaten onderkend, dit is nu al geregeld [2].

- Standaarden, normen en wet- en regelgeving.

  Kijken we naar wet- en regelgeving dan zien we dat in Nederland twee wetten een brede en sterke invloed hebben op de (digitale) registratie, gebruik en uitwisseling van patiëntgegevens in het ziekenhuis: Wet bescherming persoonsgegevens (Wbp) en de Wet op de geneeskundige behandelovereenkomst (Wgbo). De Nederlandse Wbp is de Nederlandse uitwerking van de EU Data Protection Directive. Een dergelijke Europese grondslag geldt echter niet voor de Wgbo. Verschillen in wet- en regelgeving kunnen de uitwisseling van patiëntgegevens bemoeilijken of misschien zelfs (in individuele gevallen) onmogelijk maken. Het is dus waarschijnlijk dat er nieuwe afspraken moeten worden gemaakt om dergelijke verschillen (zoveel mogelijk) weg te werken. Waar wet- en regelgeving geen uitsluitsel biedt kan het nodig zijn aanvullende afspraken te maken.

  Waar het gaat om normen dient er overeenstemming te worden over de te hanteren normen, of minimaal dienen er afspraken te worden gemaakt waar normen welke nationaal gehanteerd worden botsen. Er is overigens een Europese norm waar het gaat om gegevensveiligheid in de zorg, de Nederlandse NEN 751X norm is hier bijvoorbeeld van afgeleid.

  De inhoud van deeldossiers uit verschillende nationale zorgsystemen moeten nauwkeurig worden beoordeeld om verschillen te beperken of anders een passende oplossing te zoeken. De kwaliteit van deeldossiers moet ongeveer op hetzelfde niveau liggen om het deeldossier optimaal bruikbaar te maken in alle lidstaten. Ook kunnen er problemen ontstaan wanneer de inhoud van deeldossiers niet goed interpreteerbaar zijn voor gebruikers in lidstaten anders dan de 'bronlidstaat'. In het bijzonder kunnen er problemen ontstaan wanneer problemen niet worden opgemerkt, bijvoorbeeld wanneer begrippen een andere betekenis hebben in verschillende lidstaten. Ook moet er gekozen worden voor één taal in welke patiëntgegevens worden vastgelegd.

  Verantwoordelijkheden en eisen ten aanzien van beheer dienen eveneens onderwerp van discussie te zijn. Wie draagt immers welke verantwoordelijk als bijvoorbeeld een belangrijk deeldossier niet beschikbaar is vanwege een storing in de voorzieningen van de andere lidstaat?

  Wie ziet er toe op de correcte omgang met patiëntgegevens? En wat is een correcte omgang? Met name wanneer normen minder expliciet zijn of er sprake is van culturele verschillen, kan dit een lastige kwestie zijn.

Ook moeten er afspraken worden gemaakt over de financiële afhandeling. In het Nederlandse zorgsysteem is hiervoor het DBC geïntroduceerd. Maar hoe gaan we om met dergelijke gegevens in buitenlandse zorgsystemen?

- Open/gesloten netwerk.

  Om gegevens uit te kunnen wisselen moet er een netwerk aanwezig zijn. Er is de mogelijkheid om te kiezen voor een open netwerk of een gesloten netwerk. In Nederland is gekozen voor deze laatste optie, een oplossing welke minder (grote) risico's met zich meebrengt maar wel een grotere (initiële) investering vraagt. Kiest men voor een oplossing over het Internet dan is er een grotere noodzaak tot overeenstemming tussen de lidstaten over veiligheidskwesties.

- Verschillen tussen zorgsystemen / culturen.

  Verschillende zorgsystemen zijn verschillend ingericht. Dit maakt het mogelijk lastig om te komen met één oplossing voor dit probleem welke werkt voor alle zorgsystemen. Ook kunnen hier fundamentele culturele verschillen aan ten grondslag liggen.

Kortom een korte inventarisatie van de uitdagingen van digitale registratie, gebruik en uitwisseling van patiëntgegevens in en tussen ziekenhuizen in Europees verband toont ons dat dit probleem complex is. Vaak lijkt het redelijk om te verwachten dat een effectieve oplossing alleen bereikt kan worden door vele afspraken en hoge investeringen. Onze verwachting is dan ook niet dat dit een eenvoudige opgave zal zijn die op korte termijn werkelijkheid kan worden.

Literatuurlijst

[1] http://ec.europa.eu/health/ph_overview/co_operation/healthcare/cross-border_healthcare_en.htm
[2] http://www.ribiz.nl/diplomaenwerk/werkeninhetbuitenland/

Bijlage E. Markt

In deze bijlage werpen we een verkennende blik op de EPD-markt. We kijken naar zowel de aanbieders van ziekenhuisinformatiesystemen als wel de afnemers van deze pakketten, de ziekenhuizen. Ook voor deze bijlage geldt dat het geen deel uitmaakt van het onderzoek en een eigen literatuurlijst heeft.

Aanbieders

Op de Nederlandse markt zijn zowel nationale als internationale spelers actief. Recente en betrouwbare cijfers over het marktaandeel van de verschillende producten lijkt helaas te ontbreken, dus we beperken ons tot een aantal voorbeelden van spelers:

- Epic,
- Alert,
- Siemens (product Soarian),
- ChipSoft,
- iSOFT.

75% Van de leveranciers van ZIS'en zijn, volgens planning, medio 2009 gekwalificeerd [1] (deze inschatting gemaakt is in een rapportage over januari en februari 2009). In september 2008 wist de minister van VWS te melden dat 'Vier van de zes belangrijke ziekenhuisinformatiesystemen zijn voorzien van een kwalificatie. De leveranciers van de twee andere systemen treffen voorbereidingen voor kwalificatie.' [2]. Toch is een waarschuwing op zijn plek, met name waar het gaat om internationale spelers is het de vraag of zij altijd gemakkelijk ingang zullen vinden tot de Nederlandse markt, waar het hier vereist is een goedkeuring van NICTIZ te verkrijgen voordat men het ZIS kan aansluiten op het Landelijk Schakel Punt. Het is denkbaar dat systemen zonder XIS-typekwalificatie lastig(er) de markt zullen bereiken, zeker bij de kleinere zorgaanbieders. Het ontbreken van een XIS-typegoedkeuring betekend namelijk een traject waarbij het systeem alsnog uitgebreid moet worden getoetst aan het Programma van eisen aan een Goed Beheerd Zorgsysteem. Met name bij kleinere zorgaanbieders is het niet vanzelfsprekend dat (voldoende) kennis aanwezig is om een dergelijk traject te begeleiden en, met name, de juiste stappen te nemen om problemen te corrigeren. Bij grote organisaties zou echter de omvang en complexiteit van de organisatie het lastig kunnen maken eenvoudig wijzigingen door te voeren waardoor het systeem gaat voldoen aan de normen, na een zorgvuldige initiële selectie.

Ook kunnen er problemen ontstaan wanneer producten onvoldoende aansluiten op het Nederlandse zorgsysteem. Bedenk immers dat de specifieke invulling die gegeven is aan het EPD een nationaal karakter heeft. Weliswaar is hierbij wel gebruik gemaakt van een internationale standaard als HL7v3, echter op hoofdlijnen is het project toch eigen. Het is de vraag in hoeverre het mogelijk als ziekenhuis/IT-partner een pakket van een niet-gekwalificeerde buitenlandse leverancier hierop te laten aansluiten. Ook bijvoorbeeld het DBC is een nationale voorziening, al streeft men wel naar aansluiting op structureren in het buitenland [3]. Bovendien moet er rekening gehouden worden met vereisten welke opgelegd worden door wet- en regelgeving.

Een ander punt van aandacht is de compliance met de NEN 751X-normen, waar deze min of meer verplicht zijn gesteld door de wetgever zoals eerder al toegelicht in *hoofdstuk 3*. Veel van de vereisten in de norm hebben betrekking op organisatorische beheersmaatregelen en daardoor een lage impact op de geautomatiseerde systemen binnen het ziekenhuis. Er zijn dus echter ook eisen welke direct impact hebben op het ziekenhuisinformatiesysteem. Enkele voorbeelden hiervan zijn:

- Validatie van invoergegevens, interne verwerking en uitvoergegevens,
- Het gebruik van digitale handtekeningen,
- Het gebruik van een exclusief communicatiekanaal vanaf een matig risico,
- Eisen ten aanzien van het gebruik van versleuteling.

Er dient te worden opgemerkt dat de norm zich nauwelijks uitspreekt over te hanteren technieken. Toch zouden er problemen kunnen ontstaan wanneer system op een ongebruikelijke manier zijn ingericht en zich hierdoor moeilijk kunnen aanpassen aan de norm.

Merk overigens op dat digitale registratie van patiëntgegevens zeker geen nieuwe ontwikkeling is. Dergelijke techniek bestaan al 20 dan wel in ieder geval 30 jaar [4][5]. HIS, XIS, EMR, EHR zijn een selectie van termen welke door de tijd gebruikt zijn om systemen aan te duiden welke medische gegevens elektronisch opslaan. Ook het digitaal delen van medische gegevens is geen nieuwe ontwikkeling [4]. Toch zijn er slechts enkele landen (waaronder de UK en Zweden) welke een nationaal EPD gereed hebben.

Afnemers

Kijken we naar de afnemerszijde dan kunnen we eenvoudig constateren dat een markt verzekerd wordt door aanstaande wetgeving. De 'wet EPD' is aangenomen door de tweede kamer en ligt momenteel ter behandeling bij de Eerste kamer. Hier is men bezig met de schriftelijke voorbereiding van de behandeling van deze wet in wording en de behandeling van deze wet is uitgesteld tot na het zomerreces. Als deze wet is aangenomen zal deze wet zorgaanbieders verplichten zich aan te sluiten op het LSP, waardoor de zorgaanbieder dus gedwongen is over de juiste en gekwalificeerde systemen te beschikken om gegevens uit te wisselen via het LSP.
Circa 6500 zorgaanbieders zullen worden aangesloten op het LSP, waaronder 95 ziekenhuizen. Momenteel hebben bijna 100 zorgaanbieders zich aangesloten, hiermee zijn er ongeveer 330.000 patiënten-/cliëntendossiers beschikbaar in het EPD. Overigens wordt het LSP 1 juli 2009 opengesteld. In het tweede kwartaal van 2009 staan ruim 800 aansluitingen gepland, waaronder 16 aansluitingen van ziekenhuizen. In de tweede helft van 2009 streeft men naar 2500 tot 3000 nieuwe aansluitingen.

Belangrijk om op te merken is dat de functionaliteit van nationale systemen weliswaar niet wezenlijk verschilt van een regionaal initiatief, het is immers 'slechts' een kwestie van schaalvergroting. Echter er zijn wel degelijk andere aspecten welke extra aandacht vragen. Zo kunnen nationale initiatieven op meer aandacht rekenen van het publiek, al is het belangrijk om op te merken dat hierin wel culturele verschillen bestaan. Zo stelt men bijvoorbeeld in Scandinavië vertrouwen in de zorgprofessional voorop. Ook zal beveiliging, er zijn immers meer partijen en personen betrokken, en performance een grotere rol spelen.

Kijken we naar de acceptatie van het nationale EPD dan zien we verschillende indicaties. Concrete cijfers zijn niet altijd aanwezig, maar een greep uit het recente nieuwsaanbod en onderzoeksuitkomsten omtrent de acceptatie van het EPD geeft ons hierin wel enig inzicht:

'Bestuurders van een vijfde van de Nederlandse ziekenhuizen zien de huidige opzet van het epd niet zitten. Volgens hen staat de patiënt buitenspel bij de uitwisseling van medische gegevens.' [6]

'Men [patiënt/cliënt] ziet vaker voordelen van het EPD dan nadelen' en
'De twee grootste nadelen van het EPD die gezien worden zijn 'mijn medische gegevens kunnen op straat liggen' (52%) en 'kan mijn privacy aantasten' (48%).' en
'Bijna zeven van de tien hebben vertrouwen in de betrouwbaarheid van de uitwisseling van medische gegevens.' [7]

'Sinds de start van het informed consent proces op 1 november jl. tot half maart 2009 zijn circa 438.000 bezwaren ontvangen.' [8]

'Inmiddels heeft al 3 procent van de burgers het 'bezwaarformulier EPD' ingevuld. Onder hen een opvallend hoog aantal artsen.' [9]

SWOT-analyse van het nationale EPD

Sterktes	**Zwaktes**
+ Ruime ervaring met elektronische dossiers. + Reeds bestaande infrastructuur. + Er is veel aandacht voor het digitaal registeren, gebruiken en uitwisselen van patiëntgegevens. + Standaarden zijn beschikbaar.	- Met name kleinere ziekenhuizen beschikken mogelijk niet over voldoende expertise.
Kansen	**Bedreigingen**
+ Effectieve zorg. + Meer efficiëntie. + Kleinere kans op fouten door o.a. een betere beschikbaarheid van dossiers.	- Complexiteit van implementatietraject. - Nationaal EPD wordt onvoldoende geaccepteerd. - Veranderingen leiden tot de noodzaak van extra training in een arbeidsintensieve omgeving.

Literatuurlijst

[1] http://www.minvws.nl/kamerstukken/meva/2009/voortgangsrapportage-elektronisch-patientendossier.asp
[2] http://static.ikregeer.nl/pdf/KST121984.pdf
[3] http://www.dbconderhoud.nl/__news/53/Nieuwe_stap_gezet_in_ontwikkeling_DBC-systematiek
[4] Online medical records : A decade of experience
[5] Hospital information systems: perspectives on problems and prospects, 1979 and 2002
[6] http://www.computable.nl/artikel/ict_topics/overheid/2700050/1277202/ziekenhuizen-zien-epd-niet-zitten.html
[7] http://www.npcf.nl/uploads/files/eindrapport_epd_tns_nipo_npcf.pdf
[8] http://www.minvws.nl/kamerstukken/meva/2009/voortgangsrapportage-elektronisch-patientendossier.asp
[9] http://medischcontact.artsennet.nl/tijdschrift/archief/Tijdschriftartikel/Te-vroeg-voor-landelijk-EPD.htm
[10] http://www.eerstekamer.nl/wetsvoorstel/31466_elektronisch toegang 18 juni
[11] http://www.eerstekamer.nl/9370000/1/j9vvhwtbnzpbzzc/vi30go9l7ztv/f=y.pdf toegang 18 juni
Vraag en antwoord LSP en XIS-typegoedkeuring

Literatuurlijst

[1] Luyendijk, Wubby. "Invoering EPD in 2009 onhaalbaar", *NRC*, 29 december 2008, http://www.nrc.nl/binnenland/article2084080.ece, toegang 3 februari 2009.

[2] van der Beek, Pim. "Minister wil invoering EPD uitstellen", Computable, 22 januari 2009, http://www.computable.nl/artikel/ict_topics/overheid/2842974/1277202/minister-wil-invoering-epd-uitstellen.html, toegang 12 februari 2009.

[3] *Wat het EPD doet*. Website Informatiepunt BSN in de zorg en landelijk EPD, http://www.infoepd.nl/informatiepunt_com/patient_wat_het_epd_doet.php?print=1, toegang 3 februari 2009.

[4] *Welke gegevens worden uitgewisseld*. Website Informatiepunt BSN in de zorg en nationale EPD, http://www.infoepd.nl/informatiepunt_com/patient_welke_gegevens_worden_uitgewisseld.php?print=1, toegang 3 februari 2009.

[5] *Hoe ver staat het met de invoering van de eerste toepassingen?*. Website Nictiz, http://www.nictiz.nl/?mid=9&pg=49#Hoeverstaathetmetdeinvoering, toegang 3 februari 2009.

[6] *"Architectuurvisie AORTA"*. Nictiz, 31 oktober 2008 (versie 6.0.0.0).

[7] *Toegang tot het EPD*. Website Informatiepunt BSN in de zorg en nationale EPD, http://www.infoepd.nl/informatiepunt_com/patient_toegang_tot_het_epd.php?print=1, toegang 3 februari 2009.

[8] *Is mijn privacy voldoende gewaarborgd bij het landelijk EPD?*. Website Informatiepunt BSN in de zorg en nationale EPD, http://infoepd.nl/informatiepunt_com/zorgconsument_vraag_en_antwoord.php?page_id=is_mijn_voldoende_gewaarborgd_bij_het_landelijk_epd_&onderwerp=EPD009282727626263933 9&print=1, toegang 3 februari 2009.

[9] *Voortgangsrapportage elektronisch patiëntendossier*. Ministerie van Volksgezondheid, Welzijn en Sport, 25 maart 2009. http://www.minvws.nl/includes/dl/openbestand.asp?File=/images/meva-2920502-2-_tcm19-180613.pdf, toegang 2 juni 2009.

[10] Katzenbauer M., "Te vroeg voor landelijk EPD", Medisch Contact , nr. 20 jaargang 2009, via http://medischcontact.artsennet.nl/tijdschrift/archief/Tijdschriftartikel/Te-vroeg-voor-landelijk-EPD.htm, toegang 2 juni 2009.

[11] Groot woordenboek van de Nederlandse taal, 14de editie (2005), van Dale.

[12] *"Bedrijfsarchitectuur AORTA"*. Nictiz, 31 oktober 2008 (versie 6.0.0.0).

[13] Kenneth D Mandl, Peter Szolovits, Isaac S Kohane, "Public standards and patients' control: how to keep electronic medical records accessible but private", *Information in practice*, 3 feb, 2001, p. 283.

[14] Randolph C. Barrows, Jr., MD, Paul D. Clayton, PhD, "Privacy, Confidentiality, and Electronic Medical Records", 1996.

[15] *Ben ik de eigenaar van mijn medische gegevens?*. Website Informatiepunt BSN in de zorg en nationale EPD, http://www.infobsnzorg.nl/informatiepunt_com/eigenaar_medische_gegevens.php?print=1, toegang 16 februari 2009.

[16] Evaluatierapportage pilot WDH. Telematica Instituut, 2008.

[17] C.P. Louwerse, "Elektronisch Patientendossier", *Nederlands Tijdschrift voor Klinische Chemie en Laboratoriumgeneeskunde*, 2004 : 29, 217 - 219.

[18] Roy Schoenberg, Charles Safran, "Internet based repository of medial records that retains patient confidentiality", *BMJ*, 2000.

[19] Dan Childs, Haeree Chang, Audrey Grayson. "President-Elect Urges Electronic Medical Records in 5 Years", *ABC News*, 9 januari 2009, http://abcnews.go.com/print?id=6606536, toegang 17 feb 2009.

[20] *Summary Care Records (SCR).* Website National Health Services, http://www.connectingforhealth.nhs.uk/systemsandservices/nhscrs, toegang 17 feb 2009.

[21] David Carman, Nicky Britten, "Confidentiality of medical records: the patient's perspective*", British Journal of General Practice*, september 1995, p. 485 - 488.

[22] Ross J. Anderson, "A Security Policy Model for Clinical Information Systems", *IEEE Computer Society*, 1996.

[23] *"Informatiesysteem architectuur"*. Nictiz, 31 oktober 2008 (versie 6.0.0.0).

[24] *Wat is een zoekpad?*. Website Informatiepunt BSN in de zorg en nationale EPD, http://www.infoepd.nl/informatiepunt_com/vraag_en_antwoord_za_epd.php?page_id=wat_is_een_zoekpad&onderwerp=BSN5555555555555555444&overzicht=1, toegang 19 maart 2009.

[25] Programma van Eisen voor een Goed Beheerd Zorgsysteem. Nictiz. 31 oktober 208.

[26] Beoordelingskader voor de geautomatiseerde gegevensverwerking rondom Diagnose Behandeling Combinaties (DBC's). Norea ZekeREzorg.

[27] Prive communicatie Joost Gerrits. PricewaterHouseCoopers

[28] Prive communicatie Reino Petrona. PricewaterHouseCoopers

[29] *Afschaffen regeling Administratieve organisatie / Interne controle (AO/IC) uitgesteld*. Website Nederlandse Zorgautoriteit, http://www.nza.nl/aanbieder/Actueel/Afschaffen_AO-IC_uitgesteld/, toegang 21 mei 2009.

[30] G. Serour, "Confidentiality, privacy and security of patients' health care information", International Journal of Gynecology & Obstetrics, Volume 93, Issue 2, Pages 184-186

[31] Mr. L.B. Sauerwein, Mr. J.J. Linnemann, "Handleiding voor verwerkers van persoonsgegevens". Minsterie van Justitie, april 2002.

[32] Wet op de geneeskundige behandelingsovereenkomst.

[33] Architectuurontwerp basisinfrastructuur in de zorg. Nictiz. 16 november 2008.

[34] *About HL7*. Website HL7, http://www.hl7.org/about/hl7about.htm, toegang 11 maart 2009.

[35] *Begrippenlijst*. Website Informatiepunt BSN in de zorg en landelijk EPD, http://www.infoepd.nl/informatiepunt_com/begrippenlijst.php, toegang 3 februari 2009.

[36] Programma van Eisen LSP. Nictiz. 31 oktober 2008.

[37] NEN 7510. Nederlands Normalisatie-instituut, april 2004.

[38] Eindrapportage Evaluatie Elektronisch Patiëntdossier. TNS NIPO.

[39] Jane Grimson, William Grimson, Wilhelm Hasselbring. "The SI Challenge in health care", Communications of the ACM. Volume 43, Number 6 (2000), Pages 48-55.

[40] Handleiding voor verwerkers van persoonsgegevens: Wet bescherming persoonsgegevens. Ministerie van Justitie, april 2002. Mr. L.B. Sauerwein, Mr J.J. Linneman.

[41] Wet op de geneeskundige behandelingsovereenkomst

[42] Privacy-wetgeving en het omgaan met patiëntgegevens: KNMG Handleiding voor artsen. KNMG. mei 2001

[43] *"Informatiesysteem architectuur"*. Nictiz, 31 oktober 2008 (versie 6.0.0.0).

[44] Richard Whiddett, Inga Hunter, Judith Engelbrecht, Jocelyn Handy. "Patients' attitudes towards sharing their health information", International Journal of Medical Informatics (2006) 75, 530 - 541.

[45] Kenneth D Mandl, Peter Szolovits, Isaac S. Kohane. "Public standards and patients' control: how to keep electronic medical records accessible but private", BMJ, volume 322, 3 februari 2001.

[46] Helma van der Linden, Dipak Kalra, Arie Hasman, Jan Talmon. "Inter-organizational future proof EHR systems: A review of the security and privacy related issues", International Journal of Medical Informatics 78 (2009) 141-160.

[47] Werkprocessen landelijk EPD. Nictiz. 15 juli 2008.

[48] Teun Zuiderent, Marc Berg. *"Hergebruik van zorginformatie"*, Informatie @ zorg, jaargang 31 nr. 2 juni 2002.

[49] Randolph C. Barrows, Jr. MD, Paul D. Clayton, PHD. *Privacy, Confidentiality, and Electronic Medical Records*. Journal of the America Mecial Informatics Associaton, volume 3, nummer 2, mart april 1996.

[50] Xiping Song, Beatrice Hwong, Gilberto Matos, Arnold Rudorfer, Christopher Nelson, Minmim HJan, Andrei Girenkov. *Understanding Requirements for Computer-Aided Healthcare Workflows: Experiences and Challenges*.

[51] Frank K. Uckert, Hans-Ulrich prokosch, PHD. *Implementing Security And Access Control Mechanisms For An Electronic Healthcare Record*. AMIA, 2002.

[52] Rob Ward, Christine Stevens. *The attitudes of health care staff to information technology: a comprehensive review of the research literature*. Health Information and Libraries Journal, 25, 81-97.

[53] Bernd Blobel. *Authorisation and Acces Control for Electronic Health Record Systems*. International Journal of Medical Informatics (2004), 73, 251-257.

[54] Annette J. Braunack-Mayer, Ea C. Mulligan. *Sharing patient information between professionals: confidentiality and ethics*, MJA volume 178, 17 maart 2008.

[55] Ruth Boaden, Paul Joyce. *Developing the electronic health record: what about patient safety?*, Healht Service Management Research (2006) 19, 94-104.